Chapter 5: Post-Investment Decision Safety Activities

5.0 Post-Investment Decision Safety Activities

After a program baseline is approved, it transitions to the IPT for Solution Implementation. In this phase, the IPT prepares the necessary documentation to acquire the system. At this point, the IPT has been involved during the IA process, and has prepared the Acquisition Program Baseline, Acquisition Strategy Paper and Integrated Program Plan for approval by the JRC. It is now the team's responsibility to work with the procurement organization to prepare the Request for Proposal and Statement of Work. This chapter defines how to establish a System Safety Program for the acquisition. Chapter 6 defines guidelines for how to manage the contracting activity for a contractor's System Safety Program Plan. It is appropriate to point out that an initial System Safety Program Plan (SSPP) is prepared prior to the Investment Decision and well as one following JRC2, as described in this chapter.

5.1 Objectives and Requirements

The principal objective of an SSP within the FAA is to ensure that safety is consistent with mission requirements and is designed into systems, subsystems, equipment, facilities, and their interfaces and operation. The degree of safety achieved in a system depends directly on management emphasis and commitment. The FAA and its contractors must apply management emphasis to safety during the system acquisition process and throughout the life cycle of each system, ensuring that accident risk is identified and understood, and that risk reduction is always considered in the management review process.

A formal safety program that stresses early hazard identification and elimination or reduction of associated risk to a level acceptable to the managing activity (MA) is not only effective from a safety point of view but is also cost effective.

The FAA SSP is structured on common-sense procedures that have been effective on many programs. These procedures are commonly known as the Safety Order of Precedence as summarized in Table 5-1. These four general procedures are used to establish the following SSP activities:

- Eliminate identified hazards or reduce associated risk through design, including material selection or substitution.
- Design to minimize risk created by human error in the operation and support of the system.
- Protect power sources, controls, and critical components of redundant subsystems by separation, isolation, or shielding.
- When design approaches cannot eliminate a hazard, provide warning and caution notes in assembly, operations, maintenance, and repair instructions, and distinctive markings on hazardous components and materials, equipment, and facilities to ensure personnel and equipment protection. These will be standardized in accordance with MA requirements.

Table 5-1: Safety Order of Precedence

Description	Priority	Definition
Design for minimum risk.	1	From the first design to eliminate risks. If the identified risk cannot be eliminated, reduce it to an acceptable level through design selection.
Incorporate safety devices.	2	If identified risks cannot be eliminated through design selection, reduce the risk via the use of fixed, automatic, or other safety design features or devices. Provisions shall be made for periodic functional checks of safety devices.
Provide warning devices.	3	When neither design nor safety devices can effectively eliminate identified risks or adequately reduce risk, devices shall be used to detect the condition and to produce an adequate warning signal. Warning signals and their application shall be designed to minimize the likelihood of inappropriate human reaction and response.
Develop procedures and training.	4	Where it is impractical to eliminate risks through design selection or specific safety and warning devices, procedures and training are used. However, concurrence of authority is usually required when procedures and training are applied to reduce risks of catastrophic, hazardous, major, or critical severity.

- Design software controlled or monitored functions to minimize initiation of hazardous events or accidents.
- Review design criteria for inadequate or overly restrictive requirements regarding safety.
- Recommend new design criteria supported by study, analyses, or test data.
- Isolate hazardous substances, components, and operations from other activities, personnel, and incompatible materials.
- Locate equipment so that access during operations, servicing, maintenance, repair, or adjustment minimizes personnel exposure to hazards.
- Minimize risk resulting from excessive environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration, and vibration).
- Consider application specific approaches to minimize risk from hazards that cannot be eliminated. Such approaches include interlocks, redundancy, fail-safe design, fire suppression, and protective clothing, equipment, devices, and procedures.
- Minimize the severity of personnel injury or damage to equipment in the event of an accident.

5.1.1 Management Responsibilities

The MA, in order to meet the objectives and requirements of system safety, must conduct the following activities.

- Plan, organize, and implement an effective SSP that is integrated into all life cycle phases.
- Establish definitive SSP requirements for the procurement or development of a system. The requirements must be set forth clearly in the appropriate system specifications and contractual documents.
- Ensure that a System Safety Program Plan (SSPP) is prepared that reflects in detail how the total program is conducted.
- Review and approve for implementation the SSPPs prepared by the contractor.
- Supply historical safety data as available.
- Monitor contractors' system activities and review and approve deliverable data, if applicable, to ensure adequate performance and compliance with system safety requirements.
- Ensure that the appropriate system specifications are updated to reflect results of analyses, tests, and evaluations.
- Evaluate new design criteria for inclusion into FAA specifications and standards, and submit recommendations to the respective responsible organization.
- Establish System Safety Working Groups as appropriate to assist the program manager in developing and implementing an SSP.
- Establish work breakdown structure elements at appropriate levels for system safety management and engineering.

5.1.2 Management Risk Reviews

Management is responsible for reducing the risk of accidents to an acceptable level. The SSP is the vehicle to achieve this objective. Unless there is a dedicated SSP, safety is not a first priority regardless of intentions. Reducing risk is a primary objective of the SSP. The system safety activities assist the program manager in identifying the following:

- Nature of the accident and hazards
- Place of its occurrence
- Alternatives to control risks through design, operations, and procedures
- Implementation and effectiveness of hazard control.
- A properly planned SSP defines and funds the analyses necessary to identify risks throughout the life cycle of the system.

The following is a partial list of safety activities that can help the program manager control safety risks.

- Develop and distribute safety guidance for the entire life cycle of the system (i.e., design, development, production, test, transportation, handling, operation, and maintenance).
- Integrate safety activities into all systems engineering and National Airspace Integrated Logistics Support (NAILS) activities. This integration requires the entire design, manufacturing, test and logistics support teams to identify hazards and implement controls.
- Perform safety analysis in a timely manner.
- Communicate safety requirements and analyses to all subcontractors of safety significant equipment.
- Ensure that safety analysis results are discussed in design and document reviews.
- Execute closed loop procedures to ensure that required safety controls are actually implemented (e.g., warnings in technical manuals and training programs).
- Review historical data for similar applications.
- Demonstrate corrective actions for identified risks.

5.2 Preparing a System Safety Program Plan

An approved System Safety Program Plan (SSPP) is a contractually binding understanding between the FAA and a contractor on how the contractor intends to meet the specified system safety requirements. When there are projects or systems that have multiple subcontractors, an Integrated System Safety Program plan (ISSSPP) should be developed . These plans should describe in detail the contractor's safety organization, schedule, procedures, and plans for fulfilling the contractual system safety obligations. The SSPP is a management vehicle for both the FAA and the contractor. The FAA uses the SSPP approval cycle to ensure that proper management attention, sufficient technical assets, correct analysis and hazard control methodology, and tasks are planned in a correct and timely manner. Once approved, the FAA uses the SSPP to track contractor System Safety Program (SSP) progress. The SSPP is of value to the contractor as a planning and management tool that establishes "before the fact" an agreement with the FAA on how the SSP will be executed and in what depth. In summary, the approved SSPP is an SSP baseline document that minimizes the potential for downstream disagreement of SSP methodology. Figure 5-1 shows the position of the SSPP relative to other parts of the SSP. MIL-STD-882 and the SSMP provide guidance on establishing an SSPP. These documents describe in detail the tasks and activities of system safety management and system safety engineering that are required to identify, evaluate, and eliminate hazards, or reduce the associated risk to a level acceptable to the FAA throughout the system's life cycle.

