

Appendix A

Glossary

CONCEPT or TERM	DESCRIPTION
Acceptable Risk	The residual (final) risk remaining after application of controls, i.e. Hazard Controls / Risk Controls, have been applied to the associated Contributory Hazards; that have been identified and communicated to management for acceptance.
Accident	<p>An unplanned fortuitous event that results in harm, i.e. loss, fatality, injury, system loss; also see Risk Severity. The specific type and level of harm must be defined; the worst case severity that can be expected as the result of the specific event under study. Various contributory hazards can result in a single accident; also see Contributory Hazard, Cause, Root Cause, and Initiating Events.</p> <p><u>Accident.</u> An unplanned event that results in a harmful outcome; e.g. death, injury, occupational illness, or major damage to or loss of property.</p> <p><u>Accident.</u> An unplanned event or series of events resulting in:</p> <p>Death. Injury. Occupational illness. Damage to or loss of equipment or property. Damage to the environment.</p>
Accreditation	A formal declaration by the Accreditation Authority that a system is approved to operate in a particular manner using a prescribed set of safeguards.
Act	A formal decision or law passed by a legislative body.
Administrative Hazard Control	Administrative controls to eliminate or reduce safety related risk, i.e. training, programs, procedures, warnings, instruction, tasks, plans; also see Risk Control.
Anomalous Behavior	Behavior which is not in accordance with the documented requirements
Architecture	The organizational structure of a system, identifying its components, their interfaces and a concept of execution between them.
Assumed Risk	The residual risk associated with a specific hazardous event or primary hazard, which has been accepted by management.
Audit	An independent examination of the life cycle processes and their products for compliance, accuracy, completeness and traceability.
Audit Trail	The creation of a chronological record of system activities (audit trail) that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or an event in a transaction from its inception to its final results.
Authenticate	(1) To verify the identity of a user, device, (or other entity in a system, often as a prerequisite to allowing access to resources in the system. (2) To verify the integrity of data that has been stored, transmitted, or otherwise exposed to possible unauthorized modification.
Barrier	A material object or set of objects that separates, Demarcates, or services as a barricade; or

CONCEPT or TERM	DESCRIPTION
	something immaterial that impedes or separates. Both physical and non-physical barriers are utilized and applied in hazard control; i.e. anything used to control, prevent or impede unwanted adverse energy flow and / or anything used to control, prevent or impede unwanted event flow.
Baseline	The approved, documented configuration of a software or hardware configuration item, that thereafter serves the basis for further development and that can be changed only through change control procedures.
Cause	Something that brings about an event; a person or thing that is the occasion of an action or state; a reason for an action or condition.
Certification	<p>Legal recognition by the certification authority that a product, service, organization or person complies with the applicable requirements. Such certification comprises the activity of checking the product, service, organization or person and the formal recognition of compliance with the applicable requirements by issue of certificate, license, approval or other document as required by national law or procedures. In particular, certification of a product involves:</p> <p>(a) the process of assuring the design of a product to ensure that it complies with a set of standards applicable to that type of product so as to demonstrate an acceptable level of safety, (acceptable risk);</p> <p>(b) the process of assessing an individual product to ensure that it conforms to the certified type design;</p> <p>(c) the issue of any certificate required by national laws to declare that compliance or conformity has been found with applicable standards in accordance with item (a).</p>
Certification Authority	The organization or person responsible within the state (country) concerned with the certification of compliance with applicable requirements.
Class(es)	Parameters of risk are classified in order to conduct analysis, evaluations, reviews, presentations, etc.; i.e. generic contributory hazards, generic risks, generic events.
Code	A collection of laws, standards, or criteria relating to a particular subject.
Component	A combination of parts, devices, and structures, usually self-contained, which performs a distinctive function in the operation of the overall equipment.
Configuration	The requirements, design and implementation that define a particular version of a system or system component.
Configuration Control	The process of evaluating, approving or disapproving, and coordinating changes to configuration items after formal establishment of their configuration identification.
Configuration Item	A collection of hardware or software elements treated as a unit for the purpose of configuration management.
Configuration Management	The process of identifying and defining the configuration items in a system, controlling the release and change of these items throughout the system life cycle, recording and reporting the status of configuration items and change requests, and verifying the completeness and correctness of configuration items.
Contributory	The potential for harm. An unsafe act and / or unsafe condition which contributes to the

