

FAA-1999-5535-4

54129



U.S. Department
of Transportation
**Federal Aviation
Administration**

DEPT. OF TRANSPORTATION
DOCUMENT SECTION

99 APR 26 AM 9:09

Advisory Circular

AC 431.35-2

DRAFT

REUSABLE LAUNCH VEHICLE

System Safety Process

April 16, 1999

U.S. DEPARTMENT OF TRANSPORTATION
Federal Aviation Administration
Washington, DC

Preface

This Advisory Circular is provided for guidance and information on applying a systematic and logical safety process methodology for the identification and control of public safety hazards associated with the operation of Reusable Launch Vehicle Systems. The methods and procedures described herein provide an acceptable approach to system safety methodology. Other approaches that fulfill regulatory objectives may be acceptable to the Federal Aviation Administration.

TABLE OF CONTENTS

Preface	
Table of Contents	ii
1.0 PURPOSE.	1
2.0 REFERENCES	1
3. BACKGROUND.	
4. REQUEST FOR INFORMATION	1
5. GENERAL	1
6. SYSTEM SAFETY ENGINEERING PROCESS	3
7. VALIDATION OF SAFETY CRITICAL SYSTEMS	4
7.1 ANALYSES	7
7.2 GROUND TESTS	8
7.3 FLIGHT TESTS	9
7.4 PERFORMANCE AND RELIABILITY DATA	11
7.5 OPERATIONAL CONTROLS	12
8. DETERMINATION OF ROSK TO THE PUBLIC	14
9. DETERMINATION OF NEED FOR ADDITIONAL RISK MITIGATION	14
ATTACHMENT 1. SYSTEM SAFETY ENGINEERING PROCESS	
ATTACHMENT 2. SAMPLE REUSABLE LAUNCH VEHICLE SYSTEM SAFETY PROGRAM PLAN	

1. PURPOSE. This Advisory Circular (AC) provides guidance and information concerning the application of a systematic and logical safety process methodology for the identification and control of public safety hazards associated with the operation of Reusable Launch Vehicle (RLV) Systems. The methods and procedures described herein provide an acceptable approach to system safety methodology. Other approaches that fulfill regulatory objectives may be acceptable to the Federal Aviation Administration.

2. REFERENCES. Commercial Space Transportation, FAA, DOT, Part 415, 43 1.

3. BACKGROUND. This AC provides a description of a System Safety Engineering Process that may be applied for the identification and control of hazards associated with the launch and reentry of Reusable Launch Vehicle systems. This type of process may be tailored to various RLV concepts. Early and frequent pre-application consultation and coordination with the FAA is critical for all projects.

4. REQUEST FOR INFORMATION. If there are questions, or more information is desired about this AC, write or call FAA: Office of Commercial Space Transportation, AST: 800 Independence Avenue, SW: Washington, DC 20591; (202) 267- 8602.

5. GENERAL

An RLV applicant will be expected to apply a disciplined, systematic, and logical safety process methodology for the identification and control of hazards associated with its launch and/or reentry systems.

Explanation of Methodology of General System Safety Process:

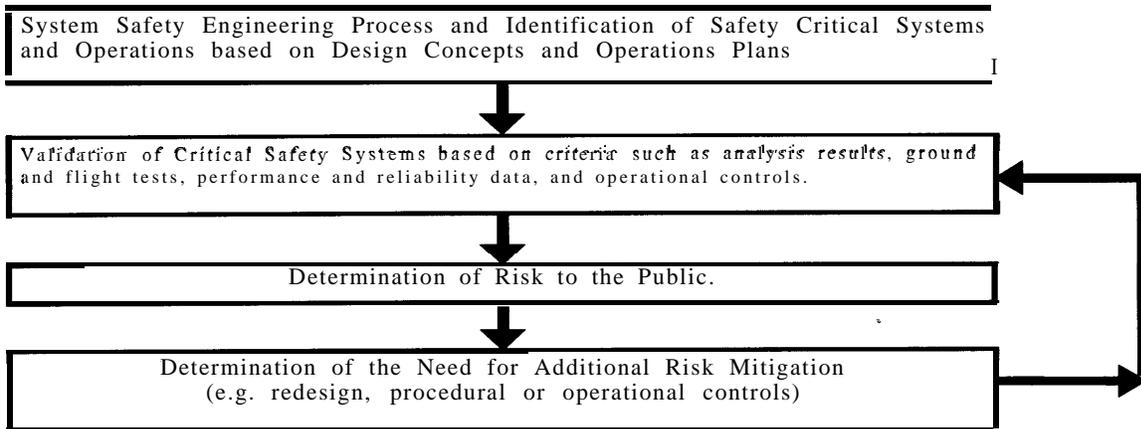


FIGURE 1A: SAFETY PROCESS FLOW

The Applicant should use the System Safety Engineering Process, or an equivalent that also includes a Risk Analysis, to show that it meets the system safety requirements of Part 43 1. Outlined above is an acceptable system safety process methodology, indicating 4 basic elements. The process flow depicted in Figure 1A represents a top level outline of the

traditional systems safety engineering process successfully used by the Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA) for decades, modified to focus only on risks to public safety. The process depicted is ongoing until all potential risks have been mitigated to an acceptable level. The System Safety Engineering Process used should be similar to that reflected in Military Standard 882C (MIL-STD-882C), or the System Safety Analysis Handbook (a System Safety Society Standard), or FAA Advisory Circular AC No: 25.1309 titled “System Design and Analysis”.