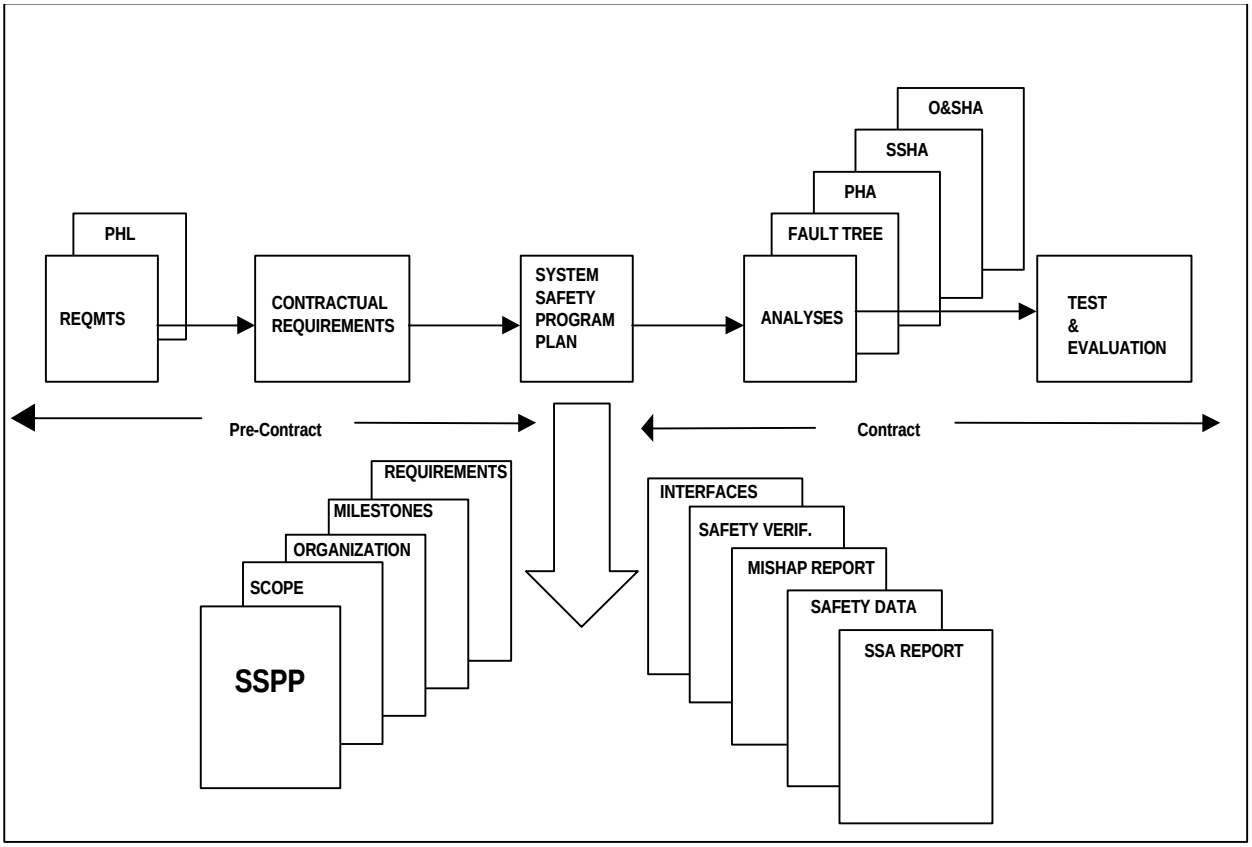


Figure 5-1: System Safety Program Plan

The FAA establishes the contractual requirements for a SSPP in the Statement of Work (SOW). The FAA requires the contractor to establish and maintain an effective and efficient SSP. This is usually the first safety requirement stated in the SOW. SSP requirements are defined by MIL-STD-882, Section 4. They are the only mandatory requirements and cannot be tailored. The System Safety Program Plan purpose is to plan and document the system safety engineering effort necessary to ensure a safe system. The SSPP will:

- Describe the program's implementation of the requirements of MIL-STD-882D, including identification of the hazard analysis and accident risk assessment processes to be used.

- Include information on how system safety will be integrated into the overall system Integrated Product Development System and Integrated Product Team structure in the FAA.
- Define how hazards and residual risk are communicated to the program manager, and how the program manager will formally accept and track the hazards and residual risk.

The SSPP contains the scope, organization, milestones, requirements, safety data, safety verification, accident reporting, and safety program interfaces.

The Statement of Work will normally include the following elements:

- Acceptable level of risk with reporting thresholds*
- Minimum hazard probability and severity reporting thresholds*
- MA requirements for accident reporting
- Requirements for and methodology to the MA for the following:
- Residual hazards/risks
- Safety critical characteristics and features
- Operating, maintenance, and overhaul safety requirements
- Measures used to abate hazards
- Acquisition management of hazardous materials
- Qualifications of key system safety personnel
- Other specific SSP requirements

Note: An asterisk (*) following an item indicates required SOW contents.

The SSPP is usually required to be submitted as a deliverable for MA approval 30 to 45 days after start of the contract. In some situations, the MA may require that a preliminary SSPP be submitted with the proposal to ensure that the contractor has planned and costed an adequate SSP. Since the system safety effort can be the victim of a cost competitive procurement, an approval requirement for the SSPP provides the MA with the necessary control to minimize this possibility.

A good SSPP demonstrates risk control planning through an integrated program management and engineering effort. It is directed towards achieving the specified safety requirements of the SOW and equipment specification. The plan includes details of those methods the contractor uses to implement each system safety task described by the SOW and those safety related documents listed in the contract for compliance (MIL-STD-882, paragraph 6.2). Examples of safety-related documents include Occupational Safety and Health Administration (OSHA) regulations and other national standards, such as the National Fire Protection Association (NFPA). The SSPP lists all requirements and activities required to satisfy the SSP objectives, including all appropriate related tasks. A complete breakdown of system safety tasks, subtasks, and resource allocations for each program element through the term of the contract is also included. A baseline plan is required at the beginning of the first contractual phase (e.g., Demonstration and Validation or Full-Scale Development) and is updated at the beginning of each subsequent phase (e.g., production) to describe the tasks and responsibilities for the follow-on phase.

Plans generated by one contractor are rarely efficient or effective for another. Each plan is unique to the corporate personality and management system. This is important to remember in competitive procurement of a developed or partially developed system. The plan is prepared so that it describes the

system safety approach to be used on a given program at a given contractor's facilities and describes the system safety aspects and interfaces of all appropriate program activities. The contractor's approach to defining the critical tasks leading to system safety certification is included.

The plan should describe an organization featuring a system safety manager who is directly responsible to the program manager or the program manager's agent for system safety. This agent must not be organizationally inhibited from assigning action to any level of program management. The plan further describes methods by which critical safety problems are brought to the attention of program management and for management approval of closeout action. Organizations that show responsibility through lower levels of management are ineffective, and therefore unacceptable.

The SSPP is usually valid for a specific phase of the system life cycle, because separate contracts are awarded as development of equipment proceeds through each phase of the life cycle. For example, a contract award may be for the development of a prototype during the validation phase. A subsequent contract may be awarded to develop pre-production hardware and software during full-scale development, and still another awarded when the equipment enters the production phase. Progressing from one phase of the life cycle to the next, the new contract's SOW should specify that the SSPP prepared for the former contract be revised to satisfy the requirements of the new contract and/or contractor.

5.3 System Safety Program Plan Contents

5.3.1 Program Scope

The SSPP must define a program to satisfy the system safety requirements imposed by the contract. It describes, as a minimum, the four elements of an effective SSP:

- A planned approach for task accomplishment
- Qualified staff to accomplish tasks
- Authority to implement tasks through all levels of management
- Appropriate staffing and funding resources to ensure tasks are completed

Each plan should include a systematic, detailed description of the scope and magnitude of the overall SSP and its tasks. This includes a breakdown of the project by organizational component, safety tasks, subtasks, events, and responsibilities of each organizational element, including resource allocations and the contractor's estimate of the level of effort necessary to effectively accomplish the contractual task. It is helpful to the evaluator if two matrices are included:

- Contractual paragraph compliance mapped to an SSPP.
- Contractual paragraph compliance mapped to those functions within the contractors organization that have the responsibility and have been allocated resources for ensuring that those requirements are met.
- The SSPP should start with a brief section, entitled Scope, that describes the equipment to be covered, the program phase, and the source of the SSP requirements.

