Chapter 6:

System Safety Guidelines for Contracting

6.0 System Safety Guidelines for Contracting

6.1 Contracting Principles

Contracting provides the legal interface between the FAA, as a buying agency, and a selling organization, usually a contractor. The contract document binds both parties to a set of provisions and requirements. This means that if desired safety criteria, analyses, or tests are not specified in the contract, the contractor is not obligated to provide them. In other words, the contractor is not required to comply with post contract requirements. It is the IPT leader's responsibility to define these requirements early enough in the acquisition cycle to include them in the negotiated contract.

6.2 Contracting Process

The AMS provides a definitive contracting process, or series of activities, which must be accomplished in order to effect an acquisition. These activities are broken into five (5) major lifecycle components: Mission Analysis, Investment Analysis, Solution Implementation, In-Service Management and Service Life Extension. These components are described in Chapter 4. This chapter focuses on the basic acquisition steps of solution implementation. They may be summarized as follows:

- Acquisition planning,
- Documentation of detail requirements
- Communicating requirements to industry, and
- Evaluation of the resulting proposals or bids,
- Negotiation and/or selection of the source to perform the contract, and
- Management of the awarded contract to assure delivery of the supplies or services required.

The execution of these steps should be tailored for each acquisition. Figure 6-1 illustrates a sample acquisition from planning through contract negotiation. The following paragraphs describe the activities within the contracting process.

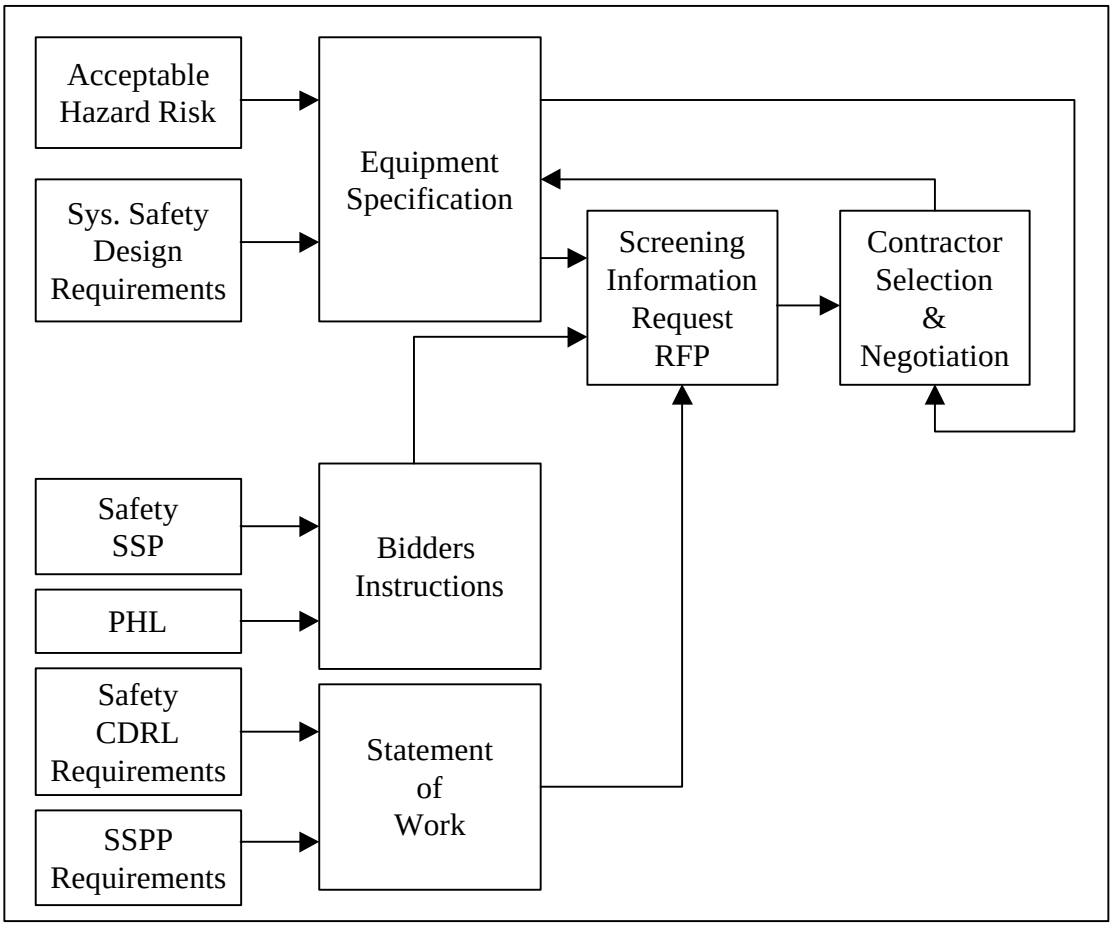

Figure 6-1 Example of the Contracting Process

6.2.1 Acquisition Planning

To insure inclusion of the desired safety criteria and system safety program (SSP) in the contract, a great deal of planning is required before proposals and costs are solicited from potential contractors. This results in technical and administrative requirements.

For the former, qualified technical personnel must either select and/or tailor an existing specification for the items required or create a new one if an appropriate one does not exist. The specification must reflect two types of safety data:

- Performance parameters (e.g., acceptable risk levels, specific safety criteria such as electrical interlocks)
- Test & Evaluation Requirements (e.g., specific safety tests to be performed and/or specific program tests to be monitored for safety.

Traditionally, administrative requirements have been specified in the request for proposal. MIL-STD-882D has taken a position that given the technical requirements, defining the administrative requirements can be left to the bidding contractor to define as part of the bidding process. The proposal evaluation team will judge the adequacy of the proposed safety program. Inadequate proposed safety programs can either be judged not-responsive or amended during negotiation.

The following administrative requirements must be defined and included in the negotiated contract and/or Statement of Work (SOW):

- Delivery Schedule (e.g., Schedule of safety reviews, analyses, and deliverables. It is suggested that delivery be tied to specific program milestones rather than calendar dates e.g., 45 days before Critical Design Review).
- Data Requirements (e.g. Number of safety analysis reports to be prepared, required format, content, approval requirements, distribution.)

Another valuable element of acquisition planning is estimating contractor costs of safety program elements to assist in:

- Determining how much safety effort is affordable; and is it enough?
- Optimize the return on safety engineering investment.
- Perform a sanity check of contractor's bids.

6.2.2 Development and Distribution of a Solicitation

To transmit the requirements to potential bidders, an Invitation for Bids, (if the Sealed Bidding method is used), or a Screening Information Request (SIR) Request for Proposals (RFP), if a competitive proposals process is used. These documents contain the specification (or other description of the requirement), data requirements, criteria for award, and other applicable information. For some programs with complex safety interfaces (e.g. multiple subcontractors), or high safety risk the IPT may require the submission of a draft System Safety Program Plan (SSPP) or Integrated System Safety Program Plan (ISSPP) with the contractor's proposal. The purpose is to provide evidence to the FAA that the contractor understands the complexity of the safety requirement and demonstrates the planning capability to control such risks. In those cases, where the responsibility for defining the SSP's administrative elements has been assigned to the contractors, the inclusion of a draft SSPP or ISSPP with the proposal is essential.

Each solicitation contains at least three sections that impact the final negotiated SSP:

- Equipment Specification
- Statement of Work (SOW)
- Instructions for preparation of proposals/bids and evaluation criteria. (Sections L and M respectively)

6.2.3 Equipment Specification

Specifications are the instructions dictating to the designer the way the system will perform. A system specification is prepared for all equipment procured by FAA. The system specification and more detailed requirements that flow down to lower level specifications define design requirements. The careful selective

use of FAA and Military Standards can simplify the specification of design criteria. For example, FAA-G-2100F provides physical safety design criteria. MIL-STD-1522 contains specific instruction for pressure vessels, placement of relief valves, gauges, and high-pressure flex hose containment. MIL-STD-454, Requirement 1 specifies design controls for electrical hazards and MIL-STD-1472 for ergonomic issues. Whether these specifications are contractor prepared or supplied by the managing activity, it is important that proper instructions are given directly to the designer who controls the final safety configuration of the system.