The use of a systematic process for the identification and control of safety critical systems and operations also provides the foundation supporting the Expected Casualty analysis. (See AC 43 1.35-1) Without a process that helps assure a disciplined approach to the design, manufacture, integration, test, and operation of a system, it will be very difficult to establish any confidence in the probabilities of success and failure provided for the Expected Casualty analysis. It is also noted that although the application of a system safety process is extremely important in creating a strong foundation for assuring the safety of a system, it does not, in and of itself, assure public safety. The application of the system safety engineering approach in combination with the expected casualty analysis (See AC 43 1.35-1) and the mandatory operational controls defined in regulations intended to help ensure an adequate level of public safety. See Figure 1B.

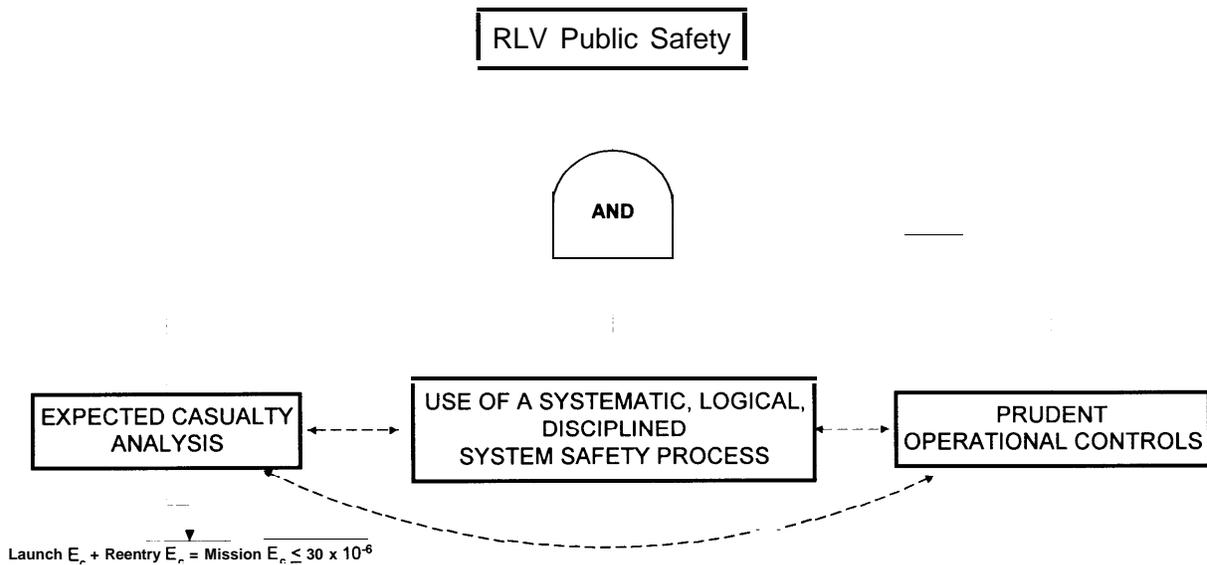


Figure 1B: RLV Public Safety

A more detailed description of an acceptable System Safety Engineering Process and a Flow Chart showing the relationship of the process to system development are included in the attached instructional tutorial (Attachment 1). While Risk Analysis is mentioned in the same attachment, a more detailed description of the analysis and measurement of risk (via expected casualty) can be found in AC 43 1.35-1.

The following discussion provides examples of an acceptable system safety process and analysis techniques, examples of safety critical systems, and typical analytical and test procedures used to verify safety critical systems and potential operational controls/constraints.

6. SYSTEM SAFETY ENGINEERING PROCESS

The System Safety Engineering Process is the structured application of system safety engineering and management principles, criteria, and techniques to address safety within the constraints of operational effectiveness, time, and cost throughout all phases of a system's life cycle. The intent of the System Safety Engineering Process is to identify, eliminate, or control hazards to acceptable levels of risk throughout a system's life cycle.

This process is performed by the vehicle developer/operator. Because of the complexity and variety of vehicle concepts and operations, such a process can help ensure that all elements affecting public safety are considered and addressed. Without such a process, very detailed requirements would have to be imposed on all systems and operations, to ensure that all potential hazards have been addressed which could have the undesired effect of restricting design alternatives and innovation or could effectively dictate design and operations concepts.

The process (as described in Mil Std 882C) includes a System Safety Program Plan (SSPP). The SSPP (or its equivalent) provides a description of the strategy by which recognized and accepted safety standards and requirements, including organizational responsibilities, resources, methods of accomplishment, milestones, and levels of effort, are to be tailored and integrated with other system engineering functions. The SSPP lays out a disciplined, systematic methodology that ensures all hazards – all events and system failures (probability and consequence) that contribute to expected casualty – are identified and eliminated, or that their probability of occurrence is reduced to acceptable levels of risk.

The SSPP should indicate the methods employed for identifying hazards, such as Preliminary Hazards Analysis (PHA), Subsystem Hazard Analysis (SSHA), Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis. Risk Mitigation Measures are likewise identified in the plan. These include avoidance, design/redesign, process/procedures and operational rules and constraints. A "Generic Sample RLV System Safety Program Plan" is included as attachment 2 of this document.