CONCEPT or TERM	DESCRIPTION
Hazard	accident, (see cause, root cause, contributory events, initiator; the potential for adverse energy flow to result in an accident.) A hazard is not an accident. A failure or a malfunction can result in an unsafe condition, and / or unsafe act. Human error can result in an unsafe act. Contributory Hazards define the contributory events that lead to the final outcome. For simplicity, Contributory Hazards can also include Initiating Events and Primary Hazards. Sequential logic defining the Hazardous Event should remain consistent throughout the hazard analysis process.
Consequence	See Risk Severity.
Control	See Risk Control
Criticality	Reliability term. The degree of impact that a malfunction has on the operation of a system.
Critical Path	Defines the sequence of events that control the amount of time needed to complete the effort described within the PERT (Program Evaluation Review Technique) network.
Danger	Danger expresses a relative exposure to a hazard. A hazard may be present, but there may be little danger because of the precautions taken.
Damage	Damage is the severity of injury, and / or the physical, and/ or functional, and /or monetary loss that could result if hazard control is less than adequate.
Debug	The process of locating and eliminating errors that have been shown, directly or by inference, to exist in software.
Deductive Analysis	A top down approach of analysis logic: "What can cause a specific event to occur?"
Derived Requirements	Essential, necessary or desired attributes not explicitly documented, but logically implied by the documented requirements.
Development Configuration	The requirements, design and implementation that define a particular version of a system or system component.
Design Handbooks, Guides and Manuals	Contain non-mandatory general rules, concepts, and examples of good and best practices to assist a designer or operator.
Emulator	A combination of computer program and hardware that mimic the instruction and execution of another computer or system.
Engineering Controls	Engineering design controls to eliminate or reduce safety related risks; also Hazard Control and Risk Control.
Entity Item	That which can be individually described and considered. May be an activity, process, product, organization, system, person or any combination thereof.
Environment	(a) The aggregate of operational and ambient conditions to include the external procedures, conditions, and objects that affect the development, operation, and maintenance of a system. Operational conditions include traffic density, communication density, workload, etc. Ambient conditions include weather, emi, vibration, acoustics, etc. (b) Everything external to a system which can affect or be affected by the system.
	An act that through ignorance, deficiency, or accident departs from or fails to achieve what

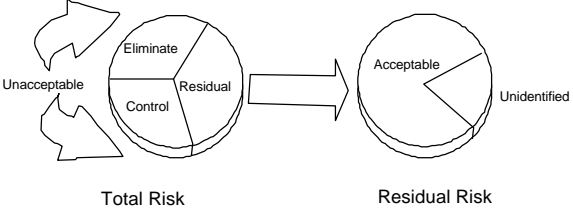
CONCEPT or TERM	DESCRIPTION
Error	should be done. Errors can be predictable and random. Errors can also be categorized as primary or contributory. Primary errors are those committed by personnel immediately and directly involved with the accident. Contributory errors result from actions on the part of personnel whose duties preceded and affected the situation during which the results of the error became apparent. The difference between a computed, observed, or measured value or condition and true, specified, or theoretically correct value or condition. A mistake in engineering, requirement specification, or design, implementation, or operation which could result in a failure, and /or contributory hazard. There are four types of Human Errors: 1) Omission 2) Commission 3) Sequence 4) Timing
Explosion Proof	The item is designed to withstand an internal explosion; designed to vent explosive bases below ignition temperature.
Fail-Operational	A characteristic design which permit continued operation in spite of the occurrence of a discrete malfunction.
Fail-safe	A characteristic of a system whereby any malfunction affecting the system safety will cause the system to revert to a state that is known to be within acceptable risk parameters.
Fail-Soft	Pertaining to a system that continues to provide partial operational capability in the event of a certain malfunction.
Failure	Reliability term. The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration. A failure may result in an unsafe condition and / or act, i.e. a hazard; the termination of the ability of a system element to perform a required function; the lack of correct performance. Failures and hazards are not interchangeable.
Firmware	The combination of a hardware device and computer instructions and data that reside as read-only software on that device.
Formal Verification	The process of evaluating the products of a given phase using formal mathematical proofs to ensure correctness and consistency with respect to the products and standards provided as input to that phase.
Formal Qualification Review	Formal evaluation by top management of the status and adequacy of the quality system in relation to quality policy and objectives.
Formal Qualification	The process that allows the determination of whether a configuration item complies with the requirements allocated to it.
Hazard	<p>The potential for harm; also see Contributory Hazard, Primary Hazard. A hazard is not an accident. Per FAA Order 8040.4 a " Condition, event, or circumstance that could lead to or contribute to an unplanned or undesired event."</p> <p><u>Hazard or hazardous condition.</u> Anything, real or potential, that could make possible, or contribute to making possible, an accident.</p> <p><u>Hazard.</u> A condition that is prerequisite to an accident.</p>
Hazardous	An accident; also see Accident. It should be noted that a Hazardous Event is not being defined

CONCEPT or TERM	DESCRIPTION
Event	<p>an occurrence that creates a hazard. This logic indicates that a Hazardous Event is an occurrence that creates the potential for harm; Initiating Event, or Root Cause, are more appropriate terms.</p> <p>The Hazardous Event (now) defines the total sequence of events from the Initiating Event to the final outcome, the harm, the Initiating Event, Contributory Hazards, Primary Hazard, and Risk Severity.</p> <p>The Hazardous Event under study is considered open or closed depending Report Status on the status of Hazard Control.</p> <p>The Hazardous Event under study is considered open; the corrective action Report Status evaluation and verification is in process. The status will remain open until (Open) management has reviewed the actions taken and accepted the associated risk. All related Contributory Hazards are to be evaluated.</p> <p>The hazardous Event under study is considered closed; the corrective Report Status action evaluation and verification is completed, and management has (Closed) reviewed the actions taken and has accepted the associated risk.</p>
Hazard Probability	<p>Hazard Probability defines in quantitative or qualitative terms, the estimated probability of the specific Contributory Hazards which are defined within the Hazardous Event under study; possible elements within a fault tree.</p> <p>Note that hazard probability is not defined as the aggregate probability of occurrence of the individual hazardous events that create a specific hazard; see Hazardous Event and Accident. Also note that Hazard Probability is not the same as likelihood; see likelihood.</p> <p><u>Hazard Probability</u>. The aggregate probability of occurrence of the individual events (conditions).</p> <p><u>Hazard Severity</u>. An assessment of the consequences of the worst credible accident that could be caused by a specific hazard.</p>
Hazard Tracking and Resolution.	<p>A tracking log is maintained for closeout. Risk Tracking and Risk Resolution should be conducted throughout the system life cycle. Risk/Hazard Controls are to be formally verified.</p>
Inadvertent Operation	<p>Unintentional operation.</p>
Independent Verification & Validation (IV&V)	<p>Confirmation by independent examination and provision of objective evidence that specified requirements have been fulfilled, and that the particular requirements for a specific intended use are fulfilled.</p>
Inductive	<p>A bottom-up analysis approach of analysis logic: "What happens if a specific failure occurs?"</p>