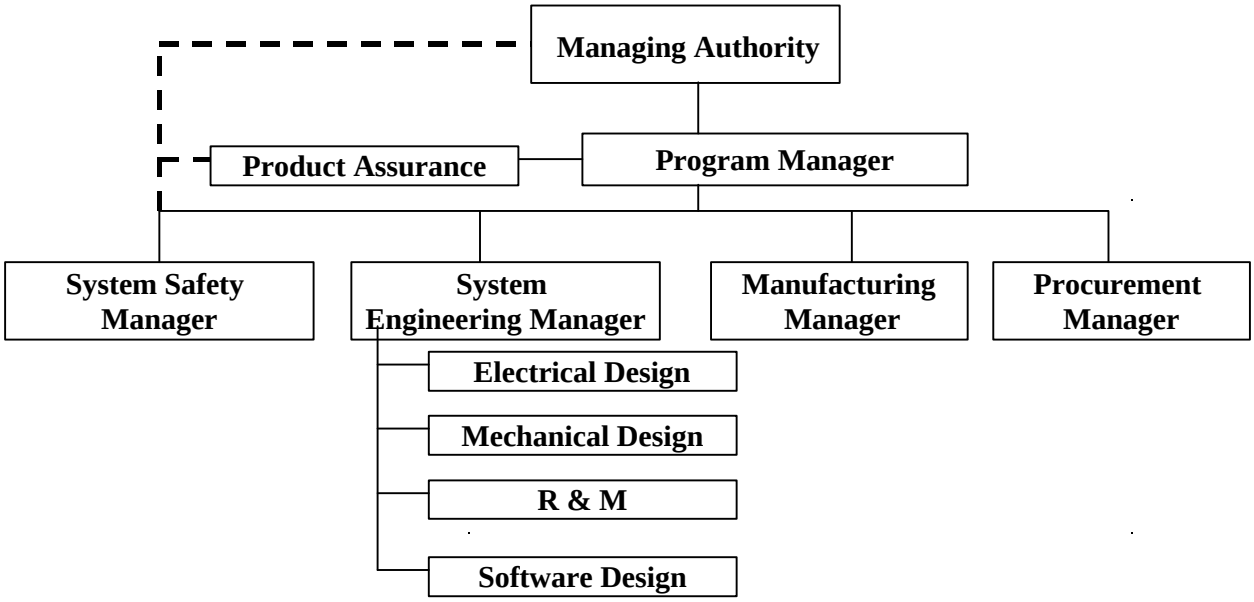
5.3.2 System Safety Organization

The SSPP contains a section that describes the details of Systems Safety Organization. These details are described below.

The system safety organization or function as it relates to the program organization

- The organizational and functional relationships
- Lines of communication.
- The position of the safety organization in a sample program organization (illustrated in Figure 5-2). Note that the system safety manager is at the same reporting level as the managers of design engineering. The organization includes:

  - The contractor's system safety personnel. Internal control for the proper implementation of system safety requirements and criteria affecting hardware, operational resources, and personnel should be the responsibility of the system safety manager through the manager's interface with other program disciplines. The system safety manager should also be responsible for initiation of required action whenever internal coordination of controls fail in the resolution of problems.
  - Other contractor organizational elements involved in the System Safety Working Groups (SSWGs). System safety responsibilities are an inherent part of every program function and task. Examples include reliability and test and evaluation (T&E).



Note: The System Safety manager is a staff function to the Program Manager, with access to all lines of upper management included within the Managing Authority.

Figure 5-2: Sample Safety Organization Chart

Responsibility and authority of all personnel with significant safety interfaces

- The contractor's system safety personnel.
- Internal control for the proper implementation of system safety requirements and criteria affecting hardware, operational resources, and personnel should be the responsibility of the system safety manager through the manager's interface with other program disciplines.
- The system safety manager should also be responsible for initiation of required action whenever internal coordination of controls fail in the resolution of problems.
- Other contractor organizational elements involved in the System Safety Working Groups (SSWGs). System safety responsibilities are an inherent part of every program function and task. Examples include reliability and test and evaluation (T&E).
- The organizational unit responsible for executing each task (e.g. reliability or T&E) and its authority in regard to resolution of all identified hazards. Resolution and action relating to system safety matters may be effective at all organizational levels but must include the organizational level possessing resolution authority (e.g. program or engineering manager). The SSP manager should be identified by name, with address and phone number.

The staffing plan of the system safety organization for the duration of the contract

It should include staff loading, control of resources, and the qualifications of key system safety personnel assigned, including those who possesses coordination/approval authority for contractor prepared documentation.

The procedures by which the contractor will integrate and coordinate the system safety efforts,

including assignment of the system safety requirements to internal organizations and subcontractors, coordination of subcontractor SSPs, integration of hazard analysis, program status reporting, and SSWGs.

The process by which contractor management decisions will be made,

including timely notification of unacceptable risks, necessary action, accidents or malfunctions, waivers to safety requirements, and program deviations.

The contractor must provide a description of a system safety function with a management authority, as the agent of the program manager, to maintain a continual overview of the technical and planning aspects of the total program. Although the specific organizational assignment of this function is a contractor's responsibility, the plan must show a direct accountability to the program manager with unrestricted access to any level of management to be acceptable.

The ultimate responsibility for all decisions relating to the conduct and implementation of the SSP rests with the program director or manager. Each element manager is expected to be fully accountable for the implementation of safety requirements in the respective area of responsibility.

In the usual performance of their duties, SSP managers must have direct approval authority over any safety critical program documentation, design, procedures, or procedural operation. A log of non-deliverable data should be maintained showing all program documentation reviewed, concurrence or non-

concurrence, reasons why the system safety engineer concurs or non-concurs, and actions taken as a result of non-concurrence. The MA should assess activity and progress by reviewing this log.

For major programs, the staffing forecast can be provided at the significant safety task level.

The contractor is required to assign a system safety manager who meets specific educational and professional requirements and who has had significant assignments in the professional practice of safety. Qualifications should reflect the system's criticality and SSP magnitude. Application of common sense is necessary. Clearly, the safety manager for an airframe program requires different credentials than one responsible for an avionics program. For major programs, a range of six to nine years of system safety experience is required. In some cases, it is justifiable to require either a registered Professional Engineer (PE) or a board Certified Safety Professional

In other cases, work experience may be substituted for educational requirements. Small programs or organizations may have limited access to personnel with full time safety experience, and the MA should be confident that such credentials are necessary for the specific application before invoking them.

The minimum qualifications for the systems safety manager or staff should be included in the contract. This may be difficult: The existence of a CSP is a rarity at electronic development and manufacturing companies. If a CSP is required, the contractor is likely to hire a part-time CSP consultant, a questionable approach. PEs are more common, but few have careers involving safety. Appendix A in MIL-STD-882 provides a table of minimum qualifications for programs based upon complexity and demands on CSP or PE qualifications. This approach ignores the hazard severity of the system.

Table 5-2 is suggested as a qualification baseline. It is not absolute and is offered only as guidance. The MA may adjust these qualifications, as appropriate.

5.3.3 Program Milestones

To be effective, the system safety activities on any program must be integrated into other program activities. To be efficient, each SSP task must be carefully scheduled to have the most positive effect. A safety analysis performed early in the design process can lead to the inexpensive elimination of a hazard through design changes. The later the hazard is identified in the design cycle, the more expensive and difficult the change. Hazards identified in T&E production, or following deployment may be impractical to change. In such cases, hazards may still be controlled through procedural and training steps but having to do so, when they could have been prevented, reflects unnecessary long-term costs and risk.

Table 5-2: Key Personnel Systems Safety Qualifications

Program Complexity	Program Severity	Education	Experience	Certification
High	Catastrophic	BS in Engineering or applicable other	Six years in system safety	CSP or PE desired; equivalent 10 yrs experience
High	Critical	BS in Engineering or applicable other	Six years in system safety or related discipline	CSP or PE desired; equivalent 10 yrs experience
High	Marginal	BS in Engineering or applicable other	Two years in system safety or related discipline	CSP or PE desired; equivalent 10 yrs experience
Moderate	Catastrophic	BS in Engineering or applicable other	Four years in system safety	CSP or PE desired; equiv. 10 yrs experience
Moderate	Critical	BS in Engineering or applicable other	Four years in system safety or related discipline	None
Moderate	Marginal	BS plus training in system safety	Two years in system safety or related discipline	None
Low	Catastrophic	BS plus training in system safety	Four years in system safety or related discipline	None
Low	Critical	BS plus training in system safety	Two years in system safety or related discipline	None
Low	Marginal	High School Diploma plus training in system safety	Two years in system safety or related discipline	None

A SSPP prepared in accordance with MIL-STD-882 provides the FAA with an opportunity to review the contractor's scheduling of safety tasks in a timely fashion, permitting corrective action when applicable. MIL-STD-882 guides the contractor to plan and organize the system safety effort and provides the MA with necessary information for FAA support planning by requiring the elements listed below. Requirements to be adjusted for program, as necessary.

SSP milestones
Program schedule of safety tasks including start and completion dates, reports, reviews, and estimated staff loading
Identification of integrated system safety activities (e.g., design analysis, tests, and demonstration) applicable to the SSP but specified in other engineering studies to preclude duplication. (See Chapter 6, System Safety Integration and Risk Assessment)

The SSPP must provide the timing and interrelationships of system safety tasks relative to other program tasks. A suitable program milestone section of an SSPP will include a Gantt chart showing each significant SSP task, the period of performance for each, and related overall program milestones. For example, one expects the establishment of design criteria and the generation of the SSPP to begin almost immediately during any design phase; analyses to run concurrent to design activities and have at least interim completions prior to major design reviews; and the establishment of hazard tracking systems prior to a significant testing. Figure 5-3 shows an example of a Gantt chart.