The System Safety Engineering Process identifies the safety critical systems. For the purposes of this AC, safety critical systems are defined as any system or subsystem whose performance or reliability can affect public health, safety and safety of property. Such systems, whether they directly or indirectly affect the flight of the vehicle, may or may not be critical depending on other factors such as flight path and vehicle ability to reach populated areas. For this reason, it is important to analyze each system for each phase of the vehicle mission from ground operations and launch through reentry and landing operations. Examples of potentially safety critical systems that may be identified through the system safety analysis process using PHA or other hazard analysis techniques may include, but are not limited to:

- Structure/integrity of main structure

- Thermal Protection System (e.g., ablative coating)
- Temperature Control System (if needed to control environment for other critical systems)
- Main Propulsion System
- Propellant Tanks
- Power Systems
- Propellant Dumping System
- Landing Systems
- Reentry Propulsion System
- Guidance, Navigation and Control System(s), Critical Avionics (Hardware and Software) - includes Attitude, Thrust and Aerodynamic Control Systems
- Health Monitoring System (hardware and software)
- Flight Safety System (FSS)
- Flight Dynamics (ascent and reentry) for stability (including separation dynamics) and maneuverability
- Ground Based Flight Safety Systems (if any) including telemetry, tracking and command and control systems
- Depending on the concept, additional “systems” might include pilot and life support systems and landing systems if they materially affect public health and safety
- Others identified through hazard analysis

7. VALIDATION OF SAFETY CRITICAL SYSTEMS

Through the system safety process, the applicant demonstrates that the proposed vehicle design and operations satisfy regulatory requirements and that the system is capable of surviving and performing safely in all operating environments including launch, orbit, reentry and recovery. Documentation must show adequate design, proper assembly, and vehicle control during all flight phases. Documentation is expected to consist of design information and drawings, analyses, test reports, previous program experience, and quality assurance plans and records.

The FAA uses a pre-application consultation process to help a potential applicant to understand what must be documented and to help identify potential issues with an applicant’s proposed activities that could preclude its obtaining a license. This process is especially important for RLV systems because most are using unique technology and operating concepts. The pre-application process should be initiated by the applicant early in their system development (if possible during the operations concept definition phase) and maintained until their formal license application is completed. This pre-application process should be used to provide the FAA with an understanding of the safety processes to be used, the safety critical systems identified, analysis and test plan development, analysis and test results, operations planning and flight rules development.

Analyses may be acceptable as the primary validation methodology in those instances where the flight regime cannot be simulated by tests, provided there is appropriate technical rationale and justification.

Qualification tests, as referenced in the safety demonstration process and the System Safety Program Plan, are normally conducted to environments higher than expected. For example, ELVs' Flight Safety Systems (FSS) are qualified to environments a factor of two or higher than expected. (See Figure 2)

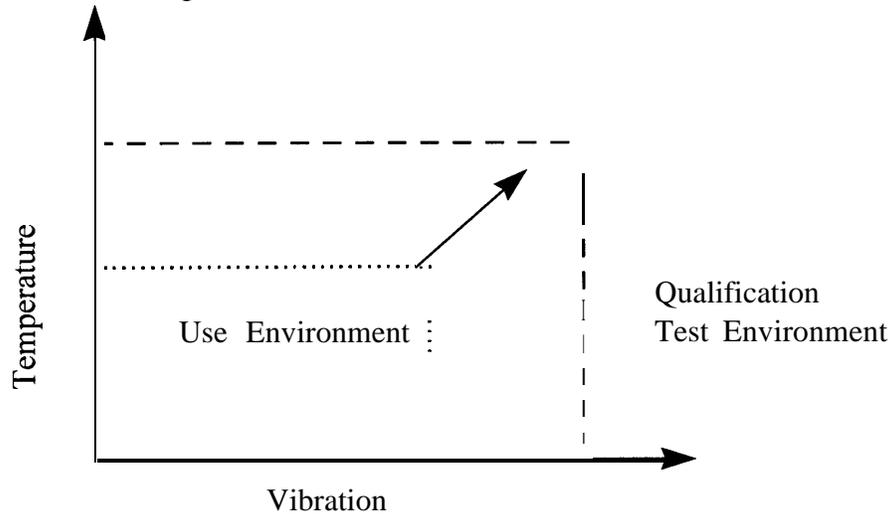


Figure 2. Relationship of Use Environment to Qualification Test Environment

These tests are conducted to demonstrate performance and adequate design margins and may be in the form of multi-environmental ground tests, tests to failure, and special flight tests. Such tests are normally preceded with detailed test plans and followed by test reports.¹ In addition, Quality assurance (QA) records are useful in establishing verification of both design adequacy and vehicle assembly and checkout (workmanship).

¹ Test plans are important elements of the ground and flight test programs. Such plans define, in advance, the nature of the test (what is being tested and what the test is intended to demonstrate with respect to system functioning, system performance and system reliability). The test plan should be consistent with the claims and purpose of the test and wherever appropriate, depending on the purpose of the test, clearly defined criteria for pass and fail should be identified. A well defined test plan and accompanying test report may replace observation by the FAA.

The following matrix identifies example approaches that may be employed to validate acceptance for critical systems. Examples of types of analyses, ground tests, and flight tests are provided following this matrix. (Note: Quality Assurance programs and associated records are essential where analysis or testing, covering all critical systems, are involved.)