CONCEPT or TERM	DESCRIPTION
Analysis	
Incident	<p>A near miss accident with minor consequences that could have resulted in greater loss.</p> <p>An unplanned event that could have resulted in an accident, or did result in minor damage, and which indicates the existence of, though may not define, a hazard or hazardous condition. Sometimes called a mishap.</p>
Initiating Events	<p>Initiating Events; initiator; the contributory hazard; unsafe act and / or unsafe condition that initiated the adverse event flow, which resulted in the hazardous event under evaluation; also see Root Cause.</p>
Intrinsically Safe Design	<p>Designers determine which hazards could be present, the level of associated risk that could constitute danger, and the controls to assure acceptable risk. Nothing is perfectly safe; see safe.</p>
Inspection	<p>A static technique that relies on visual examination of development products to detect deviations, violations or other problems.</p>
Latent	<p>Present and capable of becoming though not now visible or active.</p>
Likelihood	<p>Likelihood defines in quantitative or qualitative terms, the estimated probability of the specific Hazardous event under study. Likelihood is one element of associated risk. Fault Trees and other models can be constructed and individual Hazard Probabilities are estimated, and likelihood can be calculated via Boolean Logic. It should be noted that estimated likelihood defined in conventional hazard analysis may be appropriate due to the variability, conference, resources, and other factors.</p> <p>See chapter 3 for specific definitions of likelihood.</p>
Malfunction	<p>Fail to operate in the normal or usual manner. Any anomaly which results in system deviation.</p>
Maintainability	<p>The ability of an item to be retained in or restored to specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures, resources and equipment at each prescribed level of maintenance and repair.</p>
Managing Activity	<p>FAA organization assigned acquisition management responsibility for the system, facility, or prime or associated contractors or subcontractors who wish to impose system safety tasks on their suppliers.</p>
Methodology	<p>A particular procedure or set of procedures.</p>
Mishap	<p>A source of irritation, annoyance, grievance, nuisance, vexation, mortification. Note that mishap is not a synonym for accident. It is more appropriate to consider a mishap a minor accident.</p> <p>A hazard. Note that the use of mishap is different within the FAA community than as used in MIL-STD-882C. The latter equates mishap to an accident.</p>
N-Version Software	<p>Software developed and tested to fulfill a set of requirements where multiple versions of software are intentionally made independent and different. Differences can be in some or all of: specifications, design, use of language, algorithms, data structures, etc.</p>
Non-Developmental	<p>Deliverable part not developed as a part of the developmental process being addressed. The developer, or some other party but provides software - deliverable software that is not</p>

CONCEPT or TERM	DESCRIPTION
Item (NDI)	developed under the contract. Non-developmental software may also be referred to as reusable software, government furnished software, commercially available software, or Commercial Off-The-Shelf (COTS) software.
Non-Programmable (N-P) System	A system based upon non-programmable hardware devices (i.e., a system not based on programmable electronics. NOTE: Examples would include hardwired electrical or electronic systems, mechanical, hydraulic, or pneumatic systems, etc.
Objective Evidence	Information, which can be proved true, based on facts obtained through observation, measurement, test or other means.
Optimum Safety	The associated risks that have been identified have been accepted provided that all identified controls are implemented and enforced.
Phase	Defined segment of work. Note: a phase does not imply the use of any specific life-cycle model, nor does it imply a period of time in the development of a product.
Practice	Recommended methods, rules, and designs for voluntary compliance.
Process	Set of inter-related resources and activities, which transform inputs into outputs.
Product Service History	Historical data generated by activities at the interface between the supplier and the customer and by supplier internal activities to meet the customer needs regarding the quality, reliability and safety trends of the product or service.
Product Liability	Generic term used to describe the onus on a producer or others to make restitution for loss related to personal injury, property damage or other harm caused by a product.
Proximate Cause	The relationship between the plaintiff's injuries and the plaintiff's failure to exercise a legal duty, such as reasonable care.
Primary Hazard	A primary hazard is one that can directly and immediately results in: loss, consequence, adverse outcome, damage, fatality, system loss, degradation, loss of function, injury, etc. The primary hazard is also referred to as: catastrophe, catastrophic event, critical event, marginal event, and negligible event.
Quality Assurance	A planned and systematic pattern of actions necessary to provide adequate confidence that an item or product conforms to established requirements.
Quality Audit	Systematic and independent examination to determine whether quality activities and related results comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve objectives.
Quality Evaluation	Systematic examination of the extent to which an entity is capable of fulfilling specified requirements.
Qualification Process	Process of demonstrating whether an entity is capable of fulfilling specified requirements.
Quantitative Assessment.	In any discussion of mishap risk management and risk assessment, the question of quantified acceptability parameters arises. Care should be exercised, under such conditions not to forget the limitations of a mathematical approach. In any high-risk system, there is a strong temptation to rely totally on statistical probability because, on the surface, it looks like a convenient way to measure safety "who can argue with numbers"? To do so, however, requires that the limitations and principles of this approach are well understood and that past engineering experience is not ignored. Quantitative acceptability parameters must be well