MIL-STD-490 gives a format for preparing universally standard types of specifications. Appendix I of MIL-STD-490 identifies the title and contents of each paragraph of the system specification. Other appendices describe other types of specifications, such as prime item development, product, and so on. Several paragraphs in each specification are safety related. These include:

Health and Safety Criteria. This paragraph concerns the health of operations personnel. It should include firm requirements for radiation levels (such as X-rays from high-power amplifiers and antenna radiation patterns), toxic gases, and high noise environments. Each system has its unique operating environment. In so far as possible, associated health problems must be anticipated and a firm requirement for solving those problems should be included in this section. Those problems missed may be identified by the contractor's SSP. The advantage of identifying actual or anticipated health problems in this section of the system specification is that their solution will be included in the contract price and be a design requirement.

Safety Requirements. This paragraph should contain general system-level safety requirements. Some examples of these requirements can be found in requirement 1 of MIL-STD-454 and paragraph 5.13 of MIL-STD-1472. Citing an entire document or design handbook and expecting the contractor to comply with every thing therein is unrealistic. Where practical, assigned acceptable probability numbers for Category I and II hazards, should be included in this paragraph.

Functional Area Characteristics. This paragraph has subparagraphs that address more specific lower-level safety requirements, such as safety equipment. Paragraph 3.7 of MIL-STD-490 defines specifications and identifies all emergency-use hardware, such as fire extinguishers, smoke detection systems, and overheat sensors for the system operating environment.

Quality Conformance Inspections. This paragraph requires the contractor to verify by inspection, analysis, or actual test, each requirement in section 3 of the system specification including systems safety. Paragraph 4.2, often requires verification of corrective actions taken to manage the risk of all Category I and II hazards. The corrective measures would be verified by inspection, analysis, or demonstration.

6.2.4 Statement of Work (SOW)

The SOW, usually Section C of the RFP, defines the work anticipated to be necessary to complete the contract. This is the only means the procuring activity has available to communicate the scope of the system safety task. There are two viable approaches to preparing a SOW for a bid package. The first is to specify adherence to Section 4 of MIL-STD-882D which provides the minimum components of a SSP but not specific analyses or deliverables. The second includes these details in the SOW as part of the procurement package. The first approach increases the complexity of the source selection and negotiation processes, but may reduce acquisition costs. The latter is more traditional but is in conflict with current trends of increasing flexibility. In either case, the negotiated SOW must be explicit. The following discussion is applicable to an explicit SOW whether it be submitted with RFP package or negotiated.

The SOW task descriptions can consist of a detailed statement of the task or contain only references to paragraphs in other documents such as MIL-STD-882 or this handbook. Elaborate task descriptions are not required. A simple statement, however, in the body of the SOW such as, "The contractor shall conduct a System Safety Program to identify and control accident risk" does not define the safety requirements adequately. A contractor might argue that it is only required to caution it’s design team to look out for and minimize hazards.

System Safety Section

This section of the SOW must contain enough detail to tell the contractor exactly what kind of SSP is required. Some SSP issues that could be detailed in the SOW follow:

- The requirement for planning and implementing an SSP tailored to the requirements of MIL-STD-882.
- Defining relationships among the prime contractor and associate contractors, integrating contractors, and subcontractors i.e. "Who's the Boss?".
- The requirement for contractor support of safety meetings such as System Safety Working Groups (SSWG). If extensive travel is anticipated, either the FAA should estimate the number of trips and locations or structure the contract to have this element on a cost reimbursable basis.
- Definition of number and schedule of safety reviews, with a statement of what should be covered at the reviews. Safety reviews are best scheduled for major design reviews, such as the system design review, preliminary design review, and critical design review.
- Requirement for contractor participation in special certification activities, such as for aircraft. The FAA may anticipate that support from a communications supplier may be necessary for the aircraft certification process.
- Procedures for reporting hazards. The CDRL will specify the format and delivery schedule of hazard reports. Note that permitting contractor format can save documentation costs but, in the case where there are multiple contractors may make integration difficult.

- Definition of required analyses to be performed, such as the preliminary hazards list, preliminary hazard analysis, and system hazard analysis. The contract data requirements list specifies the format and delivery schedule of required analyses.
- The specification of required safety testing, i.e., special test of specific components or subsystems or monitoring specific other tests.
- Basic risk management criteria. Specify a set of conditions that state when the risk of the hazard is acceptable and that require the contractor to specify alternate methods for satisfying the acceptable risk requirement. (See Chapter 3 for examples of criteria for severity, likelihood, and risk acceptability.)
- Special safety training or certification that might be needed for safe operation of critical systems.
- Reviews of engineering change proposals and deviations and waivers to make sure design changes do not degrade the safety level of the system.
- Techniques for doing analyses, such as the fault hazard analysis and fault tree analysis. If included, specify on which system and subsystems the contractor should do these analyses. Specify the candidate top events for fault tree analyses, such as flight control or power systems. (See Chapters 8 & 9 for a discussion of analysis techniques and analytical tools.)

6.2.5 Contract Data Requirements List

A Contract Data Requirements List (CDRL) is usually appended to the SOW. Contractual data to be delivered falls into two general categories:

- Financial, administrative, or management data. The procuring activity requires these data to monitor contractor activities and to control the direction contractor activities are taking. Contractors that require the use of the Cost Schedule Control System $(CS)^2$ or equivalent permit the FAA to monitor expended safety engineering effort and progress on a monthly basis. This type of system makes it clear whether or not a contractor is only applying safety resources to major program milestones.
- Technical data required to define, design, produce, support, test, deploy, operate, and maintain the delivered product.

Preparing data submissions can be expensive and represent a major portion of the contractor's safety resources. The system safety data requirements listed on the CDRL, therefore, should represent only the absolute minimum required to manage or support the safety review and approval process. Two choices are to be made and reflected in the CDRL: 1) Should the contractor prepare the data in a format specified by a data item description (DID) or in contractor format. 2) Which submittals require approval for acceptance and payment.

The contractor does not get paid for data not covered by the CDRL/DID. He is not obligated to deliver anything not required by a CDRL. It is advantageous to effectively utilize the DIDs when available. When specifying DIDs they should be examined carefully, sentence by sentence, to assure applicability. It is

suggested that the data review and approval cycle be 30-45 days. Longer review cycles force the contractor, in many cases, to revise an analysis of an obsolete configuration.

6.2.6 Bidders' Instructions

The bidder's instructions reflect how the proposal will be evaluated. There are a few instructions that, when included in the instructions for the management and technical sections of the proposal, simplify evaluation. The bidders' response should be keyed to specific Specification and SOW requirements and evaluated by means of a RFP required compliance matrix (reference Figure 6-2). Proposed costs should be supplied against the Work Breakdown Structure (WBS) permitting visibility of the SSP costs. For large programs, the costs should be separable by major SSP tasks.