Candidate Critical Systems	Analyses	Ground Test	Flight Test
Structure/Integrity of Main Structure	X	X	P
Thermal Protection	X	P	P
Environmental Control (temp, humidity)	X	X	X
Propulsion: Main, Auxiliary and Reentry (de-orbit)	X	P	P
Propellant Tank Pressurization	X	X	P
GN&C, Critical Avionics *; includes de-orbit targeting (e.g., star-tracker, GPS)	X	X	X
Health Monitoring *	X	X	X
Flight Safety System (FSS)*	X	X	X
Recovery and Landing	X	P	P
Ordnance (other than Safety)	X	X	X
Electrical and Power	X	X	X
Telemetry and Tracking and Command*	X	X	X
Flight Control (ascent, separation, reentry) *	X	X	X
FSS Ground Support Equipment (if any) *	X	X	N/A

P - partial; cannot satisfy all aspects

X - if in sufficient detail when combined with test results or selected analyses

* - includes both hardware and software

7.1 ANALYSES

There are various types of analyses that may be appropriate to help validate the viability of a critical system or component. The following provides examples of some types of critical systems analysis methodologies and tools. Again these are *only examples* and should not be construed as the only analyses or software tools which may be used to validate a specific system for a specific operational environment, nor should it be interpreted that all of these example analysis and software tools will be necessary to validate a specific system.

Mechanical Structures and Components (Vehicle Structure, Pressurization, Propulsion System including engine frame thrust points, Ground Support Equipment)

- Types of Analyses: Structural Loads, Thermal, Fracture Mechanics, Fatigue, Form Fit & Function
- Software Tools for Analyses: Nastran, Algor, Computational Fluid Dynamics codes, CAD/CAM

Thermal Protection System

- Types of Analyses for TPS and Bonding Material: Transient and Steady State Temperature Analyses, Heat Load, and Heating and Ablative Analyses.
- Software Tools for Analyses: SINDA by Network Analysis Inc.

Electrical/Electronic Systems & Components (Electrical, Guidance, Tracking, Telemetry, Navigation, Communication, FSS, Ordnance, Flight Control and Recovery)

- Types of Analyses: Reliability, FMEA, Single Failure Point, Sneak Circuit, Fault Tree, Functional Analysis, Plume effects
- Software Tools for Analyses: MathCad, Relx, FaultrEase

Propulsion Systems (Propulsion, FSS, Ordnance, Flight Control)

- Types of Analyses: Analytical Simulation of nominal launch and abort sequences for Main Engines, Orbital Maneuvering System (including restart for reentry-burn) and Attitude Control System; capacity analysis for consumables; Plume Flow Field Modeling
- Software Tools for Analyses: Nastran, Algor, SPF-III, SINDA

Aerodynamics (Structure, Thermal, Recovery)

- Types of Analyses: Lift, Drag, Stability, Heating, Performance, Dispersion, Plume effects
- Software Tools for Analyses: Post 3/6 DOF, Computational Fluid Dynamics Codes, Monte Carlo Simulation Codes

Software (Guidance, Tracking & Telemetry & Command, FSS, Flight Control and Recovery)

- Types of Analyses: Fault Tree, Fault Tolerance, Software Safety (including abort logic), Voting Protocol Dead Code, Loops, and Unnecessary Code
- Validation Methodologies, such as ISO 9000-3 ²

² ISO 9000-3 is used in the design, development, and maintenance of software. Its purpose is to help produce software products that meet the customers' needs and expectations. It does so by explaining how to

7.2 GROUND TESTS

For the purposes of this AC, ground tests include all testing and inspections performed by the applicant prior to flight, including qualification, acceptance and system testing. It is anticipated that an applicant will perform various types of ground tests to validate the capability of critical systems and components. The following provides examples of some types of critical systems validation ground tests. Again these are *only examples* and should not be construed as the only types of ground tests which may be used to validate a specific system for a specific operational environment, nor should it be interpreted that all of these example ground tests will be necessary to validate a specific system.

Mechanical Systems and Components (Vehicle Structure, Pressurization, Propulsion System including engine frame thrust points, Ground Support Equipment)

- Types of Tests: Load, Vibration (dynamic and modal), Shock, Thermal, Acoustic, Hydro-static, Pressure, Leak, Fatigue, X-ray, Center of Gravity, Mass Properties, Moment of Inertia, Static Firing, Bruceton Ordnance, Balance, Test to Failure (simulating non-nominal flight conditions), Non-Destructive Inspections

Electrical/Electronic Systems (Electrical, Guidance, Tracking, Telemetry and Command, Flight Safety System (FSS), Ordnance, Flight Control and Recovery)

- Types of Tests: Functional, Power/Frequency Deviation, Thermal Vacuum, Vibration, Shock, Acceleration, X-ray, recovery under component failures, abort simulations, TDRSS integration testing (up to and including pre-launch testing with flight vehicle)

Propulsion Systems (Propulsion, FSS, Ordnance, Flight Control)

- Types of Tests: Simulation of nominal launch and abort sequences for engines (including restart, if applicable), Orbital Maneuvering System (including restart for reentry-burn) and Attitude Control System; Environmental testing (Thermal, Vibration, Shock, etc.)

Thermal Protection System

- Types of Tests (for TPS and bonding material): Thermal, Vibration, Humidity, Vacuum, Shock

Aerodynamics (Structure, Thermal, Recovery)

- Types of Tests: Wind Tunnel, Arc Jet, Drop Tests (Landing Systems)

Software (Electrical, Guidance, Tracking, Telemetry, Command, FSS, Ordnance, Flight Control and Recovery)

- Types of Tests: Functional, Fault Tolerance, Cycle Time, Simulation, Fault Response, Independent Verification and Validation, Timing, Voting Protocol,

control the quality of both products and the processes that produce these products. For software product quality, the standard highlights four measures: specification, code reviews, software testing and measurements.