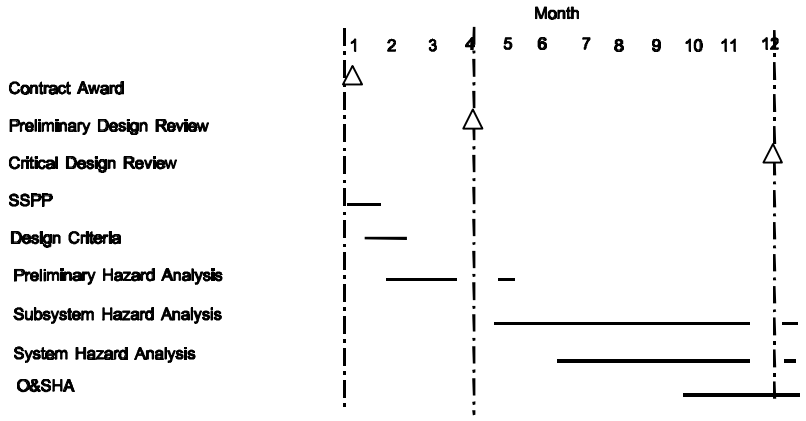


Figure 5-3: Sample SSPP Gantt Chart

The schedule for each SSP task in the SSPP should be tied to a major milestone (e.g., start 30 days after or before the preliminary design review [PDR]) rather than a specific date, as MIL-STD-882 requires. In this manner, the SSPP does not need revision whenever the master program schedule shifts. The same MA control is maintained through the program master schedule but without the associated cost of documented revision or schedule date waiver.

5.3.4 Requirements and Criteria

A formally submitted SSPP provides the opportunity for the MA and the contractor to clearly reach the same understanding of technical and procedural requirements and plans before precious assets are expended. MIL-STD-882D Appendix A, provides guidance on the type of information be included in the SSPP. The inclusion of this information expedites reaching a common understanding between the MA and the contractor. This information includes the following.

Safety Performance Requirements

These are the general safety requirements needed to meet the core program objectives. The more closely; these requirements relate to a given program, the more easily the designers can incorporate them into the system. In the appropriate system specifications, incorporate the safety performance requirements that are applicable, and the specific risk levels considered acceptable for the system. Acceptable risk levels can be defined in terms of: a hazard category developed through a accident risk assessment matrix, an overall system accident rate, demonstration of controls required to preclude unacceptable conditions; satisfaction of specified standards and regulatory requirements; or other suitable accident risk assessment procedures. Listed below are some examples of how safety performance requirements could be stated.

Quantitative requirements. – usually expressed as a failure or accident rate, such as " the Catastrophic system accident rate shall not exceed x.xx X 10^{-Y} per operational hour."
Accident risk requirements – could be expressed as " No hazards assigned a Catastrophic accident severity are acceptable." Accident risk requirements could also be expressed as a level defined by the accident risk assessment matrix. (see Chapter x. yy) such as "No Category 3 or higher accident risks are acceptable."
Standardization requirements – are expressed relative to a known standard that is relevant to the system being developed. Examples include: The system will comply with the Federal Code of Regulations CFR-XXX, or "The system will comply with international standards developed by ICAO."

Safety Design Requirements

The program manager, in concert with the chief engineer and utilizing system engineering and associated system safety professionals, should establish specific safety design requirements for the overall system. The objective of safety design requirements is to achieve acceptable accident risk through a systematic application of design guidance from standards, specifications, regulations, design handbooks, safety design checklists, and other sources. These are reviewed for safety parameters and acceptance criteria applicable to the system. Safety design requirements derived from the selected parameters, as well as any associated acceptance criteria, are included in the system specification. These requirements and criteria are expanded for inclusion in the associated follow-on or lower level specifications.

A composite list of all SSP requirements is included in the requirements and criteria section of the SSPP for several reasons. The list includes the following.

Organization and integration of safety requirements establishing clear SSP objectives. Frequently, safety requirements are included at multiple levels in a variety of specifications. Assembling a safety requirements composite list can be time consuming and, therefore, generating and formally documenting this list can expect to save significant staff labor costs and likely omissions by those without significant system safety experience.

Providing MA assurance that no safety requirements have been missed and that the safety requirements have been interpreted correctly.

Documentation

The inclusion of a description of risk assessment procedures, and safety precedence is an important example of where the SSPP contributes to the MA and the contractor reaching a common understanding. Without such details explicitly described in the SSPP, both the MA and contractor could, in good faith, proceed down different paths until they discover the difference of interpretation at a major program milestone.

The hazard analyses described in Chapters 8 & 9 illustrate some methodologies used to identify risks, and assign severity and criticality criteria. Safety precedence is a method of controlling specific unacceptable hazards. A closed loop procedure is required to ensure that identified unacceptable risks are resolved in a documented disciplined manner. The inclusion of such procedures demonstrates both necessary control and personnel independence.

The presence of the safety criteria in the SSPP is an important step in the system safety management process. This information must flow down to the system and design engineers (including appropriate subcontractors). SSPP must provide a procedure that incorporates system safety requirements and criteria in all safety critical item (CI) specifications. Such safety requirements include both specific design and verification elements.

Unambiguous communication between the FAA and the contractor depends on standardized definitions. The FAA may choose for expediency, to invoke a MIL-STD-882 SSP. It must be noted that the definitions included in MIL-STD-882 are not identical to those used in the FAA community. Therefore, the SOW should indicate that the definitions in this handbook (or other FAA documents) supersede those in MIL-STD-882, see Glossary for examples.

5.3.5 Hazard Analyses

The SSPP describes the specific analyses to be performed during the SSP. The following characteristics of those analyses should be included.

The analysis techniques and formats to be used in the qualitative or quantitative analysis to identify risks, their hazards and effects, hazard elimination, or risk reduction requirements, and how these requirements are met.
The depth within the system to which each technique is used, including risk identification associated with the system, subsystem, components, personnel, ground support equipment, GFE, facilities, and their interrelationship in the logistic support, training, maintenance, and operational environments.
The integration of subcontractor hazard analyses with overall system hazard analyses.
Analysis is the method of identifying hazards. A sound analytical and documentation approach is required if the end product is to be useful. An inappropriate analytical approach can be identified in the contractor's discussion within the SSPP.

Each program is required to assess the risk of accident in the design concept as it relates to injury to personnel, damage to equipment, or any other forms of harm. The result of this assessment is a definition of those factors and conditions that present unacceptable accident/accident risk throughout the program. This definition provides a program baseline for formulation of design criteria and assessment of the adequacy of its application through systems analysis, design reviews, and operational analysis. System

safety analyses are accomplished by various methods. As noted in Chapters 8&9 of this handbook, the basic safety philosophy and design goals must be established prior to initiation of any program analysis task. Without this advanced planning, the SSP becomes a random identification of hazards resulting in operational warnings and cautions instead of design correction (i.e., temporary, not permanent solutions)

The SSPP, therefore, describes the methods to be used to perform system safety analyses. The methods may be quantitative or qualitative, inductive or deductive, but must produce results consistent with mission goals.

It is important that the SSP describes procedures that will initiate design change or safety trade studies when safety analyses indicate such action is necessary. Specific criteria or safety philosophy guides trade studies or design changes. Whenever a management decision is necessary, an assessment of the risk is presented so that all facts can be considered for a proposed decision. It is common to find budget considerations driving the design without proper risk assessment. Without safety representation, design decisions may be made primarily to reduce short-term costs increasing the accident risk. Such a decision ignores the economics of an accident. In many cases accident and accident costs far exceed the short-term savings achieved through this process.

The contractor's system safety engineers should be involved in all trade-studies. The SSPP must identify the responsible activity charged with generating CRAs, and with reviewing and approving the results of trade-studies to assure that the intent of the original design criteria is met.

The hazard analysis section of the SSPP should describe in detail, the activities which will identify the impact of changes and modifications to the accident potential of delivered and other existing systems. All changes or modifications to existing systems must be analyzed for impact in the safety risk baseline established by the basic system safety analysis effort. In many cases, this analysis can be very limited where in others a substantial effort is appropriate. The results must be included for review as a part of each engineering change proposal.

5.3.6 Safety Data

The SSPP should illustrate the basic data flow path used by the contractor. This information shows where the system safety activity includes reviewing internally generated data and where it has approval authority. The safety data paragraph should list system safety tasks, contract data requirements list (CDRL) having safety significance but no specific safety reference, and the requirement for a contractor system safety data file. The data in the file is not deliverable but is to be made available for the procuring activity review on request.