RFP	PROPOSAL
Specification **3.6.3 Acceptable Hazard Level** **Electrical Design Criteria**	**Tech. Vol. 8.3** **Tech. Vol. 4.7, 8.3, 12.0**
SOW **6.3 SSP Tasks** **CDRLs**	**Tec. Vol. 8.3, Appendix B** **Appendix B**
Instructions to Bidder **13a Draft SSPP** **13.b Draft PHL**	**Appendix B** **Tech. Vol. 8.3, Mgmt. Vol. 2.0**

Figure 6-2: Sample Compliance Matrix

The details of the proposed SSP are important to the safety program evaluator, either as a separable document or section of the proposal. Requiring a draft plan as part of the proposal package is an excellent communication tool but it must be remembered that such a requirement increases the contractor's cost of bidding for a contract. For large programs, this cost may be incidental, for others it may significant. When the requirement for a SSPP is included in the RFP, the following type of statement tailored to specific program needs could be contained in the management section of the bidders' instructions:

> The offeror shall submit an initial SSPP in accordance with DI-SAFT-80100 as modified by CDRLXXX. This plan shall detail the offeror’s approach to paragraph 10 of DID DI-SAFT-80100 (as modified). This preliminary plan shall be submitted as a separate annex to the proposal and will not be included in overall proposal page limitations.

NOTE: This approach takes advantage of standardized DIDs and does not mean to imply that page limitations on system safety plans are inappropriate. A well-prepared plan can cover the subject in less than 50 pages.

To encourage attention on system safety in the technical proposal, the bidders instructions should include wording such as: "The offeror shall submit a summary of system safety considerations involved in initial trade studies." In later development phases, it may be advantageous to require the offeror to "submit a preliminary assessment of accident risk." The validation phase may require the bidder to describe system safety design approaches that are planned for particularly high-risk areas (i.e., separated routing of

hydraulic lines, or separate room installation of redundant standby generators.) During this program phase, the following statement could be included:

> The offeror shall submit a description of the planned system safety design and operational approach for identification and control of safety-critical, high-risk system design characteristics.

As previously noted, the RFP can request submission of draft data items, such as the SSPP or Preliminary Hazard List (PHL), before contract award. Alternatively, the bidders can be instructed to discuss their proposed SSP in detail, including typical hazards and design solutions for them or candidate hazards for analysis. Careful wording can provide almost the same results as a draft data item. Key areas of interest, such as personnel qualifications or analysis capabilities, can be cited from data items as guides for the bidders' discussions. For example, "discuss your proposed SSP in detail using data item DI-SAFT-80100, paragraphs 10.2 and 10.3, as a guide." Using DI-SAFT-80100 as a guide, sample criteria could include the following:

- Describe in detail the system safety organization, showing organizational and functional relationships and lines of communication
- Describe in detail the analysis technique and format to be used to identify and resolve hazards
- Justify in detail any deviations from the RFP.

Proposals are evaluated against the award criteria included in the RFP. If safety is not listed in the award criteria, the bidder's responses to safety requirements have little impact on the award decision. Negotiations take place with each contractor still in contention after initial review. The IPT members review in detail all segments of each contractor's proposal and score the acceptability of each element in the evaluation criteria. Extensive cost and price analysis of the contractors' proposals must be accomplished so that a determination that the final price is "fair and reasonable" to the government and to the contractor. The relative proposed cost of the SSP reflects on the seriousness that each contractor places on System Safety. It is not, in itself the ultimate indicator, as some contractors may "work smarter" than others.

6.3 Evaluating Bidding Contractors (System Safety Checklist)

There are three components of the evaluation process:

- Proposal Evaluation
- Contractor Evaluation
- Negotiation

6.3.1 Proposal Evaluation

This section provides an extensive list of SSP criteria that can either be used to structure a SSP requirement for a solicitation or used to evaluate a contractor's response to a Request for Proposal (RFP). Caution should be taken not to penalize a contractor for not responding to a requirement found below that is not explicitly or reasonably implicitly included in the specified requirements.

The data that follows is divided into eight groups and provided in a checklist format. The contents are comprehensive and should be tailored for each application. A contractor's response to an RFP that addresses all issues listed below is likely to be large for most proposals. Additionally, adherence to the complete list is not appropriate for many acquisitions. Formal questions to the bidders or discussions during negotiations can resolve reasonable omissions.

System Safety Program Plan (SSPP)

A SSPP should provide the following information:

- Details of the system safety manager to program manager relationship and accountability.
- Identification of the organization(s) directly responsible for accomplishing each subtask and company policies, procedures, and/or controls governing the conduct of each subtask.
- A description of methods to be used in implementation of each SSPP task including a breakout of task implementation responsibilities by organizational component discipline, functional area, or any planned subcontractor activity.
- A composite listing of applicable company policies, procedures, and controls, by title, number, and release date.
- A chart showing the contractor's program organization identifying the organizational element assigned responsibility and authority for implementing the SSP.
- Identification of the interfaces of the system safety organization and other organizations, including cross-references to applicable sections of other program plans.
- A clearly detailed method by which problems encountered in the implementation of the SSP and requirements can be brought to the attention of the contractor program manager.
- Procedures to be used to assure resolution of identified unacceptable risks.
- The internal controls for the proper and timely identification and implementation of safety requirements affecting system design, operational resources, and personnel.
- A schedule of the system safety activities and a milestone chart showing relationships of the system safety activities with other program tasks and events. Tasks and data inputs and outputs which correspond to the program milestones should be identified. Milestones are controlled by program master schedule and internal operations directives.
- Staffing levels required for successful completion of contractually required tasks.
- A description of the contractor's program and functional system safety organization.

See Chapter 5 for a more detailed discussion of SSPP contents and the SSPP template. The ISSPP should be considered a special case of the SSPP that involves multiple major subcontractors that must be integrated by the Prime Contractor/Integration Contractor.

Contractor's System Safety Program Management

An SSPP is only as good as the contractor's management commitment to systems safety. The FAA should not dictate prospective (or contracted) contractor's organizational structures. An assessment can be made of such organizations to determine if the contractor can meet the Government's objectives. Criteria include:

- A centralized accident risk management authority, as delegated from the contractor program manager. It must maintain a continuous overview of the technical and planning aspects of the total program.
- An experienced system safety manager directly accountable to the program manager for the conduct and effectiveness of all contracted safety effort for the entire program.
- A single point of contact for the FAA interface with all contractor internal program elements, and other program associate or subcontractors for safety-related matters. The contractor system safety manager maintains liaison with Government sources to obtain:
  - Safety data as a design aid to prevent repetitive design or procedural deficiencies.
  - Information on operational systems which are similar to the system under this contract and should be studied for past safety problems and their solutions.
  - Authority for access of personnel to nonproprietary information on accident and failure causes and preventive measures in possession of government agencies and contractors involved with those systems.
- Approval authority for critical program documentation and all items related to safety contained in the contract data requirements list (CDRL).
- Internal approval authority and technical coordination on waiver/deviations to the contractually imposed system safety requirements, as defined.
- Internal audits of safety program activities, as defined, and support FAA audits, when requested.
- Participation in program level status meetings where safety should be a topic of discussion. Provide the contractor program manager the status of the SSP and open action items.

Contractor's SSP

Requirements and guidance for a contractor's SPP are specified in the Statement of Work (SOW) and the Data Item Description (DID). Good SSP's have the following characteristics which should be reflected in either the SSPP or internal documented practices:

- Review of and provide inputs to all plans and contractual documents related to safety.
- Maintenance of safety-related data, generated on the program by the safety staff.