Abort sequences (flight and in-orbit) under non-nominal conditions with multiple system failures, Integrated Systems Tests

7.3 FLIGHT TESTS

If an applicant's System Safety Plan includes a flight test program, then a considerable amount of planning is needed to define the flight test program that will establish the performance capabilities of the vehicle for routine and repetitive commercial operations. When flight testing is indicated, a flight test plan will be needed to demonstrate that the RLV's proposed method of operations is acceptable and will not be a hazard to the public health, safety and safety of property.

The purpose of flight-testing is to verify the system performance, validate the design, identify system deficiencies, and demonstrate safe operations. Experience repeatedly shows that while necessary and important, analyses and ground tests cannot and do not uncover all potential safety issues associated with new launch systems. Even in circumstances where all known/identified safety critical functions can be exercised and validated on the ground, there is still the remaining concern with unrecognized or unknown interactions ("the unknown unknowns").

The structure of the test program will identify the flight test framework and test objectives, establish the duration and extent of testing; identify the vehicle's critical systems, identify the data to be collected, and detail planned responses to nominal and unsatisfactory test results.

Test flight information includes verification of stability, controllability, and the proper functioning of the vehicle components throughout the planned sequence of events for the flight. All critical flight parameters should be recorded during flight. A post-flight comparative analysis of predicted versus actual test flight data is a crucial tool in validating safety critical performance. Below are examples of items from each test flight that may be needed to verify the safety of a reusable launch vehicle. Listed with each item are examples of what test-flight data should be monitored or recorded during the flight and assessed post-flight:

- Vehicle/stage launch phase: Stability and controllability during powered phase of flight.
 - Vehicle stage individual rocket motor ignition timing, updates on propellant flow rates, chamber temperature, chamber pressure, and burn duration, mixture ratio, thrust, specific impulse (ISP)
 - Vehicle stage trajectory data (vehicle position, velocity, altitudes and attitude rates, roll, pitch, yaw attitudes)
 - Vehicle stage Attitude, Guidance and Control system activities
 - Functional performance of the Vehicle Health Monitoring System
 - Functional performance of the Flight Safety System/Safe Abort System
 - Electrical power, and other critical consumables, usage and reserves (i.e. gases, fluids, etc.. .)

- Actual thermal and vibroacoustic environment
- Actual structural loads environment
- Staging/separation phase of boost and upper stages: Stable shutdown of engines, and nominal separation of the booster & upper stages.
 - Separation activity (timestamp, i.e., separation shock loads, and dynamics between stamps)
 - Functional performance of the Vehicle Health Monitoring System
 - Electrical power, and other critical consumables, usage and reserves (i.e. gases, fluids, etc.. .)
 - Functional performance of the Flight Safety System/Safe Abort System
- Booster stage turn-around (re-orientation) or “loft” maneuver phase (if applicable).
 - Rocket motor re-start (if applicable): timing, updates on propellant flow rates, chamber temperature, chamber pressure, bum duration, mixture ratio, thrust, ISP
 - Attitude, Guidance and Control system activities
 - Actual structural loads environment
 - Actual thermal and vibroacoustic environment
 - Functional performance of the Flight Safety System/Safe Abort System
- Booster stage flyback phase (if applicable): Flyback engine cut-off, fuel dump or vent (if required), nominal descent to the planned impact area, proper functioning and reliability of the RLV landing systems.
 - Booster stage post-separation (flyback) trajectory data
 - Electrical power usage and reserves
 - Booster stage landing system deployment activity (timestamp)
 - Actual thermal and vibroacoustic environment
 - Actual structural loads environment
 - Functional performance of the Vehicle Health Monitoring System
 - Functional performance of the Flight Safety System/Safe Abort System
 - Attitude, Guidance and Control system activities
- Vehicle stage ascent phase (if multistage): nominal ignition of the stage’s engine, stability and controllability of the stage during engine operation, orbital insertion – simulated (for suborbital) or actual – of the vehicle.
 - Vehicle individual rocket motor ignition timing, updates on propellant flow rates, chamber temperature, chamber pressure, and bum duration
 - Vehicle circularization and phasing bum activities (ignition timing, updates on propellant flow rates, chamber temperature, chamber pressure, and bum duration)

- Vehicle trajectory data (vehicle position, altitude, velocity, roll, pitch, yaw attitudes at a minimum)
 - Attitude, guidance and control system activities
 - Functional performance of the Vehicle Health Monitoring System
 - Functional performance of the Flight Safety System/Safe Abort System
 - Electrical power, and other critical consumables, usage and reserves (i.e. gases, fluids, etc.. .)
 - Actual structural loads environment
 - Actual thermal and vibroacoustic environment
- Vehicle descent (including vehicle's de-orbit burn targeting and execution phases): Function of the programmed flight of the vehicle/upper stage to maintain the capability to land (if reusable) at the planned landing site, or to reenter for disposal (if expendable), assurance of fuel dump or depletion, and proper descent and navigation to the planned or alternate landing site.
 - Vehicle pre-deorbit burn trajectory data
 - Vehicle deorbit burn data (ignition timing, updates on propellant flow rate, chamber temperature, chamber pressure, and burn duration)
 - Vehicle descent trajectory data (position, velocity, and attitude)
 - Attitude, Guidance and Control system activities
 - Actual thermal and vibroacoustic environment
 - Actual structural loads environment
 - Functional performance of the Vehicle Health Monitoring System
 - Functional performance of the Flight Safety System/Safe Abort System
 - Electrical power and other critical consumables usage and reserves (i.e. gases, fluids, etc. . .)
 - Vehicle landing system deployment activity (timestamp)