CONCEPT or TERM	DESCRIPTION
	<p>defined, predictable, demonstrable, and above all, useful. They must be useful in the sense that they can be easily related to the design and the associate decision criteria. More detail may be found in chapter 7 on the limitations of the use of probabilities.</p> <p>Many factors fundamental to system safety are not quantifiable. Design deficiencies are not easily examined from a statistical standpoint. Additionally, the danger exists that system safety analysts and managers will become so enamored with the statistics that simpler and more meaningful engineering processes are ignored. Quantification of certain specific failure modes, which depend on one of two system components, can be effective to bolster the decision to accept or correct it.</p> <p>General risk management principles are:</p> <ol style="list-style-type: none"> a. All human activity involving a technical device or process entails some element of risk. b. Most hazards (safety risks) can be neutralized or controlled. c. Hazards should be kept in proper perspective. Weighing the risk does this by knowledge gained through analysis and experience against program need. d. System operations represent a gamble to some degree; good analysis assists the MA in controlling the risk. e. System safety analysis and risk assessment does not eliminate the need for good engineering judgment. f. It is more important to establish clear objectives and parameters for risk assessment than to find a cookbook approach and procedure. g. There is no "best solution" to a safety problem. There are a variety of directions to go. Each of these directions may produce some degree of risk reduction.
Redundancy	The existence in a system of more than one means of accomplishing a given function.
Reliability	The ability of a system to perform its required functions under stated conditions for a specified period of time. A reliable system is no total assurance of acceptable risk.
Requirements	Statements describing essential, necessary or desired attributes.
Requirements Specification	Specification that sets forth the requirements for a system or system component.
Risk	Risk is an expression of possible loss over a specific period of time or number of operational cycles. It may be indicated by the probability of an accident times the damage in dollars, lives,

CONCEPT or TERM	DESCRIPTION
	<p>and / or operating units.</p> <p>Hazard Probability and Severity are measurable and, when combined, give us risk.</p> <p><u>Total risk</u> is the sum of identified and unidentified risks.</p> <p><u>Identified risk</u> is that risk which has been determined through various analysis techniques. The first task of system safety is to identify, within practical limitations, all possible risks. This step precedes determine the significance of the risk (severity) and the likelihood of its occurrence (hazard probability). The time and costs of analysis efforts, the quality of the safety program, and the state of technology impact the number of risks identified.</p> <p><u>Unidentified risk</u> is the risk not yet identified. Some unidentified risks are subsequently identified when a mishap occurs. Some risk is never known.</p> <p><u>Unacceptable risk</u> is that risk which cannot be tolerated by the managing activity. It is a subset of identified risk that must be eliminated or controlled.</p> <p><u>Acceptable risk</u> is the part of identified risk that is allowed to persist without further engineering or management action. Making this decision is a difficult yet necessary responsibility of the managing activity. This decision is made with full knowledge that it is the user who is exposed to this risk.</p> <p><u>Residual risk</u> is the risk left over after system safety efforts have been fully employed. It is not necessarily the same as acceptable risk. Residual risk is the sum of acceptable risk and unidentified risk. This is the total risk passed on to the user.</p> 
Risk Analysis	The development of qualitative and / or quantitative estimate of risk based on evaluation and mathematical techniques.
Risk Acceptance.	<p>Accepting risk is a function of both risk assessment and risk management. Risk acceptance is not a simple matter and the concept is difficult for some to accept. Several points must be kept in mind.</p> <p>(1) Risk is a fundamental reality.</p>

CONCEPT or TERM	DESCRIPTION
	<p>(2) Risk management is a process of tradeoffs.</p> <p>(3) Quantifying risk doesn't ensure safety.</p> <p>(4) Risk is a matter of perspective.</p> <p>On the surface, taking risks seems foolish and to be avoided. Everything we do, however, involves risk. Defining acceptable risk is subjective and perceived risks are often as important as actual risks. Risks imposed on us by others are generally considered to be less unacceptable than those inherent in nature. There are dangers in every type of travel, but there are dangers in staying home--40 percent of all fatal accidents occur there. There are dangers in eating most food caused by pesticides, preservatives, natural fats, or just eating more than necessary. There are breathing related dangers in industrial and urban areas. The results of air pollution leads to the death of at least 10,000 Americans each year; inhaling natural radioactivity is believed to kill a similar number; and many diseases are contracted by inhaling germs. 12,000 Americans are killed each year in job related accidents, and probably 10 times that number die from job related illness. There are dangers in exercising and dangers in not getting enough exercise. Risk is an unavoidable part of our everyday lives.</p> <p>We all accept risk, knowingly or unknowingly. In a FAA program, it is the ultimately the responsibility of the MA to determine how much and what kind is to be accepted and what is not. In the real world, making this decision is a trade-off process involving many inputs. As tradeoffs are being considered and the design progresses, it may become evident that some of the safety parameters are forcing higher program risk. From the program manager's perspective, a relaxation of one or more of the established parameters may appear to be advantageous when considering the broader perspective of cost and performance optimization. The program manager has the authority and responsibility, in some circumstances, to make a decision against the recommendation of his system safety manager. The system safety manager must recognize such management prerogatives.</p> <p>A prudent program manager must make a decision whether to fix the identified problem or formally document acceptance of the added risk. In some cases, this requires contract or system specification modification. When the program manager decides to accept the risk, the decision must be coordinated with all affected organizations and then documented so that in future years everyone will know and understand the elements of the decision and why it was made. It also provides necessary data if the decision must be revisited.</p>
Risk Assessment	The process by which the results of risk analysis are used to make decisions.
Risk Control	The Risk associated with the hazardous event under study is adequately controlled, by the reduction of severity and / or likelihood, via the application of engineering and/ or administrative hazard controls. Anything that mitigates or ameliorates the risk. See system