- Maintenance of a log, available for FAA review, of all program documentation reviewed and records all concurrence, non-concurrence, reasons for non-concurrence, and actions taken to resolve any non-concurrence.
- Coordination of safety-related matters with contractor program management and all program elements and disciplines.
- Coordination of system safety, industrial safety, and product safety activities on the program to ensure protection of the system during manufacture and assembly.
- Establishment of internal reporting systems and procedures for investigation and disposition of accidents and safety incidents, including potentially hazardous conditions not yet involved in an accident/incident; such matters are reported to the purchasing office as required by the contract.
- Performance of specified Hazard Analyses.
- Participation in all requirements reviews, preliminary design reviews, critical design reviews, and scheduled safety reviews to assure that:
    - All contractually imposed system safety requirements are met.
    - Safety program schedule and CDRL data deliverable content are compatible.
    - Hazard analysis method formats, from all safety program participants, permit integration in a cost effective manner.
    - Technical data are provided to support the preparation of required analyses.
- Participates in all test, flight, or operational readiness reviews and arranges for presentation of required safety data.
- Provision for technical support to program engineering activities on a daily basis. Such technical support includes consultation on safety-related problems, research on new product development, and research and/or interpretation of safety requirements, specifications, and standards.
- Planned participation in configuration control board activities, as necessary, to enable review and concurrence with safety-significant system configuration and changes.
- Review of all trade studies. Identification of those that involve or affect safety. Participation in all safety related trade studies to assure that system safety trade criteria are developed and the final decision is made with proper consideration of accident risk.
- Provisions for system safety engineering personnel participation in all trade studies identified as being safety-related. Ensure that safety impact items and accident risk assessments are given appropriate weight as decision drivers.
- Provides trade study documentation that shows the accident risk for the recommended solution is equal to or less than the other alternative being traded, or provide sufficient justification for recommending another alternative.

- Identification of any deficiencies regarding safety analysis or risk assessment, when they are not provided with government-furnished equipment and property.
- Identification of deficiencies where adequate data to complete contracted safety tasks is not provided.
- Acknowledgement of specified deliverable safety data format, as cited on the CDRL. Where no format is indicated, the contractor may use any format that presents the information in a comprehensible manner.
- Provision for safety certification of safety-critical program documentation and all safety data items contained in the CDRL.
- Recognition that the SSP encompasses operational site activities. These activities include all operations listed in operational time lines, including system installation, checkout, modification, and operation.
- Acknowledgment that SSP consideration must be given to operations and interfaces, with ground support equipment, and to the needs of the operators relating to personnel subsystems, such as panel layouts, individual operator tasks, fatigue prevention, biomedical considerations, etc.
- Incorporation of facility safety design criteria in the facility specifications.
- Evaluation of the safety impact of system design changes. Revisions or updates subsystem hazard analyses and operating and support hazard analyses to reflect system design changes during the life of the program.
- Attention given to planning, design, and refurbishment of reusable support equipment, including equipment carried on flight vehicles, to assure that safety is not degraded by continued usage.
- Planned review of engineering change proposals (ECP) to evaluate and assess the impact on safety design baseline. This safety assessment must be a part of the ECP and include the results of all hazard analyses done for the ECP.
- Planned system safety training for specific types and levels of personnel (i.e., managers, engineers, and technicians involved in the design, product assurance operations, production, and field support). Safety inputs to training programs are tailored to the personnel categories involved and included in lesson plans and examinations.
- Contractor safety training may also include government personnel who will be involved in contractor activities.
- Safety training includes such subjects as hazard types, recognition, causes, effects, and preventive and control measures; procedures, checklists, and human error; safeguards, safety devices, and protective equipment, monitoring and warning devices, and contingency procedures.
- Provision for engineering and technical support for accident investigations when deemed necessary by the management activity. This support includes providing contractor technical personnel to the accident investigation board.

Integrated System Safety Program Plan

Complex programs with many contractors often require a systems integration contractor. The systems safety staff of the systems integrator contractor is required, in-turn, to generate an Integrated System Safety Plan (ISSP), which establishes the authority of the integrator and defines the effort required from each associate contractor for integration of system safety requirements for the total system. The system safety integrator initiates action to ensure that each associate contractor is contractually required to be responsive to the SSP. If the associate contractors are not system integrator subcontractors, the integrator contractor should propose contractual modifications when required for the successful performance of the ISSP. Associate contractor system safety plans can be incorporated as appendices to the ISSP.

Detailed Contractor Integration Activities

Generation of the System Safety Program Plan (SSPP) is the first management task of a System Safety Program (SSP) following contract award as discussed in Chapter 4. These are primarily management tasks and are applicable to many SSPs. When selected, they should be included in the requirements of the Request for Proposal (RFP) or contract Statement of Work (SOW). The SSPP must include planning for these activities when they are contractually specified. These management tasks activities, are:

- Contractor Integration
- System Safety Program Reviews/Audits
- System Safety Working Group/System Safety Working Group Support
- Hazard Tracking/Risk Resolution
- System Safety Progress Report

Figure 6.3 illustrates the improved communications.

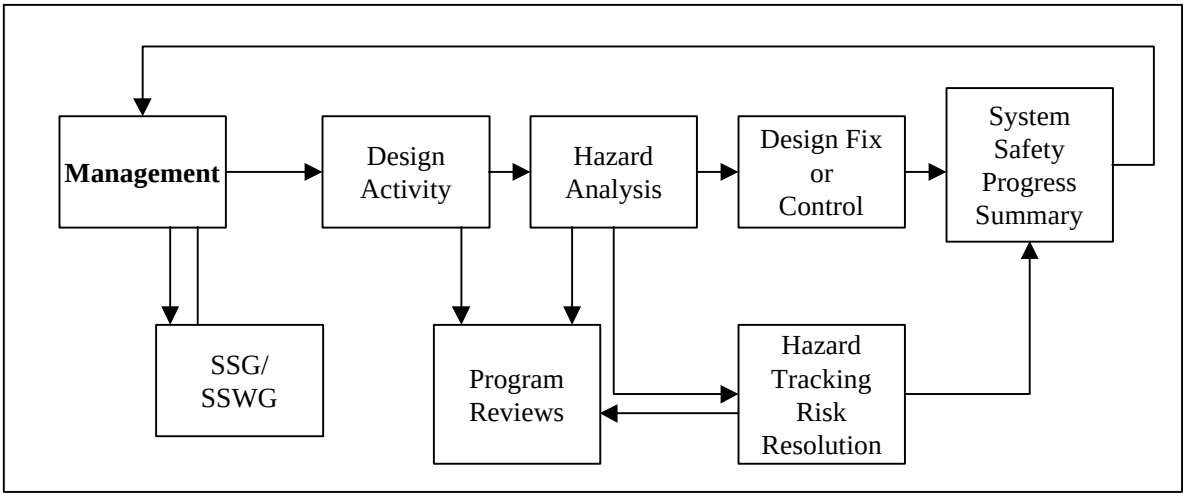

Figure 6-3: Improved Communication Paths

Contractor Integration

Major program projects often require multiple associate contractors, subcontractors, integration contractors, and architect and engineering (AE) firms. On these programs, the integrating contractor often has the responsibility to oversee system safety efforts of associate contractors or AE firms.

A program with many associate contractors or subcontractors requires an ISSPP that provides, major emphasis on the integration process, flowdown of system safety requirements and responsibilities, and monitoring of subcontractor performance. This SSPP is called an Integrated System Safety Program Plan (ISSPP), which generally follows the requirements of MIL-STD-882. Figure 6-4 illustrates the ISSPP additional tasks.

The systems integrator or construction contractor has the visibility and, therefore, must have the responsibility of performing the system hazard analyses and assessments that cover the interfaces between the various contractors' portions of the system or construction effort. When an integration contractor does not exist, and the managing authority procures the subsystems directly, this responsibility is given to the managing authority. In situations where an integration contractor exists, the managing authority must clearly and contractually define the role and responsibilities of the integration contractor for the associate contractors. Management is responsible for assisting the integrator in these efforts to ensure that all contractors and firms mutually understand the system safety requirements and their respective responsibilities in order to comply with them.