5.3.7 Safety Verification

Safety verification must be demonstrated by implementing a dedicated safety verification test and/or assessment program. The following information should be included in the SSPP.

- The verification (e.g., test, analysis, inspection) requirements for ensuring that safety is adequately demonstrated. Identify any certification requirements for safety devices (e.g., fire extinguisher, circuit breakers) or other special safety features (e.g., interlocks). Note that

some certification requirements will be identified as the design develops so the SSPP should contain procedures for identifying and documenting these requirements.

- Procedures for making sure test information is transmitted to the MA for review and analysis.
- Procedures for ensuring the safe conduct of all tests.

The FAA System Engineering Manual may be consulted for further information on verification and validation.

5.3.8 Audit Program

The contractor's SSPP should describe the techniques and procedures to be used in ensuring the accomplishment of the internal and subcontractor SSPs. Specific elements of an audit program by the prime contractor should include the following:

- On-site inspection of subcontractors.
- Major vendors, when appropriate.
- An accurate staff-hour accounting system.
- Hazard traceability.

5.3.9 Training

This portion of the SSPP contains the contractor's plan for using the results of SSP in various training areas. Often hazards that relate to training are identified in the Safety Engineering Report (SER) or in the System Engineering Design Analysis Report. Procedures should provide for transmitting this information to any activity preparing training plans. The specifics involved in safety training may be found in Chapter 14.

The SSP will produce results that should be applied in training operator, maintenance, and test personnel. This training should not only be continuous but also conducted both formally and informally as the program progresses. The SSPP should also address training devices.

5.3.10 Accident/Incident Reporting

The contractor should be required to notify the MA immediately in case of an accident. The SSPP must include details and timing of the notification process.

The SSPP should also define the time and circumstances under which the MA assumes primary responsibility for accident and incident investigation. The support provided by the contractor to government investigators should be addressed. The procedures by which the MA will be notified of the results of contractor accident investigations should be spelled out. Provisions should be made for a government observer to be present for contractor investigations.

Any incident that could have affected the system should be evaluated from a system safety point of view. An incident in this case is any unplanned occurrence that could have resulted in an accident. Incidents involve the actions associated with hazards, both unsafe acts or unsafe conditions that could have resulted in harm. Participants within the system safety program should be trained in the identification of

incidents; this involves a concept called behavioral-based safety, which is discussed in Chapter 12, Facilities System Safety.

5.3.11 Interfaces

Since conducting an SSP will eventually affect almost every other element of a system development program, a concerted effort must be made to effectively integrate support activities. Each engineering and management discipline often pursues its own objectives independently, or at best, in coordination only with mainstream program activities such as design engineering and testing.

To ensure that the SSP is comprehensive, the contractor must impose requirements on subcontractors and suppliers that are consistent with and contribute to the overall SSP. This part of the SSPP must show the contractor's procedures for accomplishing this task. The prime contractor must evaluate variations and specify clear requirements tailored to the needs of the SSP. Occasionally, the MA procures subsystems or components under separate contracts to be integrated into the overall system. Subcontracted subsystems that impact safety should be required to implement an SSP.

The integration of these programs into the overall SSP is usually the responsibility of the prime contractor for the overall system. When the prime contractor is to be responsible for this integration, the Request for Proposal (RFP) must specifically state the requirement. This subparagraph of the SSPP should indicate how the prime contractor plans to effect this integration and what procedures will be followed in the event of a conflict.

The MA system safety manager should be aware that the prime contractor is not always responsible for the integration of the SSP. For example, in some SSPs, the MA is the SSP integrator for several associate contractors. The next section of this chapter contains guidance specific to the management of a complex program with multiple subcontractors requiring an Integrated System Safety Program Plan.

5.4 Integrated System Safety Program Plan

The tasks and activities of system safety management and engineering are defined in the System Safety Program Plan, (SSPP). An Integrated System Safety Program Plan (ISSPP) is modeled on the elements of an SSPP, which is defined in Mil-Std 882C.[1] An ISSPP is required when there are large projects or large systems; the system safety activities should be logically integrated. Other participants, tasks, operations, or sub-systems within a complex project should also be incorporated.

The first step is to develop a plan that is specifically designed to suit the particular project, process, operation, or system. An ISSPP should be developed for each unique complex entity such as a particular line-of -business, project, system, development, research task, or test. Consider a complex entity that is comprised of many parts, tasks, subsystems, operations, or functions and all of these sub-parts should be combined logically. This is the process of integration. All the major elements of the ISSPP should be integrated. How this is accomplished is explained in the following paragraphs.

5.4.1 Integrated Plan

The Program Manager, Prime Contractor, or Integrator develops the Integrated System Safety Program Plan. The Plan includes appropriate integrated system safety tasks and activities to be conducted within

[1] Military Standard 882C, explains and defines System Safety Program Requirements, Military Standard 882D is a current update as of 1999. This version no longer provides the details that version C had provided.

the project. It includes integrated efforts of management, team members, subcontractors and all other participants.

5.4.2 Integrated Program Scope and Objectives

The extent of the project, program, and system safety efforts is defined under scope. The system safety efforts should be in-line with the project or program. Boundaries are defined as to what may be excluded or included within the ISSPP.

The objective is to establish a management integrator to assure that coordination occurs between the many entities that are involved in system safety. The tasks and activities associated with integration management are defined in the document. The ISSPP becomes a model for all other programs within the effort. Other participants, partners, sub-contractors are to submit plans which are to be approved and accepted by the integrator. The Plans then become part of the ISSPP.

5.4.3 Integrated System Safety Organization

The integrated system safety organization is detailed within the plan. The duties and responsibilities are defined for the System Safety Integration Manager and staff. Each sub-entity such as a partner, or sub-contractor, should appoint a manager or senior system safety engineer or lead safety engineer that will manage the entity's SSPP. All appropriate system safety participants are to be given specific responsibilities. The participants should have specific qualifications in system safety, which include a combination of experience and education.

5.4.4 Integrated System Safety Working Group

A System Safety Working Group (SSWG) is formed to help manage and conduct tasks associated with the program. The group specifically provides a consensus entity that enhances work performed. The SSWG is a major part of the SSPP.

For large or complex efforts where an ISSPP has been established, activities of the Integrated System Safety Working Group (ISSWG) are defined in the ISSPP. The ISSWG includes responsive personnel who are involved in the system safety process. The plan specifically indicates that, for example, Operations, System Engineering, Test Engineering, Software Engineering, and System Safety Engineering personnel are active participants in the ISSWG. The integrator may act as the chair of the ISSWG with key system safety participants from each sub-entity. The group may meet formally on a particular schedule. Activities are documented in meeting minutes. Participants are assigned actions.

The ISSWG activities may include:

- Monitoring interface activities to assure that system safety is adequately integrated.
- Reviewing or conducting activities, analysis, assessments, and studies, appropriate to system safety.
- Conducting hazard tracking and risk resolution activities.
- Conducting formal safety reviews.

5.4.5 Integrated Program Milestones

The Integrated System Safety Process Schedule is defined within the ISSPP. The schedule indicates specific events and activities along with program milestones. To accomplish the integration specific

system analysis techniques have evolved. One example is the use of Program Evaluation Review Technique (PERT).[2] It is essentially the presentation of system safety tasks, events and activities on a network in sequential and dependency format showing independencies, and task duration and completion time estimates. Critical paths are easily identifiable. Its advantage is the greater control provided over complex development and production programs as well as the capacity for distilling large amounts of scheduling data in brief, orderly fashion. Management decisions are implemented. Needed actions may be more clearly seen, such s steps to conduct a specific test.

A similar or sub-technique of PERT is known as Critical Path Method (CPM).[3] It also involves the identification of all needed steps from a decision to a desired conclusion --depicted systematically –to determine the most time-consuming path through a network. This is designated on the diagram as the "critical path". The steps along the path are "critical activities".

Because of the dynamics and the variability of safety management efforts, the networks developed should suit the complexity required. For large programs a master PERT network can be developed with lower level PERT charts referenced to provide needed detail. The use of CPM, in conjunction with PERT, can explore possible variables that influence programs.[4] Further detail on PERT and CPM can be acquired from the references.