CONCEPT or TERM	DESCRIPTION
	safety design order of precedence in Chapter 3.
Risk Hazard Index.	<p>By combining the probability of occurrence with hazard severity, a matrix is created where intersecting rows and columns are defined by a Risk Hazard Index (RHI). The risk hazard index forms the basis for judging both the acceptability of a risk and the management level at which the decision of acceptability will be made. The index may also be used to prioritize resources to resolve risks due to hazards or to standardize hazard notification or response actions.</p> <p>Prioritization may be accomplished either subjectively by qualitative analyses resulting in a comparative hazard risk assessment or through quantification of the probability of occurrence resulting in a numeric priority factor for that hazardous condition.</p>
Risk Management	<p>The application of management methods for the identification, evaluation, elimination and control of all forms of risk. This effort is not confined only to safety-related risks. Risk Management comprised of two parts, Risk Control and Risk Finance. Risk Control considers all aspects in System Safety, Safety Management, and Safety Engineering. Risk Finance considers insurance, risk pooling, and self-insurance.</p>
Risk Perspectives.	<p>There are three different perspectives in safety risk assessment:</p> <ol style="list-style-type: none"> 1. Standpoint of an INDIVIDUAL exposed to a hazard. An individual exposed to a hazard is primarily concerned with the questions: How large is the probability that I will be killed or injured in an accident? How much does my individual risk due to this hazard increase my normal fatality rate? INDIVIDUAL RISK is defined as the (usually annual) probability that an identified person will be killed or injured as a consequence of an accident. 2. Standpoint of the SOCIETY. Besides being interested in guaranteeing minimum individual risk for each of its members, society is concerned about the total risk to the general public: How large are the total losses (e.g., per year) from a hazardous activity? The risk to society is called COLLECTIVE RISK. If expressed in terms of annual risks, it corresponds to the respective value shown in annual accident statistics. 3. Standpoint of the INSTITUTION RESPONSIBLE FOR THE ACTIVITY. The institution responsible for an activity can be a private company or a government agency. From their point of view, it is not only essential to keep individual risks of employees or other persons and the collective risk at a minimum but also to avoid catastrophic and spectacular accidents. As experience clearly demonstrates (Bhopal, Seveso, Challenger, etc.), such catastrophic accidents damage the reputation, the image, and even the prosperity of the, institution responsible for the activity. Such risks are defined as INSTITUTIONAL RISKS. <p>3.7 Residual Risk. To make important program decisions, the PM must know what residual risk exists in the system being acquired. When such risks are marginally acceptable or potentially unacceptable, the PM is required to raise the presence of residual risk to higher levels of authority such as the Service Director or Associate/Assistant Administrator for action</p>

CONCEPT or TERM	DESCRIPTION
	<p>or acceptance. To present a cohesive description of the hazard to this higher level of decision making, all analyses performed and either the contractor or the FAA must document actions taken to control the hazard. In some contractual situations, the PM may apply additional resources or other remedies to help the contractor satisfactorily resolve the issue. If not, the PM can add his position to the contractor information and forward the matter to a higher decision level. A decision matrix very similar to a Risk Hazard Index called in this example a Risk Hazard Level index can be used to establish which decisions fall under the PM and which should be forwarded to a higher organizational level.</p>
Risk Severity	<p>The harm expected should the hazardous event occur, (i.e., loss, consequence, adverse outcome, damage, fatality, system loss, degradation, loss of function, injury) considering the risk associated with the hazardous event under evaluation.</p> <p>See chapter three for specific definitions of severity. Severity ranges should be sized so that events within each category are of comparable severity. Equating the severity of event and conditions, which can cause one fatality with those, which can cause 100 or 1,000 does not make sense. The potential problems associated with sizing of the severity ranges grow as the size of the system grows. Program managers need to be provided with risk information that has the fidelity to distinguish the hazardous events that meet general criteria.</p> <p>Severity range thresholds for each severity category should be comparable when considering personal, system, or facility losses. For example, events or conditions that could cause the loss of an entire aircraft or facility would be categorized by MIL-STD-882 as catastrophic. Loss of a single crewman, mechanic, or passenger would also fall in the catastrophic category. Severe injuries, such as total loss of sight of a mechanic, and system damage of several million dollars are not normally considered to have equal value, even though both are in the critical category.</p> <p>If the RHI ranking criteria use risk as a function of severity and probability, quantitative scales or qualitative scales based on quantitative logic should be used. If the concept that the expected losses (or risk) associated with a hazardous event or condition may be estimated by multiplying the expected severity of the accident by the probability of the accident, then some sort of quantitative basis is necessary. Failure to provide a quantitative basis for the scales can cause significant confusion and dissipation of safety resources when an arbitrary risk ranking scale is used.</p> <p>Develop the severity values using order of magnitude ranges. There are several advantages to separating severity categories by orders of magnitude ranges: They include:</p> <ul style="list-style-type: none"> Limiting the likelihood of misuse of the analysis. Avoiding meaningless hair-splitting arguments. Simplifying severity assessment during PHAs without impacting usefulness.