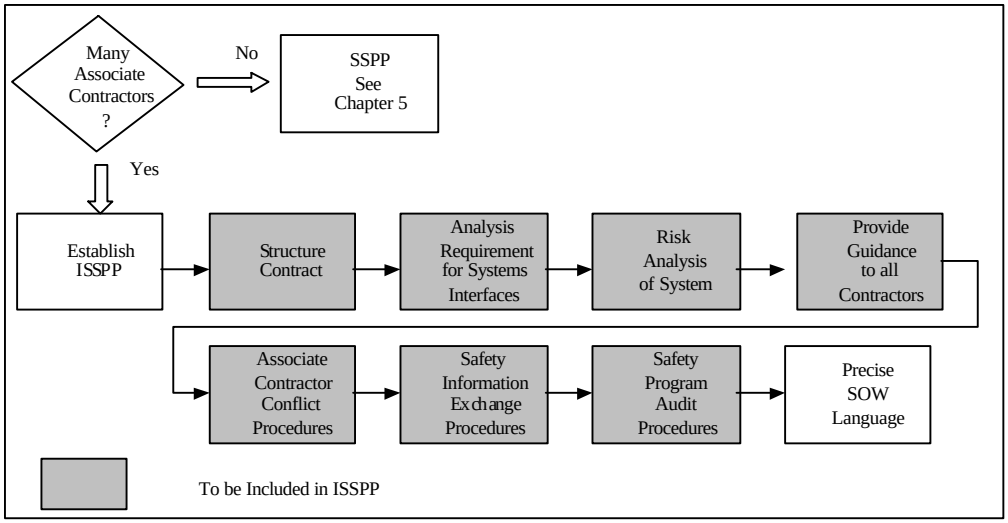

Figure 6-4 ISSPP Additional Tasks

The following is a list of tasks from which the managing authority may choose the systems integration contractor's responsibilities. Those selected should be included in the RFP and SOW.

1. Prepare ISSPP following the requirements. The ISSPP will define the role of the systems integration contractor and the effort required from each associate contractor to help integrate system safety requirements for the total system. In addition, the plan may address and identify:

(a) Definitions of where the control, authority, and responsibility transitions from the integrating contractor to the subcontractors and associate contractors

(b) Analyses, risk assessment, and verification data to be developed by each associate contractor with format and method utilized

(c) Data each associate contractor is required to submit to the integrator and scheduled delivery keyed to program milestones

(d) Schedule and other information considered pertinent by the integrator

(e) The method of development of system-level requirements to be allocated to each associate contractor as a part of the system specification, end-item specifications, and other interface documents

(f) Safety-related data pertaining to off-the-shelf items

(g) Integrated safety analyses to be conducted and support required from associate contractors and subcontractors

(h) Integrating contractor's roles in the test range or other certification processes

(i) SSP milestones

2. Initiate action through the managing authority to ensure each associate contractor is required to be responsive to the ISSPP. Recommend to the management contractual modification where the need exists.

3. Examine the integrated system design, operations, and specifically the interfaces between the products of each associate contractor during risk assessment. This requires using interface data that can often only be provided by an associate contractor.

4. Summarize the mishap risk presented by the operation of the integrated system during safety assessments.

5. Provide assistance and guidance to associate contractors regarding safety matters.

6. Resolve differences between associate contractors in areas related to safety, especially during development of safety inputs to systems and item specifications. When the integrator cannot resolve problems, notify the managing authority for resolution and approval.

7. Initiate action through the managing authority to ensure information required by an associate contractor from the integrating contractor (or other associate contractors) to accomplish safety tasks is provided in an agreed-to format. Establish associated logs to prevent such requests from "becoming lost."

8. Develop a method of exchanging safety information between contractors. If necessary, schedule and conduct technical meetings between all associate contractors to discuss, review, and integrate the safety effort. Provide for informal one-on-one telephone contact. Consider establishing system safety databases at the systems integration contractor with telephone access and/or the distribution of monthly safety reports featuring contributions from each contractor. These may be extracted from monthly progress reports, if the progress report requirements are specified accordingly.

9. Implement an audit program to ensure that the objectives and requirements of the SSP are being accomplished. Notify in writing, any associate contractor of its failure to meet contract program or technical system safety requirements for which it is responsible. The integrator for the safety effort will send a copy of the notification letter to the managing authority, whenever such written notification is given. Establish a deficiency log to track the status of any such issues

Details to be specified in the SOW shall include, as applicable:

- Imposition of MIL-STD-882D
- Imposition of this System Safety Handbook
- Designation of the system safety integrating contractor
- Designation of the status of the other contractors
- Requirements for any special integration safety analyses
- Requirements to support test, environmental, and/or other certification processes.

Test and Evaluation (T&E) Guidelines

Consideration of the safety aspects testing is important as they present the earliest opportunity in a program for accidents to occur and for risk mitigations to be demonstrated. The T&E and operations safety interfaces encompass all development, qualification, acceptance, and pre-operational tests and activities. The following guidelines should be considered, as appropriate, for inclusion in the RFP, contractual requirements, and/or the SSPP:

- Test procedures must include inputs from the safety analyses and identify test and operations and support requirements.
- Verification of system design, and operational planning compliance with test or operating site safety requirements, is documented in the final analysis summary.
- Establishment of internal procedures for identification and timely action or elimination/control of potentially hazardous test conditions induced by design deficiencies, unsafe acts, or procedural errors. Procedures should be established to identify, review, and supervise potentially hazardous, high-risk tests, including those tests performed specifically to obtain safety data.
- Contractor system safety organization review and approval of test plans, procedures, and safety surveillance, procedures, and changes to verify incorporation of safety requirements identified by the system analysis. The contractor system safety organization assures that an assessment of accident risk is included in all pretest readiness reviews.
- Safety requirements for support equipment are identified in the system safety analyses.
- Support equipment safety design criteria are incorporated in the segment specifications.
- Test, operations, and field support personnel are certified as having completed a training course in safety principles and methods.
- Safety requirements for ground handling have been developed and included in the transportation and handling plans and procedures. Safety requirements for operations and servicing are included in the operational procedures. The procedures are upgraded and refined, as required, to correct deficiencies that damage equipment or injure personnel.

Safety Audits

System safety audits should be conducted by the system safety manager and, on a periodic basis, by a contractor management team independent of the program. The list of issues to be included in the audit program may be selected from the following list:

- The status of each safety task
- Interrelationship between safety and other program disciplines
- Identification and implementation of safety requirements criteria
- Documented evidence which reflects planned versus actual safety accomplishment.
- Program milestones and safety program milestones
- Schedule incompatibilities that require remedial corrective action
- Contractor initiates positive corrective actions where deficiencies are revealed by the audits.
- Verification or corrective action on problems revealed by previous audits.
- Subcontractor audits to ensure that:
    - They are designing and producing items whose design or quality will not degrade safety
    - Safety analyses are conducted as required
    - System safety problems are being brought to the attention of their own program managers and prime contractor management.

How to Use The Checklist

The checklist above can be used for evaluating a bidders response and/or a SSPP submitted to the for approval. The process to use the checklist for evaluation is as follows:

- For each program, group the items in the checklist into four categories:
    - Those explicitly required by the SOW and/or contract
    - Those that, in the view of the reviewer, are desirable or necessary to perform in meeting the explicitly stated requirements
    - Those that are not applicable to the program for which the evaluation is being performed
    - Those that, in the opinion of the evaluator, were not included in the RFP, SOW, or contract.
- For purposes of evaluation, the latter two categories must handled delicately. If an important omission was made by a bidder(s) and not explicitly included in the RFP, all bidders must be given an equal opportunity to bid the missing SSP elements.
- Ultimately, the first two categories are used for evaluation. Clearly, the decision process must utilize the explicitly stated or negotiated requirements. The applicable elements in the checklist can be graded requirement by requirement either as simply compliant or non-compliant or by assigning "grades" to the response of each requirement. Grade responses numerically reflect the degree of compliance as:

0	Unacceptable (does not meet minimum requirements)
1	Marginal (success doubtful)
2	Acceptable (probable success)
3	Excellent (success likely)
4	Superior (success very likely)
5	Outstanding (high probability of success)

A variation of grading management responses might be:

0	No management planning, personnel not qualified, no authority, resources minimal
1	Planning barely adequate, little management involvement, resources inadequate
2	Planning adequate, implementation weak, management modestly concerned, resources ineffectively utilized
3	Planning generally good, implementation good, management involved, resources adequate and used effectively, program well received in most program areas
4	Strong planning, implementation, management involvement; good use of resources, program well received in all affected areas
5	Strong, excellently implemented program in all areas
6	Outstanding innovative program. Industry leader.