5.4.6 Integrated System Safety Requirements

The integrated engineering requirements for system safety are described within the ISSPP. As the design and analysis matures specific system safety standards and system specifications are to be developed and the ISSPP is to be updated. Initially, generic requirements are defined for the design, implementation, and application of system safety within the specific project, or process. The Integrator defines the requirements needed to accomplish the objectives of the ISSPP. Here one specifies the system safety products to be produced, the risk assessment code matrix, risk acceptability criteria, and residual risk acceptance procedures. This effort should also include guidelines for establishing project phases, review points, and levels of review and approval.[5]

5.4.7 Integrated Risk/Hazard Tracking and Risk Resolution

Integrated Risk/Hazard Tracking and Risk Resolution is described within the ISSPP. This is a procedure to document and track contributory system risks and their associated controls by providing an audit trail of risk resolution. The controls are to be formally verified and validated and the associated contributory

[2] J.V. Grimaldi and R.H. Simonds, Safety Management, Richard D. Irwin, Inc. Homewood, Illinois, Third Edition, 1975.
[3] IBID, Grimaldi
[4] System Safety Society, System Safety Analysis Handbook, 2nd Edition, 1997.
[5] J. Stephenson, System Safety 2000, A Practical Guide for Planning, Managing, and Conducting System Safety Programs, Van Nostrand Reinhold, New York, 1991.

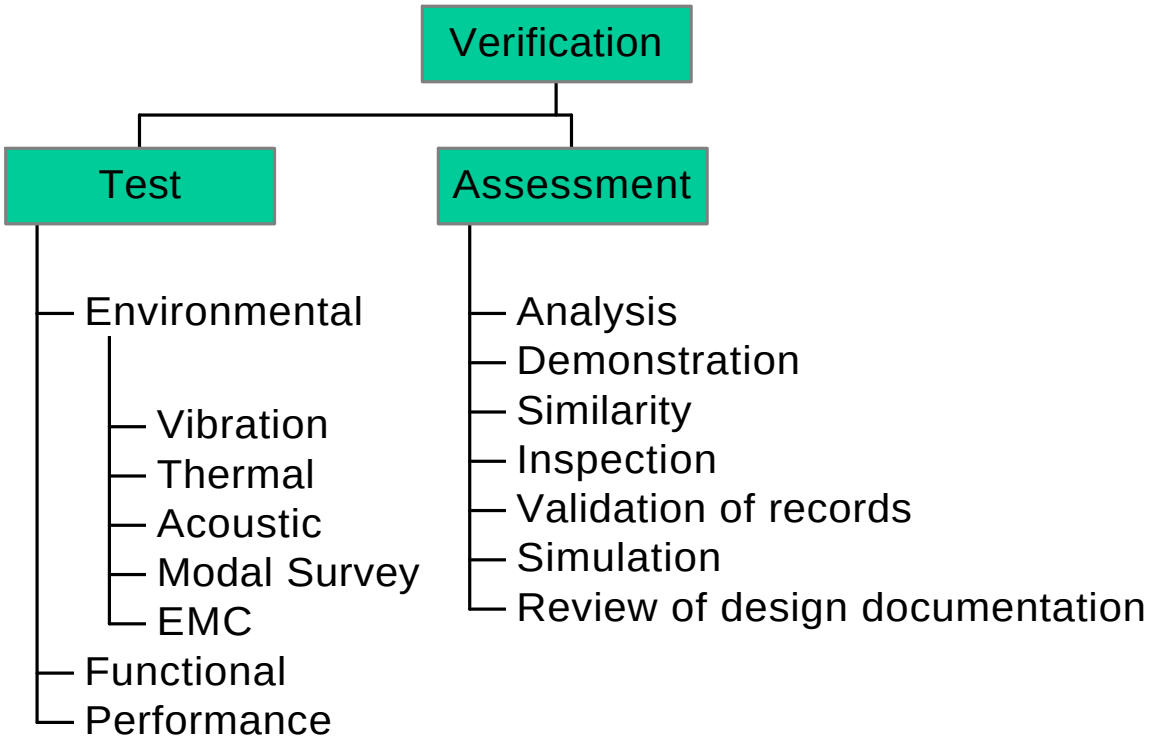


Figure 5-4: Safety Verification Methods

hazard is to be closed. This activity is conducted and/or reviewed during ISSWG meetings or formal safety reviews.

Integrated Risk/Hazard Tracking and Risk Resolution is accomplished by the use of the Safety Action Record (SAR). The SAR document captures the appropriate elements of hazard analysis, risk assessment and related studies, conducted in support of system safety. See Chapter 2 for a discussion of the Hazard Tracking/Risk Resolution process (Paragraph 2.2.1.5)

5.4.8 Integrated Safety Verification and Validation

Specific verification techniques are discussed within the ISSPP. Safety verification is needed to assure that system safety is adequately demonstrated and that all identified system risks that have not been eliminated are controlled. Risk controls (mitigation) must be formally verified as being implemented. Safety verification is accomplished by the methods shown in Figure 5-4.

It should be noted that no single method of verification indicated above provides total system safety assurance. Safety verification is conducted in support of the closed-loop hazard tracking and risk resolution process.

Hazard Control Analysis considers the possibility of insufficient control of the system. Controls are to be evaluated for effectiveness. They are to enhance the design. Keep in mind that system safety efforts are

not to cause harm to the system. Consider that any change to a system must be evaluated from a system risk viewpoint. For more information regarding verification and validation see the FAA System Engineering Manual.

5.4.9 Integrated Audit Program

The ISSPP should call for the Quality Assurance function to audit the program. All activities in support of system safety are to be audited. This includes contractor internal efforts and all external activities in support of closed-loop Hazard Tracking and Risk Resolution. The government will be given access to audit data.

5.4.10 Integrated Training

When required, ISSPP participants are to receive specific training in system safety in order to conduct analysis, hazard tracking and risk resolution. Additional training is to be provided for ISSWG members and program auditors to assure awareness of the system safety concepts discussed herein.

Specific training is to be conducted for system users, controllers, systems engineers, and technicians. Training considers normal operations with standard operating procedures, maintenance with appropriate precautions, test and simulation training, and contingency response. Specific hazard control procedures will be recommended as a result of analysis efforts. See Chapter 14 for more information on System Safety training.

5.4.11 Integrated Incident Reporting and Investigation

Any incident, accident, malfunction, or failure effecting system safety is to be investigated to determine causes and to enhance analysis efforts. As a result of investigation, causes are to be determined and eliminated. Testing and certification activities are also to be monitored; anomalies, malfunctions, failures that affect system safety are to be corrected.

Concepts of system safety integration are also applied systematically through formal accident investigation techniques. Many systematic techniques have been successfully applied for example[6]: Scenario Analysis (SA), Sequentially Timed Events Plot (STEP), Root Cause Analysis (RCA), Energy Trace Barrier Analysis (ETBA), Management Oversight and Risk Tree (MORT), and Project Evaluation Tree (PET).[7] For further details consult the references provided. Consider that hazard analysis is the inverse of accident investigation and similar techniques are applied in the application of inductive and deductive processes of hazard analysis and accident investigation.

5.4.12 System Safety Interfaces

System Safety interfaces with other applicable disciplines both internally to systems engineering and externally. System Safety is involved in all Program disciplines, i.e., Risk Management, Facilities, Software Development, Certification, Testing, Contract Administration, Health Management, Environmental Management, Ergonomics, Human Factors, as examples. These disciplines may be directly involved in the hazard analysis, hazard control, hazard tracking, and risk resolution activities.

[6] IBID, System safety Society
[7] IBID, Stephenson

5.4.13 Integrated Inputs to the ISSPP

The external inputs to the system safety process are the design concepts of the system, formal documents, engineering notebooks, and design discussions during formal meetings and informal communications. The on-going output of the system safety process is hazard analysis, risk assessment, risk mitigation, risk management, and optimized safety.

Inputs:

- Concept of Operations
- Requirements Document
- System/Subsystem Specification
- Management and System Engineering Plans, (e.g. Master Test Plan)
- Design details

Outputs: Hazard Analysis consists of

- Identifying safety related risks (contributory hazards) throughout system life cycle
- Conducting system hazard analysis evaluating human, hardware, software, and environmental exposures
- Identifying and incorporating hazard (risk) controls
- Risk Assessment involves:
- Defining risk criteria i.e., severity and likelihood
- Conducting risk assessment i.e., Risk Acceptability and Ranking
- Risk Management consists of:
- Conducting Hazard Tracking and Risk Resolution
- Optimize safety (assure acceptable safety related risks)
- Monitoring controls

5.5 Program Balance

The purpose of an SSP is to eliminate or reduce risk of a accident to an acceptable level within the available program assets. The system safety activity, like all other systems engineering functions, is sized through a trade-off between cost, schedule, and performance. The sizing of an SSP must find a balance between acceptable risk and affordable cost. Neither a system with unacceptable accident risk nor one that cannot be procured because of the costs of achieving unreasonable safety goals is acceptable.