7.4. PERFORMANCE AND RELIABILITY DATA

Performance and reliability data may be supported by flight history on other vehicles with similar or comparable safety critical systems, sub-systems, and components, and by conducting both analyses and tests, at the respective levels. Having a flight history could mean extensive documentation may not be required if it can be shown through test results, analyses, or empirical data, that the flight regimes experienced are similar to the proposed flight regime. The degree of applicability of data depends on the degree of similarity to environmental conditions and how environmental conditions compare to the history and anticipated reactions of this system. Even when the same system, sub-system, or component is known to have an extensive (and favorable) flight history in the same or more severe environments, interfaces and integration with other systems must still be examined and

tested. Another method of acquiring data is through estimating system, sub-system, and component 3-sigma performance and reliability numbers from testing evaluations and (where applicable) flight data.

The use of similarity is not new to launch operations. EWR 127-1, para. 4.14.1.2, states: as required, qualification by similarity analysis shall be performed; if qualification by similarity is not approved, then qualification testing shall be performed. For example, if component A is to be considered as a candidate for qualification by similarity to a component B that has already been qualified for use, component A shall have to be a minor variation of component B. Dissimilarities shall require understanding and evaluation in terms of weight, mechanical configuration, thermal effects, and dynamic response. Also, the environments encountered by component B during its qualification or flight history shall have to be equal to or more severe than the qualification environments intended for component A.

7.5. OPERATIONAL CONTROLS

There is an interrelationship between the system design capabilities and the systems operational limitations. Figure 3 depicts the relationship between the vehicle systems and the scope of operations within which the vehicle is operated. What constitutes a safety critical system may depend on the scope and nature of the vehicle design and its proposed operations. Intended operational requirements affect the proposed vehicle design requirements and vehicle capabilities/limitations and also establish the operational system constraints necessary to protect public health and safety. For example, landing sites may have to be within some minimum cross-range distance from the orbital ground trace because of cross-range limitations of the vehicle. A vehicle operator may choose, or be required, to mitigate certain vehicle limitations through the use of operational controls rather than relieving vehicle limitations through design changes.

Test parameters and analytic assumptions will further define the limits of flight operations. The scope of the analyses and environmental tests, for example, will constitute the dimensions of the applicant's demonstration process and therefore define the limits of approved operations if a license is issued. Such testing limits, identified system and subsystem limits, and analyses also are expected to be reflected in mission monitoring and mission rules addressing such aspects as commit to launch, flight abort, and commit to reentry.

Vehicle capabilities/limitations and operational factors such as launch location and flight path each affect public risk. The completion of system operation demonstrations, such as flight simulations and controlled flight tests, provide additional confidence in the vehicle systems and performance capabilities. As confidence in the system's overall operational safety performance increases, key operational constraints such as restrictions on overflight of populated areas may be relaxed.

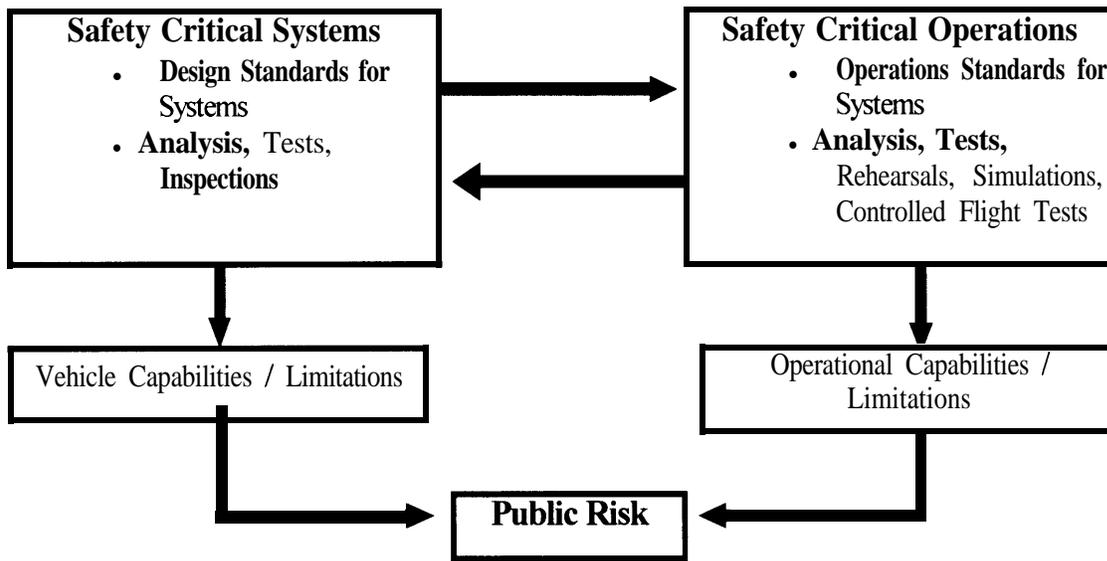


FIGURE 3: INTERRELATIONSHIP BETWEEN SAFETY CRITICAL SYSTEMS AND OPERATIONS

The following are examples of the types of operations-related considerations that may need to be addressed by the applicant when establishing their operations scenarios.