The final step is to add (or average) the scores for each bidder to determine acceptability or the best. For close decisions, the process can be repeated for the implicit requirements as described in group 2 above.

6.3.2 Contractor Evaluation

A good proposal must be backed up with a competent and dedicated staff. A number of programs have stumbled because the winning organization either did not have the necessary staff or management processes to execute the proposed program.

Contractor System Safety Components

One way of assessing both contractor system safety capability and intent is to break down the system safety "big picture" into important organizational activities and examine the documentation used or generated by each. The following describes six such components, the associated SSP responsibilities, and benefits.

- **Corporate or Division.** Many companies establish safety policies at the Corporate and Division levels. These safety policies or standards are imposed on all company development and/or production activities. The presence of such standards, accompanied by audit procedures can provide the evaluation team with an indication of company commitment, standardized safety approaches, and safety culture.
- **Procurement Activity.** Contractors write specifications and SOWs for subcontractors and vendors. An internal procedure or actual examples of previous subcontracts should demonstrate an intelligent process or requirements "flow down". It is not sufficient to impose system safety requirements on a prime contractor and monitor that contractor's SSP if that contractor uses major system components developed without benefit of a SSP.
- **Management of Program's SSP.** The contractor's SSPP describes in detail planned management controls. The plan should reflect a combination of contractual direction, company polices, and "hands-on" experience in developing, managing, and controlling the SSP and its resources. The contractor's SSP manager's credentials must include knowing not only company policies, procedures, and practices but also the technical requirements, necessary activities and tools, and the characteristics of the operational environments.
- **Contractor's Engineering SSP**. The system safety engineer should possess in-depth knowledge of engineering concepts including hazard risk assessment and control, the system, and associated accident risk to implement the SSP. The engineer develops design checklists, defines specific requirements, performs hazard analyses, operates or monitors hazard tracking systems, and in conjunction with the design team implements corrective action. Qualifications of system safety personnel are discussed in Chapter 4.
- **Specifications and Requirements.** The potential exists for engineers and designers, possessing minimal safety knowledge, to be charged with incorporating safety criteria, specifications, and requirements into the system or product design. It is essential that this activity be monitored by system safety engineering to verify that these requirements and criteria are incorporated in the design. It is important that someone with system safety competence "flow down" the safety requirements throughout the "specification tree". It is the lower level specifications (C typically) that are the detailed design criteria which get translated into the design. If safety requirements are not properly incorporated at this level they will be missed in the design process.
- **Operational or Test Location**. The contractor must demonstrate in his SSPP, Test Plans, and Logistics documentation that the SSP does not end at the factory door. The contractor must consider safety during test programs and planned support for government or system integrator activates.

Management and Planning of an SSP

Four primary drivers of an effective SSP are:

- Personnel qualifications and experience
- Managerial authority and control
- Effective program planning
- Sufficient resources.

If one of these is missing or insufficient, the program will fail.

Personnel Qualifications and Experience. To provide decision makers with competent hazard risk assessments, the FAA's program/assistant manager must insist that the contractor have qualified, responsive system safety management and technical personnel. This is necessary since the contractor's system safety manager is the one who certifies, for his employer, that all safety requirements have been met. Necessary qualifications vary from program to program as discussed in Chapter 5, Table 5-2

FAA sponsored programs are either the procurement of hardware/systems or services. In the former, the role of the evaluator is often to determine if bidding contractors have the capability (and track history) to meet contractual requirements. In the latter case of acquisition of services, the evaluation may be more focused on the qualification of individuals. In either case, the evaluator is usually provided resumes for proposed individuals, in others more generic "job descriptions" that establish minimum qualifications for well defined "charters".

A useful approach to evaluating either proposed key positions resumes or job descriptions is to utilize a "Job Analysis Worksheet". A sample is included as Figure 6-5. It is appropriate to require key resumes (and an obligation to use the associated individuals post award) in the Request for Proposal's (RFP) instructions to bidders. A Job Analysis Worksheet is a checklist of desired job requirements per required skill level reflecting the knowledge, skills, and abilities (KSA) necessary to implement the program successfully. The submitted key resumes or alternatively position descriptions is reviewed against the job requirements as reflected in each KSA to determine if the candidate meets the FAA's requirements. A sample position description is provided as Exhibit 6-4.

Figure 6-5 Sample Job Analysis Worksheet: System Safety Manager

Knowledge, Skills, and Abilities (KSA)

1 Knowledge and ability to manage interrelationships of all components of an SSP in support of both management and engineering activities. This includes planning, implementation, and authorization of monetary and personnel resources.
2 Knowledge of theoretical and practical engineering principles and techniques.
3 Knowledge of systems
4 Knowledge of operational and maintenance environments.
5 Knowledge of management concepts and techniques.
6 Knowledge of this life-cycle acquisition process.
7 Ability to apply fundamentals of diversified engineering disciplines to achieve system safety engineering objectives.
8 .Ability to adapt and apply system safety analytical methods and techniques to related scientific disciplines.
9 Ability to do independent research on complex systems to apply safety criteria.
10 Skill in the organization, analysis, interpretation, and evaluation of scientific/engineering data in the recognition and solution of safety-related engineering problems.
11 Skill in written and oral communication.
12 Ability to keep abreast of changes in scientific knowledge and engineering technology and apply new information to the solution of engineering problems.

Major Job Requirements

1 Acts as agent of the program manager for all system safety aspects of the program. Provides monthly briefings to the program management on the status of the SSP.

2 Serves as system safety manager for safety engineering functions of major programs. (KSA 1 through 11)

3 Manages activities which review and evaluate information related to types and location of hazards. (KSA 1,2,3,4,7,9,12)

4 Manages activities to perform extensive engineering studies to determine hazard levels and to propose solutions. (KSA 1,2,6,7,8,9,11)

5 Manages the development of system guidelines and techniques for new/developing systems and emerging technologies. (KSA 6,7,8,9,10,12)

6 Provides system safety engineering expertise to identify/solve multidisciplinary problems involving state-of-the-art technology. (KSA 2,7,8,9,10,12)

TITLE: ENGINEER, STAFF - SYSTEM SAFETY

Qualifications

Minimum of a baccalaureate degree in an engineering, applied science, safety or other closely related degree appropriate to system safety. Some education or experience in Business Administration is desirable; Certification as a Professional Engineer or as a Certified Safety Professional (CSP) licensed as a PE, preferably in safety engineering, or credentials as a CSP in system safety aspects. Approximately 10 years diversified experience in various aspects of system safety is desired; or demonstrated capability through previous experience and education to perform successfully the duties and responsibilities shown below.

Duties and Responsibilities

Serve as a professional authority for the SSP covering the planning, designing, producing, testing, operating, and maintaining of product systems and associated support equipment. May be assigned to small programs as system safety representative with duties as described below.

Review initial product system designs and advise design personnel concerning incorporation of safety requirements into product system, support equipment, test and operational facilities based on safety standards, prior experience, and data associated with preliminary testing of these items.

Assure a cooperative working relationship and exchange of operational and design safety data with government regulatory bodies, customers, and other companies engaged in the development and manufacture of aerospace systems. Act as a company representative for various customer and industry operational and design safety activities and assist in the planning and conducting of safety conferences.