5.6 Program Interfaces

Both the nature of safety objectives and economics require the use of information available through other engineering disciplines. The capability of the safety engineering staff can be greatly increased through integration with other engineering disciplines. System Safety integration and risk assessment have been discussed in earlier sections of this Chapter. For a summary of other organizations that need to be involved in system safety, see Table 5-4.

Design engineers are key players in the system safety effort. Together with systems engineers, they translate user requirements into system design and are required to optimize many conflicting constraints. In doing this, they eliminate or mitigate known hazards but may create unidentified new hazards. System safety provides design engineers with safety requirements, validation and verification requirements, and

advice and knowledge based on the SSP's interfacing with the many participants in the design and acquisition processes.

On a typical program, safety engineers interface with a number of other disciplines as reflected in Table 5-3. In most cases, the frequency of interfacing with these other disciplines is less than that with the design engineers. Nevertheless, the exchange of data between safety engineering and the program functions is both important and in some cases mutually beneficial.

Reliability engineers, for example, perform analyses usable by and often without additional cost to safety engineering. These analyses do not supplant safety-directed analyses. They provide data that improve the quality and efficiency of the safety analysis process. Three types of reliability analyses are reliability models, failure rate predictions, and Failure Modes and Effects Criticality Analysis (FMECA).

The safety/maintainability engineering interface is an example of providing mutual benefits. The system safety program analyzes critical maintenance tasks and procedures. Hazards are identified, evaluated, and appropriate controls employed to minimize risk. Maintainability analyses, on the other hand, provide inputs to the hazard analyses, particularly the Operational and Support Hazard Analyses (O&SHA).

Table 5-3: Other Engineering Organizations Involved in Safety Programs

ORGANIZATION	NORMAL FUNCTIONS	SAFETY FUNCTIONS
Design Engineering	Design equipment and system to meet contractual specifications for mission	Analyses safest designs and procedures. Ensures that safety requirements in end product item specifications and codes are met. Incorporates safety requirements for subcontractors and vendors in specifications and drawings.
Human (Factors) Engineering	Ensures optimal integration of human, machine, and environment.	Analyses human machine interface for operation, maintenance, repair, testing, and other proposed tasks to minimize human error, provide safe operating conditions, and to prevent fatigue. Makes procedural analysis.
Reliability Engineering	Ensures equipment will operate successfully for specific periods under stipulated conditions.	Performs failure modes and effects criticality analysis (FMECA) and failure rate predictions quantifying probability of failure. Performs tests, as necessary, to supplement analytical data. Reviews trouble and failure reports for safety connotations.
Maintainability Engineering	Ensures hardware status and availability.	Ensures that operating status can be determined, minimizes wearout failures through preventative maintenance, and provides safe maintenance access and procedures. Participates in analyzing proposed maintenance procedures and equipment for safety aspects.
Test Engineering	Conducts laboratory and field tests of parts, subassemblies, equipment, and systems to determine whether their performance meets contractual requirements.	Evaluates hardware and procedures to determine whether they are safe in operation, whether additional safeguards are necessary. Determines whether equipment has any dangerous characteristics or has dangerous energy levels or failure modes. Evaluates effects of adverse environments on safety.
Product (Field) Support	Maintains liaison between customer and producing company.	Assists customer on safety problems encountered in the field. Constitutes the major channel for feedback of field information on performance, hazards, accidents, and near misses.
Production Engineering	Determines most economical and best means of producing the product in accordance with approved designs.	Ensures that designed safety is not degraded by poor workmanship and unauthorized production process changes.
Industrial Safety	Ensures that company personnel are not injured nor company property damaged by accidents.	Provides advice/information on accident prevention for industrial processes and procedures.
Training	Improves technical and managerial capabilities of company and user personnel.	Ensures that personnel involved in system development, production, and operation are trained to the levels necessary for safe accomplishment of their tasks.

Close cooperation between system safety and quality assurance (QA) benefits both functions in several ways. QA should incorporate, in its policies and procedures, methods to identify and control critical items throughout the life cycle of a system. The safety function flags safety-critical items and procedures. QA then can track safety-critical items through manufacturing, acceptance tests, transportation, and maintenance. New or inadequately controlled hazards can then be called to the attention of the safety engineer.

Human engineering (HE) and safety engineering are often concerned with similar issues and related methodologies, (See Chapter 17, Human Factors Safety Principles). HE analyzes identified physiological and psychological capabilities and limitations of all human interfaces. A variety of human factors inputs affect the way safety-critical items and tasks impact the production, employment, and maintenance of a system. Environmental factors that affect the human-machine interface are also investigated and safety issues identified.

The safety/testing interface is often underestimated. Testing can be physically dangerous. The safety and test engineers must work together to minimize safety risk. Testing is a vital part of the verification process and must be included in a comprehensive SSP. It verifies the accomplishment of safety requirements. Testing may involve:

- Components
- Mock-ups
- Simulations in a laboratory environment
- Development and operation test and evaluation efforts.

System safety may require special tests of safety requirements or analyze results from other tests for safety verification.

The requirements for interface between safety and product support are similar to those involving safety and manufacturing. Each examines personnel and manpower factors of design. System safety ensures that these areas address concerns related to identified hazards and the procedures. Operational, maintenance, and training hazard implication are passed on to the user as a result of the design and procedural process.

5.7 Tailoring

An effective SSP is tailored to the particular product acquisition. The FAA's policy is to tailor each SSP to be compatible with SSMP, the criticality of the system, the size of the acquisition, and the program phase of that system's life cycle. The resultant safety program becomes a contractual requirement placed upon system contractors and subcontractors.

Readily adaptable to the FAA's mission, MIL-STD-882D was created to provide a standardized means for establishing or continuing SSPs of varying sizes at each phase of system development. The SSMP along with Mil-Std-882 contains a list of tasks from which the FAA program manager may tailor an effective SSP to meet a specific set of requirements. Each task purpose is stated at the beginning of each task description. Fully understanding these purposes is critical before attempting to tailor an SSP. There are three general categories of programs: Low Risk, Moderate Risk, and High Risk.

Selecting the appropriate category is difficult and in practice depends on some factors difficult to quantify, particularly in the early phases of a program. Therefore, this decision should be reviewed at each phase of the program, permitting the best information available to direct the magnitude of the safety program. The following steps applied to the risk methodology in Chapter 3 illustrate the technique used for the program risk decision process.

- Generate a CRA (and PHA if needed) in the IA phase. These analyses will provide the types and risks of hazards. The development of an airframe and that of a ground communications system could both produce a system that can lead to death, a Severity 1 or 2 hazard. A development program that is far more complex and includes more Severity 1 or 2 hazards, with a higher probability of occurrence than another, is clearly a high risk program, the other a low risk one. The PHL includes information from sources such as safety, analytical, and historical experience from similar systems and missions. The PHL process should be updated and continued in the investment analysis phase.
- Begin the Preliminary Hazard Analysis (PHA) as soon as possible. The PHA focuses on the details of the system design. In addition to the historical experiences used for the PHL, information about technologies, materials, and architectural features such as redundancy are available as sources to the PHA. Systems using new and immature technologies or designs are more risky than those that use proven technologies or modifications of existing designs.
- Use a detailed hazard analysis to provide new and more precise information about safety risk for the program production and deployment phases. This step will minimize the risk of accidents during the test and evaluation process.

A major challenge that confronts government and industry organizations responsible for an SSP is the selection of those tasks that can materially aid in attaining program safety requirements. Scheduling and funding constraints mandate a cost-effective selection, one that is based on identified program needs. The considerations presented herein are intended to provide guidance and rationale for this selection. They are also intended to provoke questions and encourage problem solving by engineers, operations, and support personnel.

After selection, the tasks must be identified and tailored to match the system and program specifications. It is important to coordinate task requirements with other engineering support groups (e.g., reliability, logistics) to eliminate duplication of tasks and to become aware of additional information of value to system safety. The timing and depth required for each task, as well as action to be taken based on task outcome, are program requirements. For these reasons, precise rules are not stated.

Some contractual activities provide cost savings, flexibility, and pre-award planning without affecting compliance or control. These are:

- Coordinate the delivery schedule of safety analysis deliverables with program milestones such as a major design review rather than days after contract award. This prevents the need for contractual changes to adjust for schedule changes. The deliverables should be provided approximately 30 days prior to the milestones, thereby providing current information and the ability of the reviewer to prepare for the design review. The deliverable can be established as a major program milestone; however, this carries the risk of halting an entire program for a single deliverable.
- Consider requiring updates to the first deliverable rather than autonomous independent deliverables at major milestones. For example, if the first system hazard analysis is

scheduled for delivery at the Systems Design Review (SDR), the submittal required at the Preliminary Design Review (PDR) might be limited to substitute and supplementary pages. This requires planning such as configuration control requirements (e.g., page numbering and dating schemes).