CONCEPT or TERM	DESCRIPTION
	<p>Quantify the threshold values for the probability ranges. Quantification reduces confusion associated with strictly qualitative definitions. Although it is impossible to quantify the ranges in 882(C) due to its extremely broad application, developing quantified probability ranges for specific systems is a relatively easy task to accomplish.</p> <p>The probability of occurrence should refer to the probability of an accident/consequence as opposed to the probability of an individual hazard/basic event occurring. The typical accident sequence is much more complicated than a single line of erect dominos where tipping the first domino (hazard) triggers a clearly predictable reaction.</p> <p>Develop the probability values using order of magnitude ranges.</p>
Reaction Time	Human response movement time plus response initiation time.
Root Cause	The contributory events, initiating events, which started the adverse event flow are considered root causes. Should these causes be eliminated the hazardous event would not have occurred. It should be noted that accidents are the result of many contributors, both unsafe acts and /or unsafe conditions; also see Contributory Hazards, Hazard.
Safe	<p>Freedom from all forms of harm. Nothing is safe. General term denoting an acceptable level of risk of, relative freedom from, and low probability of harm. The associated risks that have been identified have been accepted provided that all identified controls are implemented and enforced.</p> <p><u>Safety or Safe.</u> Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment.</p> <p>Note that absolute safety is not possible because complete freedom from all hazardous conditions is not possible. Therefore, safety is a relative term that implies a level of risk that is both perceived and accepted. Thus the emphasis in SSPs as reflected in the definitions above is in managing risk. Chapter 3(FAA SS HB) describes the risk management process. "System" is also a relative term. A subsystem can be viewed as a system with more narrow predetermined boundaries than the system. System safety is not an absolute quantity either. System safety is an optimized level of risk that is constrained by cost, time, and operational effectiveness (performance). System safety requires that risk be evaluated and the level of risk accepted or rejected by an authority. Finally, system safety is a discipline employed from the initial design steps through system disposal (also known as "cradle to grave or "womb to tomb").</p>
Safety Analysis	All associated analysis methods, process, and / or techniques to systematically evaluate safety related risks.
Safety Risk Management Committee (SRMC)	The principal reason to employ risk management and/or risk analysis is to improve decision-making. Risk analysis and risk management is at the heart of many FAA regulatory decisions. For example, risk analysis was performed to determine the hazards to flight from airborne wind shear. Risk management was also evident in the decision to require that all airliners be equipped with airborne wind shear detection. Risk management requires first analyzing risk in turn requiring access to sufficient credible data, and then developing policies and procedures to

CONCEPT or TERM	DESCRIPTION
	<p>eliminate, mitigate, and/or manage them. In keeping with this process, an intra-agency team (the SRMC) was formed to examine the FAA’s approach to risk management. The committee was and remains open to representatives of all FAA organizations interested in risk management.</p> <p>If the RHI ranking criteria use risk as a function of severity and probability, quantitative scales or qualitative scales based on quantitative logic should be used. If the concept that the expected losses (or risk) associated with a hazardous event or condition may be estimated by multiplying the expected severity of the accident by the probability of the accident, then some sort of quantitative basis is necessary. Failure to provide a quantitative basis for the scales can cause significant confusion and dissipation of safety resources when an arbitrary risk ranking scale is used.</p> <p>This committee inventoried existing FAA risk management processes, capabilities, and practices. Processes included types of decisions appropriate for risk management and current technical approaches. Capabilities included personnel skill levels, tools, and access to needed data. Practices include details of implementation and documentation.</p> <p>The SRMC has become a standing committee to serve as a resource for the FAA. It currently: exchanges risk management information between offices and other government agencies to avoid duplication of effort. It provides support across program lines including risk management/analysis training assistance capability. It identifies and recommends needed enhancements to FAA risk management/analysis capabilities and/or efficiencies.</p>
Safety Critical	All interactions, elements, components, subsystems, functions, processes, interfaces, within the system that can affect a predetermined level of risk.
Safety Engineering Report	Documents the results of safety analyses, including Operational Safety Assessments (OSA), Comparative Risk Assessments (CRA), Preliminary Hazard Analyses (PHA), System Hazard Analyses (SHA), Subsystem Hazard Analyses (SSHA), and Operational and Support Hazard Analysis (O&SHA).
Security Risk	<p>Some safety risks that the FAA must manage are the result of security issues. By its nature, the details of methodologies used to analyze and assess security hazards/risks cannot be published in this document. The section does, however, summarize a top-level approach to security risk management, especially as it relates to the methodologies used for safety risk management. Since the development of safety and risk management has not always been parallel, their terminology is sometimes different. Several security unique terms are introduced.</p> <p>Safety and Security hazards are both caused by experiencing a series of events that lead to a questionable condition. In security analyses, the term vulnerability is used to summarize the event path (approach used to achieve negative effect) that leads to the hazard.</p>
Single Point Failure	A single item of hardware, the failure of which would lead directly to loss of life, and / or system. Actually, a single malfunction, and / or failure, and /or error, of which would lead to loss of life, and / or system.