Evaluate new or modified product systems, to formulate training programs, for updating operating crews and indoctrinating new employees in systems test and operational procedures. Establish training programs reflecting latest safety concepts, techniques, and procedures.

Direct investigations of accidents involving design, test, operation, and maintenance of product systems and associated facilities, and present detailed analysis to concerned customer and company personnel. Collect, analyze, and interpret data on malfunctions and safety personnel, at all organizational levels; and keep informed of latest developments, resulting from investigation findings, affecting design specifications or test and operational techniques. Collaborate with functional safety organizations in order to set and maintain safety standards. Recommend changes to design, operating procedures, test and operational facilities and other affected areas; or other remedial action based on accident investigation findings or statistical analysis to ensure maximum compliance with appropriate safety standards.

Coordinate with line departments to obtain technical and personnel resources required to implement and maintain safety program requirements.

Figure 6-6 Sample Job Description

6.3.3 Negotiation

Negotiation consists of fact finding, discussion, and bargaining. The process leads to several benefits:

- A full understanding of the safety requirement by the contractor and of the contractor's commitment to meeting and understanding of these requirements
- Correction of proposed SSP deficiencies.
- A mutual understanding of any safety tradeoffs that may be necessary. Trade-off parameters include performance, schedule, logistics support, and costs.

The negotiation process is the last chance to insure that all necessary safety program and safety risk criteria is incorporated in the contract. It permits both the FAA and the contractor to clear-up different requirement interpretations and implementation conflicts. Just as importantly, the contractor and the FAA can maximize effectiveness for planned safety program cost expenditures. Delivering System Safety Assessment Reports (SSAR) or Safety Engineering Reports (SER), for example, in a specific media format, e.g., a desktop publishing package may be an unexpected cost driver for a company that has standardized on an office suite such as MS or Corel Office. Similarly, when approval of SARs is specified, the contractor needs to cost assumed rework. If the assumption is high, the FAA may choose to forgo approval on early program submittals and substitute comments instead. There are obvious risks associated with foregoing approval on deliverables.

6.4 Managing Contractor System Safety (Contract Oversight)

Proactive Government participation in the contractor's system safety program is a critical path in achieving confidence in the effectiveness of the contractors system safety program and accuracy and coverage of safety analyses. The appropriate issues are:

- Contract direction can only be provided through the Government contracting office.
- Government personnel must provided corrective feedback, as needed, in such a manner that does not discourage candor and sharing of information. To that end, participation in frequent Technical Information Meetings (TIMs) and other activities such as Hazard Record Review Boards is a positive action.
- Formal review with official feedback is primarily provided through Major Program Milestones (such as a Critical Design Review , CDR) and the contract deliverables, e.g., S/SHA and SAR.

6.4.1 Major Program Milestones

System Design Review (SDR)/SDR Safety Review

For SDR, the following should be available for review:

- SSPP
- Work breakdown of system safety tasks, subtasks, and manpower

- Overview of system and mission, including safety-critical systems, subsystems, and their interrelationship with mission operations
- Proposed support equipment
- Operational scenarios
- Tabulation of hazards identified
- Review of initial checklist.

The following key points should be considered in the review:

- Identification of key safety people in the contractor's organization
- Authority and responsibility of key safety positions
- Key system safety personnel qualifications
- Safety program milestones
- Proposed hazard analysis methods
- Control system for identification, recording, tracking, resolution, and closeout of problems.
- Contractor staffing and monetary resources.
- The nature of the hazards the applicable to the system application and design. For example, on a recent program the contractor decided that failure to detect weather conditions couldn't be a hazard for a ground based system. In this case, the weather protection system provided information to aircraft so it was a hazardous condition. In another case, hazard analyses were planned only for hardware and the FAA safety team leader was concerned about software hazard mitigation.

Minimum requirements for a successful SSP are:

- Contractor's demonstration of capability to perform system safety activities in compliance with contractual requirements such as tailored MIL-STD-882 and/or the FAA SSMP.
- Contractor's demonstration of understanding of applicability of safety requirements and specific hazard identification

Preliminary Design Review (PDR)/PDR Safety Review

This phase occurs early in system development prior to the detailed design process. It measures the progress and adequacy of the design approach and establishes physical and functional interfaces between the system and other systems, facilities, and support equipment.

The safety review performed at PDR considers the identified hazards and looks at the intended design controls. The cognizant FAA system safety manager usually reviews the following documents at this point:

- Preliminary Hazard or Accident Risk Assessment Reports approved by both the contractor's program manager and system safety manager
- Draft preliminary checklists
- Scenarios, including planned operations
- Current hazards lists and risk assessments
- System and subsystem descriptions
- Other hazard reports.

During the documentation review, the following key points should be checked:

- Preliminary hazards analysis activities
- Effectiveness of verification effort
- Changes to the SDR baseline
- Proposed operations and ground support equipment
- Proposed facilities design.

Finally, the government system safety manager must determine if the following requirements have been met:

- Preliminary design meets requirements established by the negotiated contract
- Hazards, compatible with the level of system development have been identified
- Proposed hazard controls and verification methods are adequate
- Safety-critical interfaces have been established and properly analyzed.
- A Hazard Tracking and Incident Reporting System are in place.

Critical Design Review (CDR)/CDR Safety Review

CDR occurs when the detail design is complete and fabrication drawings are ready to release. The Safety CDR centers on the final hazard controls incorporation into the final design and intended verification techniques. Requirements compliance is assessed. By this review, some design related safety hazards/risks will be closed, however, some hazards/risks may remain open with management's cognizance. The information sources to review are:

- SER and/or DAR verified by program manager
- Operating and support hazard analysis approach
- Operating timeline matrices.
- Operational scenarios identifying:
  - Hazardous operations
  - Support equipment planning and preliminary design

  - Proposed procedures list
  - Proposed operational hazard controls.
- Hazard Tracking and Risk Resolution Results

The key points for evaluation are:

- System hazard analysis activities
- Operating and support hazard analysis activities
- Training requirements
- Personnel protection requirements
- Safety-critical support equipment design
- Effectiveness of design hazard controls
- Interface analysis.

The requirements that must be met at CDR for a successful program are:

- Final design meets negotiated contractual requirements
- Hazard controls have been implemented and verification methods defined
- Support equipment preliminary design hazards and controls have been identified
- All interface analyses are complete
- Contractor certification that all contractual design requirements are met.

Pre-operational Safety Review

At this review, the contractor presents the final hazard reports with controls incorporated and verified for both the operational hardware and the support equipment. Ideally, procedures and technical orders are complete; however, if they are not, then a tracking system must ensure that controls are incorporated and safety validation is performed prior to first use. The following information sources should be reviewed:

- Completed and verified operating and support hazard analyses (O&SHA)
- Approved change proposals
- Completed and verified system hazards analyses
- Completed and verified checklists
- Contractor's hazard closeout logs
- Summary of hazards analysis results and assessment of residual risk

The key points for evaluation are:

- Operating and support hazards analysis

- Changes to CDR baseline
- System hazard analysis
- Closeout of action items
- Assessment of residual risk.

The requirements for a successful safety program at the pre-operational phase are:

- Acceptable systems and operational hazards analysis
- Operational procedures/technical orders are complete and verified
- All hazards are controlled effectively and controls verified as effective
- Checklists are completed and actions verified
- All hazard records in the SAR database are reviewed and the residual risk accepted by the MA.
- Demonstrated a complete validation, verification, and if applicable certification program, to the FAA

System Safety Program Reviews

SSP status and results to date should be on the agenda of all major program milestone reviews such as the preliminary and critical design reviews. The criticality of some systems under development may be important enough for the managing authority to require special safety reviews or audits. Such special meetings are appropriate for many National Airspace System (NAS) programs.