- If major design decisions that significantly affect the cost of safety analyses are expected during the contract, fix the size of the effort in a manner that maintains FAA control. An example would be a flight control methodology decision such as would be applied to fly-by-wire, glass cockpit, or mechanical systems. The number of fault trees required in a safety analysis depends on the system selected. A good contractual approach would be to fix the number of fault trees to be provided during negotiations. The contract would reflect that both the FAA and the contractor must agree on which fault trees are to be performed. Thus the task can be tailored to the design well downstream from contract award without affecting performance or cost.
- Maintain a reasonable balance between the analyses and deliverables specified. When the program manager determines that limiting the deliverables is economically necessary, the contractor must maintain a detailed controlled and legible project log that is available for MA review and audit. A compromise approach would be to permit deliverables in contractor format eliminating formatting costs. Requiring FAA approval of alternating deliverables may also be considered. In this situation, program control is maintained at the program major milestones. The MA has the option of reviewing the status of all safety tasks and analyses at these points in the program. The MA has approval authority at each formal design review. This control is more significant than that of a single deliverable.

5.7.1 Small Programs

Tailoring of safety program requirements is important for small programs, because the cost of an SSP can easily match or exceed the cost of the program itself. The program manager must carefully consider both the cost of an item and its criticality in establishing the SSP requirements for such items. The actual benefit may not justify the actual cost of safety. However, sometimes the perceived risk is so high that increased cost is justified. In most situations, such as for the development of a router bridge, a modem, or a fiber optic communications local area network (LAN), SSP costs can be limited without measurably increasing the risk of accident.

The tasks below are recommended as a minimum effort for a small SSP.

- Prepare a preliminary hazards list (PHL)
- Conduct a preliminary hazard analysis (PHA)
- Assign a Risk Assessment code (see Chapter 3).
- Assign a priority for taking the recommended action to eliminate or control the hazard, according to the risk assessment codes.
- Evaluate the possibility of negative effects from the interfaces between the recommended actions and other portions of the system.
- Take the recommended actions to modify the system.
- Prepare a SER or Design Analysis Report (DAR) [8]as completion to the SSP.

[8] FAA System Engineering Manual

There are hazard review checklists available for hazard risk identification. These checklists can be found in System Safety literature and within safety standards and requirements. (See bibliography)

The PHA is developed as an output of the preliminary hazard list. It is the expansion of this list to include risks, hazards, along with potential effects and controls.

An in-depth hazard analysis generally follows the PHA with a subsystem hazard analysis (SSHA), a system hazard analysis (SHA), and an operating and support hazard analysis (O&SHA) as appropriate. For most small programs, a PHA will suffice when appropriate. The PHA then should include all identified risks, hazards, and controls that are associated with the lifecycle of the system.

A comprehensive evaluation is needed of the risks being assumed prior to test or evaluation of the system or at contract completion. The evaluation identifies the following:

- All safety features of the hardware, software, human and system design
- Procedural risks that may be present
- Specific procedural controls and precautions that should be followed

The risks encountered in a small program can be as severe and likely to occur as those in a major program. Caution needs to be exerted to ensure that in tailoring the system safety effort to fit a small program, one does not over-reduce the scope, but instead uses the tailoring process to optimize the SSP for the specific system being acquired, or evaluated.

5.7.2 Government-Furnished Equipment

As part of a system acquisition effort, the FAA may provide equipment necessary for the system development. The interface between the GFE and the new system must be examined if not previously examined. This type of analysis, once considered a separate MIL-STD-882 task, is now considered as part of the overall system analyses. The contractor is responsible for the overall system's safety but not for the inherent risk of the GFE itself. For such situations, the following contractual requirements are suggested:

- If hazard data are available, identify the system safety analyses needed and date they are required.
- Identify and perform any additional system safety analyses needed for interfaces between GFE and the other systems.
- Ideally, the GFE has sufficient history available to the FAA that unsatisfactory operating characteristics are well known or have been identified in previous hazard analyses. The MA should identify these unsatisfactory characteristics or provide the analyses, if available, to the contractor. The contractor will then compensate for these characteristics in the interface design. In some cases, such characteristics may not be known or analyses and/or history is not available. Then either the contractor or the MA must perform the analyses necessary for interface design.

5.7.3 Commercial Off The Shelf/Non-developmental Items (COTS/NDI)

COTS/NDI are commercially developed hardware or software that are currently being marketed publicly. A computer modem, LAN card (or system), radio, and desktop computers are some examples. Procurement of these items saves development costs but is difficult for the system safety activity to

assess, and even more difficult to influence. Simple items, such as the examples above, are usually developed without an SSP. The amount of safety attention required should vary depending on the criticality of the application and the available characterization history. Ideally, experience with the device or more likely a similar model is available to provide the MA with guidance on the safety attention required.

More complex and critical items require a MA decision process to ensure that the risk of accident is acceptable. Commercial subsystem development for items such as a radio or system development for aircraft are likely to include some form of failure-related analysis such as a FMECA or fault tree analysis. A review of this contractor-formatted analysis may provide the necessary assurance. A poorly or non-documented analysis provides the opposite effect.

The COTS/NDI concept provides significant up-front cost and schedule benefits but raises safety and supportability issues. For the NAS to benefit fully from COTS/NDI acquisitions, the SSP must be able to ensure the operational safety of the final system without unnecessarily adding significantly to its acquisition cost. The retrofitting of extensive safety analyses or system modifications may negate any advantage of choosing COTS/NDI

For COTS/NDI acquisitions, a safety assessment for the intended use should be performed and documented before purchase. Such analyses should contribute to source and/or product selection. This should be contained in the buyer's SSPP. COTS/NDI will be evaluated for operational use by considering all aspects of the item's suitability for the intended purpose. Suitability criteria should include technical performance, safety, reliability, maintainability, inter-operability, logistics support, expected operational and maintenance environment, survivability, and intended life cycle. To assure risk acceptability, appropriate hazard analysis must be conducted to evaluate the risks associated with initial field testing of COTS/NDI.

Many developers of COTS/NDI may not have SSPs or staff to assess the suitability of COTS/NDI proposed for NAS applications. Therefore, the MA must do the following.

- Establish minimum analysis requirements for each procurement. These vary due to the nature of the item being procured and the criticality of its mission. Examples include mission and usage analysis and specific hazard analyses to determine the potential system impact on the remainder of the system or the NAS itself.
- Include in each procurement document the system safety analyses required for accurate and standardized bidding
- Restrict the application of the procured COTS/NDI to the missions analyzed, or reinitiate the analysis process for new missions.
- Apply skillful, creative tailoring when limiting the SSP scope to accommodate program size and procurement schedules.
- Marketing investigation, hazard analysis, and System Safety Working Groups are additional considerations and are explained below.

5.7.4 Marketing Investigation

The MA could conduct a market investigation to identify the safety or other appropriate standards used to design the system. The MA must determine the extent to which the system was certified or otherwise

evaluated by government and non-government agencies such as the FAA, Department of Defense (DOD), and Underwriter Labs. It must then determine what this information provides when compared to mission requirements. The following basic questions form the basis of a COTS/NDI procurement checklist, such as:

- Has the system been designed and built to meet applicable or any safety standards? Which ones?
- Have any hazard analyses been performed? Request copies of the analyses and the reviewing agency comments.
- What is the accident and accident history for the system? Request specifics.
- Are protective equipment and/or procedures needed during operation, maintenance, storage, or transport? Request specifics.
- Does the system contain or use any hazardous materials, have potentially hazardous emissions, or generate hazardous waste?
- Are special licenses or certificates required to own, store, or use the system?

Hazard Analysis

A safety engineering report may be all that is necessary or available to gather detailed hazard information concerning a COTS/NDI program. If the selected program must be modified to meet mission requirements, other hazard analyses may be required, especially if the modifications are not otherwise covered.

System Safety Working Groups.

Requiring an SSWG meeting early in the program will help clarify system safety characteristics versus mission requirements and allow time to address issues. A follow-up SSWG meeting can be used to ensure satisfactory closure of issues. Periodic SSWG meetings throughout the life cycle of the system can be used to address ongoing concerns and special issues. See Chapter 6.4.2 for more information.