CONCEPT or TERM	DESCRIPTION
Software	Computer programs, procedures, rules, and associated documentation and data pertaining to the operation of a computer system.
Software Code	A software program or routine or set of routines, which were specified, developed and tested for a system configuration.
Structured Programming	Any software development technique that includes structured design and results in the development of structured programs.
Subprogram	A separately compilable, executable component of a computer programs.
Subroutine	A routine that returns control to the program of subprogram that called it.
Subsystem	An element of a system that, in itself, may constitute a system.
Syntax	The structural or grammatical rules that define how the symbols in a language are to be combined to form words, phrases, expressions, and other allowable constructs.
System	<p>A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, requirement; a set of arrangement of components so related or connected as to form a unity or organic whole.</p> <p>A composite of people, procedures, materials, tools, equipment, facilities, and software operating in a specific environment to perform a specific task or achieve a specific purpose, support, or mission requirement.</p>
Systems Approach	A step - by - step procedure for solving problems; a decision making process which moves from the general to the specific; an iterative process.
System Safety	<p>The application of engineering and management principles, criteria, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.</p> <p>A standardized management and engineering discipline that integrates the consideration of man, machine, and environment in planning, designing, testing, operating, and maintaining FAA operations, procedures, and acquisition projects. System safety is applied throughout a system's entire life cycle to achieve an acceptable level of risk within the constraints of operational effectiveness, time, and cost.</p>
System Safety Analysis	The analysis of a complex system by means of methods, techniques, and / or processes, to comprehensively evaluate safety related risks that are associated with the system under study.
System Safety Engineer	<p>An engineer qualified by appropriate credentials: training, education, registration, certification, and / or experience to perform system safety engineering.</p> <p>One should have an appropriate background and credentials directly related to system safety in order to practice in the field, i.e., CSP, PE, training, education, and actual experience.</p>
System Safety Engineering	An engineering discipline requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate, or reduce safety related risks.
System Safety	A formally charted group of persons representing organizations associated with the system

CONCEPT or TERM	DESCRIPTION
Working Group	under study, organized to assist management in achieving the system safety objectives.
System Safety Manager	A person responsible for managing the system safety program.
System Safety Objectives	<p>System safety is achieved through the implementation and careful execution of an SSP. As stated previously, the ultimate objective of system safety is eliminated or minimize accidents and their results. The objectives of an SSP are to ensure that:</p> <ul style="list-style-type: none"> • Safety, consistent with system purpose and program constraints, is designed into the system in a timely, cost-effective manner. • Hazards are identified, evaluated, and eliminated, or the associated risk reduced to a level acceptable to the managing activity (MA) throughout the entire life cycle of a system. • Historical safety data, including lessons learned from other systems, are considered and used. • Minimum risk is sought in accepting and using new designs, materials, and production and test techniques. • Actions taken to eliminate hazards or reduce risk to a level acceptable to the MA are documented. • Retrofit actions are minimized. • Changes in design, configuration, or operational requirements are accomplished in a manner that maintains a risk level acceptable to the MA. • Consideration is given to safety, ease of disposal, and storage of any hazardous materials associated with the system. • Significant safety data are documented as "lessons learned" and are submitted to data banks, design handbooks, or specifications. • Hazards identified after production are minimized consistent with program restraints.
System Safety Order of Precedence.	The overall goal of a system safety program is to design systems that do not contain unacceptable hazards. However, the nature of most complex systems makes it impossible or impractical to design them completely hazard-free. As hazard analyses are performed, hazards will be identified that require resolution. System safety precedence defines the order to be followed for satisfying system safety requirements and reducing the presence and impact of risks. The alternatives for eliminating the specific hazard or controlling its associated risk must be evaluated so that an acceptable method for risk reduction can be pursued.

CONCEPT or TERM	DESCRIPTION
	<p>Design for Minimum Risk. The most effective safety program is one that eliminates hazards through design. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level, as defined by the MA, through design selection. Defining minimum risk is not a simple matter. It is not a cookbook process that can be numerically developed without considerable thought. Minimum risk varies from program to program. See paragraph 3.6 for more information.</p> <p>Incorporate Safety Devices. If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk should be reduced to a level acceptable to the MA through the use of fixed, automatic, or other protective safety design features or devices. Provisions should be made for periodic functional checks of safety devices when applicable.</p> <p>Provide Warning Devices. When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, devices should be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application must be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems.</p> <p>Develop Procedures and Training. Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training should be used. However, without a specific waiver from the MA, no warning, caution, or other form of written advisory shall be used as the only risk reduction method for Category I or II hazards. Procedures may include the use of personal protective equipment.</p>
System Safety Program	The tasks and activities of system safety that enhance effectiveness by ensuring that requirements are met, in a timely, cost-effective manner throughout all phases of the system life cycle.
System Safety Program Plan	A description of the planned methods to be used to implement the system safety requirements.
System Safety Requirements by Acquisition Phase	<p>Concept Exploration</p> <ul style="list-style-type: none"> • Evaluate system safety design features • Identify possible interface problems • Highlight special safety considerations • Describe safety tests/data needed for next phase • Update requirements based on analysis results • Review designs of similar systems • Use past experience with similar system requirements • Identify waiver requirements • Prepare a report for milestone reviews • Tailor subsequent phase SSPs.