- Launch commit criteria/rules
- Human override capability to initiate safe abort during launch and reentry
- System monitoring, inspection and checkout procedures
- For reflight: inspection and maintenance
- Selected primary and alternate landing sites for each stage
- Surveillance/control of landing areas
- Standard limits on weather
- Coordination with appropriate air space authorities
- Limits on flight regime (ties in with analysis, testing and demonstrating confidence in system performance and reliability)
- Limits on over-flight of populated areas
- Others identified through hazard analysis

8. Determination of Risk to the Public

Expected casualty is used in the space transportation industry as a measure of risk to public safety. Expected casualty is the expected average number of human casualties per mission. Human casualty is defined as a fatality or serious injury. The application of the expected casualty analysis to determine public risk is further defined in AC#431.35-1.

9. Determination of Need for Additional Risk Mitigation

The results of the expected casualty analysis may identify the need for additional risk mitigation measures that need to be employed. These measures may include additional operational controls or may require the redesign of certain safety critical systems. As shown in Figure 1 A, these additional risk mitigation measures would be evaluated within the System Safety Process and the resultant risk to the public would be determined.

ATTACHMENTS

Attachment 1: System Safety Engineering Process

Attachment 2: Sample Reusable Launch Vehicle System Safety Program Plan

Attachment 1

SYSTEM SAFETY ENGINEERING PROCESS?

1.0 INTRODUCTION

The System Safety Engineering Process has been defined as the application of system safety engineering and management principles, operational standards, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system's life cycle. Within this definition resides four explicit, and one implicit, major components. The four explicit components are:

1. System Safety Engineering
2. System Safety Management
3. The System Life Cycle
4. The System

The implicit component is the System Safety Program.

1.1 DEFINITIONS

1.1.1 System A system may be defined as a composite structure of personnel, procedures, materials, tools, equipment, facilities, and software integrated, through the application of sound systems engineering processes and practices, into a designed format to efficiently and effectively accomplish a predetermined objective.

1.1.2 System Life Cycle A system's Life Cycle can be separated into six (6) distinct phases starting with conception and terminating with disposition. Those 6-phases are:

1. Conception
2. Research and Development (R&D)
3. Design
4. Deployment
5. Operation
6. Disposition

1.1.3 System Safety Management System Safety Management defines the system safety program requirements and ensures the planning, implementation and accomplishment of the identified system safety tasks and activities within the scope of the overall system design, engineering, and integration program.

³ The following documentation incorporates sections, paragraphs and passages from both Military Standard 882 and the Systems Safety Manual (System Safety Society Standard)

1.1.4 System Safety Engineering System Safety Engineering is the application of scientific and engineering principles, criteria, and techniques necessary to identify and eliminate hazards or reduce the probability of their occurrence, and the associated risk . System Safety engineering performs those system safety tasks and activities identified by System Safety Management.

1.1.5 System Safety Program The implicit component of the System Safety Engineering Process is the definition and implementation of a System Safety Program. Military Standard (Mil Std) 882, System Safety Program Requirements, defines a system safety program as:

“The combined tasks and activities of system safety management and system safety engineering that enhance operational effectiveness by satisfying the system safety requirements in a timely, cost-effective manner throughout all phases of the system life cycle.”

The objectives of a system safety program are to ensure that:

- a. Safety, consistent with overall system objectives and requirements, is designed into the system in a efficient and cost effective manner.
- b. Hazards associated with the form, fit, function, operation, and support of the system are identified, evaluated, and eliminated, or the associated risk reduced to acceptable levels throughout its entire life cycle.
- c. Safety data, including lessons learned from similar systems are identified and applied.
- d. The proper safety evaluation and analytical techniques are selected and applied to new designs, materials, processes, and procedures to minimize the associated risk.
- e. All methods employed to eliminate hazards and reduce risks, and their effectiveness, are properly applied and documented.
- f. Design changes required to meet specified levels of risk are minimized through the efficient and effective application of safety features during the R&D or acquisition⁴ phase of the system.
- g. Changes in system design, configuration, or application are evaluated and analyzed for impacts to overall system safety and the established acceptable level of risk.
- h. Environmental concerns and impacts associated with the use or disposal of hazardous materials are identified and provided for.
- i. Data banks are established to ensure that significant safety data is retained and readily available for trend analysis.

⁴ It is not uncommon to find that it is more cost effective to acquire a system, major component (subsystem) or support and test equipment (S&TE). From the end user’s perspective, it is a purchase or acquisition. Within the System Life Cycle, the design phase becomes the acquisition phase.

The methodology by which the System Safety Program and System Safety Engineering Process is defined and implemented is the System Safety Program Plan.

1.1.6 System Safety Program Plan The System Safety Program Plan provides a description of the planned methods by which recognized and accepted safety standards and requirements, including organizational responsibilities, resources, methods of accomplishment, milestones, and levels of effort, are to be tailored and integrated with other system engineering functions to ensure hazards are identified and eliminated, or that their probability of occurrence is reduced to acceptable levels of risk. Tailoring refers to the selection and application of recognized and accepted safety standards, requirements, and procedures that are necessary, appropriate, and consistent with overall system objectives. Integration refers to the application of hazard elimination and reduction techniques in a manner that complements or enhances the implementation of the other system engineering functions.

2.0 APPLICATION

It can be stated, in general terms, that the intent of the System Safety Engineering Process is to identify and eliminate, or reduce or control hazards to acceptable levels of risk throughout a system's life cycle. Hazard reduction or control is commonly referred to as mitigation; i.e. reduce or moderate the effect thereof. This requires an understanding of terminology associated with the word "hazard" as it is used in this document.