The purpose of such meetings is to provide greater emphasis on the details of the SSP progress and analyses than is practical at a major milestone review. Given that they are required, the schedule duration, the pace of development, and the phase of the program should determine the frequency. One scenario for a two-year full-scale development program might include a kick-off safety meeting shortly after contract award and one safety review prior to Preliminary Design Review (PDR). Special meetings during the T&E phase would be held when test results suggest a need. Since one of the primary purposes of a special safety review is to discuss safety program tasks in greater detail than is compatible with a major program milestone schedule, some cost savings may be achieved by requesting parallel safety sessions at a major milestone review. This approach permits the desired detail to be discussed without accumulating the costs of an independent meeting.

All program reviews and audits provide an opportunity to review and assign action items and to explore other areas of concern. A mutually acceptable agenda/checklist should be negotiated in advance of the meeting to ensure all system safety open items are covered and that all participants are prepared for meaningful discussions.

SSP reviews to be specified in the SOW shall include, as applicable:

6.4.2 System Safety Working Groups/Work Group Support

The acquisition of expensive, complex, or critical systems, equipment, or major facilities requires considerable interaction between the integration contractor and associate contractors simultaneously. In these situations, the managing authority may require the formation of a System Safety Working Group/System Safety Working Group (SSWG). The SSWG is a formally chartered group of staff, representing organizations participating in the acquisition process. This group exists to assist the managing authority system program manager in achieving the system safety objectives. Contractor support of an SSWG is useful and may be necessary to ensure procured hardware or software is acceptably free from risks that could injure personnel or cause unnecessary damage or loss of resources.

The contractor, as an active member of the SSWG, may support the managing authority by providing or supporting presentations to the government certifying activities such as phase safety reviews or safety review boards. The following list provides management with SSWG support options to selectively impose on contractors:

- Present the contractor safety program status, including results of design or operations risk
- Summarize hazard analyses, including identification of problems and status of resolution
- Present results of analyses of prior mishaps or accidents, and hazardous malfunctions, including recommendations and action taken to prevent recurrences
- Respond to action items assigned by the chairman of the SSWG
- Develop and validate system safety requirements and criteria applicable to the program
- Identify safety deficiencies of the program and providing recommendations for corrective actions or prevention of recurrence
- Plan and coordinate support for a required certification process
- Document and distribute meeting agendas and minutes

SSWG details to be specified in the SOW should include, as applicable:

- Contractor membership requirements and role assignments (e.g., recorder, member, alternate, or technical advisor)
- Frequency or total number SSWG meetings and probable locations
- Specific SSWG support tasks required

6.4.3 Hazard Tracking and Risk Resolution

Each program with or without an active system safety effort can identify system hazards that require control to an acceptable risk level. A system is required to document and track hazards and resolution progress to ensure that each is controlled to an acceptable risk level.

Hazard tracking need not be a complex procedure. Any hazard tracking tool that tracks the information contained in Section 6.2 and complies with the SSMP and SSPP is acceptable for hazard tracking in the FAA at the program level. The managing authority, the system integrator, or each contractor may maintain the Safety Action Record (SAR) database. Each risk that meets or exceeds the threshold specified by the

managing authority should be entered into the SAR database when first identified. Each action taken to eliminate the risk or reduce the associated risk is documented. Management will detail the procedure for closing out the hazard or acceptance of any residual risk. The SAR may be documented and delivered as part of the system safety progress summary using, Safety Engineering Report, or it can be included as part of an overall program engineering/management report.

Management has considerable flexibility in choosing a closed loop system to closing out a risk. See Figure 6-7. The key is the maintenance and accessibility of a SAR. The contractor can be required to establish the SAR and include within it a description of the specific corrective action taken to downgrade a medium and high risk hazards. The corrective action details and log updates can be included in monthly reports, subsequent data submissions, and at major program milestones.

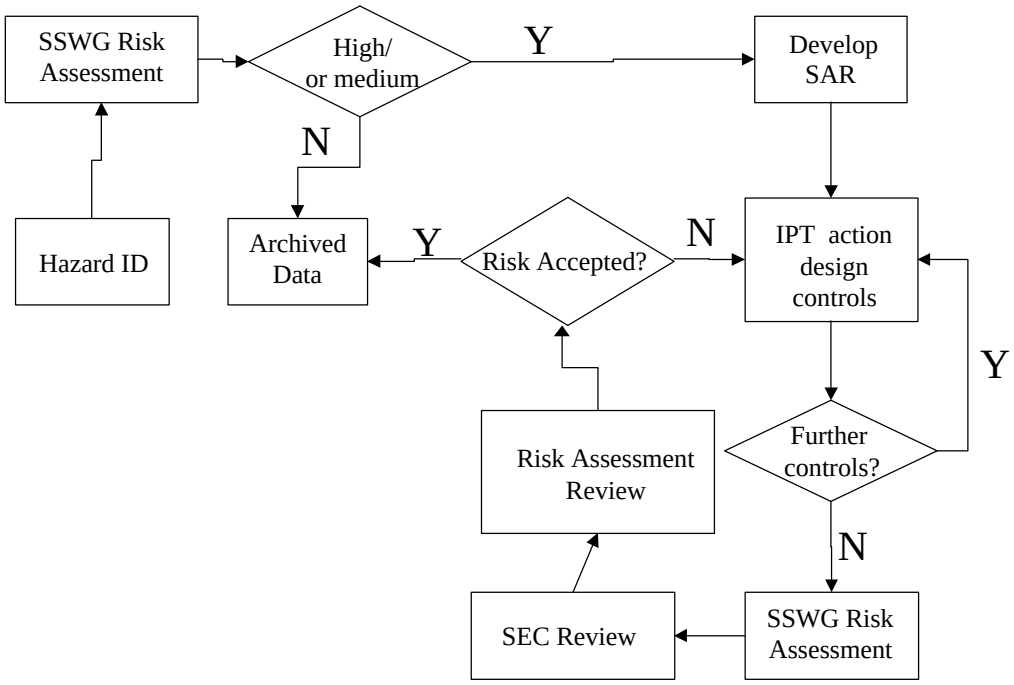

Figure 6-7: Hazard Resolution System(s)

Management can review and approve/disapprove the corrective action or its impact by mail, at major program milestones, SSWG meetings, safety reviews board meetings, or any other engineering control process found to be effective. Although the method selected is flexible, a "paper trail" reflecting the identification of medium and high risk, a summary of the corrective action alternatives considered, conclusions, and the names of the review team is desirable.

Details to be specified in the SOW shall include, as applicable, the following:

- Hazard threshold for inclusion in the hazard log
- Complete set of data required on the hazard log, including format

- Procedures to record hazards into the log and the level of detail of the log entry
- Procedure by which the contractor shall obtain close out or risk acceptance by the MA for each hazard

6.4.4 System Safety Progress Report

Comprehensive and timely communication between management, the system integrator (when applicable), and each contractor is critical to an effective SSP. The system safety progress report provides a periodic written report of the status of system safety engineering and management activities. This status report may be submitted monthly or quarterly. It can be formatted and delivered as a Safety Engineering Report, or it can be included as part of an overall program engineering/management report.

The contractor may prepare a periodic system safety progress report summarizing general progress made relative to the SSP during the specified reporting period and projected work for the next reporting period. The report should contain the following information.

- A brief summary of activities, progress, and status of the safety effort in relation to the scheduled program milestones. It should include progress toward completion of safety data prepared or in work.
- Newly recognized significant hazards and significant changes in the degree of control of the remaining known hazards.
- Status of all recommended corrective actions not yet implemented.
- Significant cost and schedules changes that impact the safety program.
- Discussion of contractor documentation reviewed by SSWG during the reporting period. Indicate whether the documents were acceptable for safety content and whether or not inputs to improve the safety posture were made.
- Proposed agenda items for the next SSWG meeting, if such groups are formed.