CONCEPT or TERM	DESCRIPTION
	<p>Demonstration/Validation</p> <ul style="list-style-type: none"> • SSPP describing contractor's proposed safety program effort • Establish criteria for validating contractor performance • Update specifications, requirements, safety characteristics • PHA for hazards and inherent risks • Safety Interface study for subsystems, e.g., Subsystem Hazard Analysis (SSHA) • Trade-off studies • Identify risks from design, operating environment, and technology • Identify qualification/quantitative system safety requirements • Perform system and equipment interface analyses e.g., System Hazard Analysis (SHA) and Operating and Support Hazard Analysis (O&SHA) • Update test plans • Prepare summary reports for major program milestones • Review test plans • Review training plans • Evaluate hazards and failures for corrective actions • Perform SHA on test model • Identify need for special production and maintenance tools (e.g. barriers) • Review all related maintenance and production instructions • Review applicable safety requirements from FAA, DOT, EPA, and Occupational Safety and Health Administration (OSHA). <p>Full Scale Development</p> <ul style="list-style-type: none"> • Timely implementation of SSPP • Update system safety requirements • Perform hazard analyses. (SHA/O&SHA) • Evaluate system design for hazards and safety improvements • Establish test requirements and ensure verification of design • Participate in design reviews • Provide inputs to training manuals, emergency procedures • Evaluate mishaps/failures and make recommendations • Review/input to trade-off studies • Review drawings/specifications for safety • Identify safety/protective equipment • Provide safety input to training • Ensure designs incorporate safety • Correct hazards identified demonstration/validation phase

CONCEPT or TERM	DESCRIPTION
	<ul style="list-style-type: none"> • Evaluate storage, packing, and handling requirements/plans • Review production plans, drawings, procedures • Review plans for disposal of hazardous materials • Prepare documentation for major milestones • Tailor requirements for production • Review National Airspace Integrated Logistics Support (NAIS) considerations. <p>Production and Deployment</p> <ul style="list-style-type: none"> • Monitor system for adequacy of design safety • Evaluate design changes to prevent degraded inherent safety • Review operations and maintenance publications for safety information • Evaluate accidents; recommended design changes • Review deficiency reports for operators • Review disposal of hazardous materials • Update SSPP • Monitor production line for safety and safety control of system • Review production, maintenance, and operation manuals for necessary cautions, warnings etc. for previously identified hazards • Review system for necessary cautions, warning labels, etc. previously identified (e.g., high voltage) • Verify safety precautions in test and evaluation (T&E) plans and procedures • Identify safety related aging problems and associated controls. • Update O&SHA • Identify critical parts, procedures, facilities, and inspections • Continue to monitor design and procedures to uncover residual hazards; follow-up on corrective action. <p>Facilities-Related Requirements</p> <ul style="list-style-type: none"> • Ensure building, fire, and other related requirements are met • Review facility and installed systems interfaces • Review equipment plans • Update hazard tracking system • Evaluate accidents for deficiencies/oversights/corrective actions • Review design modifications for hazards; monitor corrective actions.
Test Case	A set of test inputs, execution conditions, and expected results developed for a particular objective, such as to test a particular program path or to verify compliance with a specific requirement.
Testing	The process of operating a system under specified conditions, observing or recording the results, and making an evaluation of some aspect of the system.
Test Procedure	(a) Specified way to perform a test.

CONCEPT or TERM	DESCRIPTION
	(b) Detailed instructions for the set-up and execution of a given set of test cases, and instructions for the evaluation of results of executing the test cases.
Traceability	Ability to trace the history, application or location of an entity by means of recorded identifications.
Transient Error	An error that occurs once, or at unpredictable intervals.
Validation	The process of evaluating a system (and subset), during or at the end of the development process to determine whether it satisfies specified requirements. Conformance to requirements is no total assurance of acceptable risk.
Verification	The process of evaluating a system (and subset) to determine whether the products of a given development phase satisfy the conditions imposed at the start of the phase.
Volatile Memory	Memory that requires a continuous supply of power to its internal circuitry to prevent the loss of stored information.
Voting	A scheme in which the outputs of three or more channels of a system implementation are compared with each other in order to determine agreement between two or more channels, and to permit continued operation in the presence of a malfunction in one of the channels. A degree of fault / malfunction tolerance is obtained.
Watchdog Timer	A device that monitors a prescribed operation of computer hardware and / or software and provides an indication when such operation has ceased.
Zero Energy State	<p>All energy within the system has been reduced to the lowest possible energy level, at “zero energy level” if possible. All stored or residual energy, such as within capacitors, springs, elevated devices, rotating flywheels, hydraulic systems, pneumatic systems, have been dissipated.</p> <p>It should be noted that it is not possible to dissipate / de-energize all energy within the system additional controls should be implemented, i.e. lockout, repositioning, isolating, restraining, guarding, shielding, relief, bleed off devices.</p>