2.1 HAZARD DEFINITIONS

The following definition of hazard and associated terms have been taken from Mil Std 882:

2.1.1 Hazard A condition that is a prerequisite to a mishap.

2.1.2 Mishap An unplanned event or series of events that results in death, injury, occupational illness, or damage to or loss of equipment or property.

2.1.3 Hazardous Event An occurrence that creates a hazard.

2.1.4 Hazard Probability The aggregate probability of occurrence of the individual hazardous event that create a specific hazard. The probability that a hazard will be created during the planned life expectancy of a system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning hazard probabilities should be documented in hazard analysis reports. The terminology is commonly applied to qualitative hazard probability assessments:

2.1.4.1 Frequent Likely to occur frequently; commonly experienced.

2.1.4.2 Probable Will occur several times in the system's life cycle.

2.1.4.3 Occasional Likely to occur sometime in the system's life cycle.

2.1.4.4 Remote Unlikely but possible to occur sometime in the system's life cycle.

2.1.4.5 Improbable So unlikely, it can be assumed the occurrence may not be experienced.

2.1.5 Hazardous Event Probability The likelihood, expressed in quantitative or qualitative terms, that a hazardous event will occur.

2.1.6 Hazard Severity An assessment of the worst credible mishap that could be caused by a specific hazard. Hazard severity categories are defined to provide a qualitative measure of the worst credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction as follows:

2.1.6.1 Catastrophic Death or system loss.

2.1.6.2 Critical Severe injury or occupational illness; severe system damage.

2.1.6.3 Marginal Minor injury or occupational illness; minor system damage.

2.1.6.4 Negligible Less than minor injury or occupational illness; or less than minor system damage.

2.2. CONCEPTUAL PHASE

During the Conceptual Phase, safety standards, specifications, regulations, and relevant system safety design requirements are identified and evaluated for relevance and applicability. It is during this phase that System Safety Management develops and System Safety Engineering initiates implementation of the System Safety Program Plan (SSPP) which, at a minimum, should define:

- a. The Purpose, Scope and Objectives of the SSPP.
- b. The System Safety Organization including all interfaces and Working Group.
- c. System Safety Program Reviews and Milestones.
- d. General System Safety Requirements and Operational Standards.
- e. Hazard Analyses.
- f. System Safety Data and Assessments.
- g. Safety Compliance Assessment.
- h. Safety Review of Engineering Change Proposals and Deviation/Waiver Request.

- i. Safety Program Verification, Validation and Auditing.
- j. Safety Training
- k. Mishap and Hazardous Malfunction Analysis and Reporting.

2.3 RESEARCH AND DEVELOPMENT (R&D) PHASE

During the R&D phase, those safety standards, specifications, regulations, and relevant system safety design requirements identified as relevant or applicable during the Conceptual Phase are evaluated against design documentation and developmental hardware for the purpose of:

- a. Eliminating hazards or reducing the associated risk through design, material selection, or substitution.
- b. Identifying and isolating hazardous materials and operations.
- c. Positioning components so that access during operations, servicing, or maintenance minimizes personnel exposure to hazardous conditions or situations.
- d. Minimizing risk due to extreme temperatures, pressure, noise, or toxicity, accelerations or vibrations.
- e. Eliminating or mitigating risk due to human factors.
- f. Mitigating or controlling damage due to component failure.
- g. Providing system and personnel protection by utilizing emergency systems or devices.
- h. Minimizing the severity of personnel injury or system damage in the event of a mishap.
- i. Incorporating software controlled or monitored functions to minimize initiation of hazardous events or mishaps.

2.3.1 Preliminary Hazard List (PHL)

A byproduct of the Conceptual Phase that is fully implemented and utilized during the R&D Phase is the PHL. The PHL is used to document those possible hazards identified as being applicable to or inherent in the design to ensure their recognition, visibility and investigation. The PHL may also identify hazards that require special safety design emphasis or hazardous areas where in-depth safety analyses are needed as well as the scope of those analyses. At a minimum, the PHL should identify:

- The Hazard

- When identified (phase of system life cycle)⁵
- How identified (analysis, malfunction, failure) and by whom.
- Severity and Probability of Occurrence.
- Probable/actual cause(s)
- Proposed elimination/mitigation techniques.
- Status (Open-action pending /Closed-eliminated/Mitigated)
- Process of elimination/mitigation.
- Oversight/approval authority.

2.3.2 Preliminary Hazard Analysis (PHA)

The PHA is the initial effort relative to the conduct of hazard analyses. The purpose of the PHA is not to effect control of all risks but to fully recognize the hazardous states and all of the associated risks. It is the basic hazard analysis that establishes the framework for other hazard analyses that may be performed. The output of the PHA may also be used to develop system safety requirements and design specifications. The PHA will usually include, but is not limited to, the identification and analysis of:

- a. Hazardous components such as fuels, propellants, lasers, explosives, toxic substances, pressure systems and other energy sources.
- b. Safety related interfaces, material incompatibilities, electromagnetic interference (EMI), inadvertent activation, fire/explosion initiation and propagation, and hardware and software controls.
- c. Environmental constraints including the operating environments, exposure to toxic substances, health hazards, fire, electrostatic discharge (ESD), lightning, ionizing and non-ionizing radiation.
- d. Operating, test, maintenance and emergency procedures, human factor engineering and human error analysis, life support requirements, human safety systems (egress, rescue, survival), and equipment salvage operations.
- e. Facilities, Support and Test Equipment (S&TE), packaging, handling, storage, and transportation (PHS&T) requirements, provisions for storage, assembly, checkout, and testing of hazardous systems/ subsystems/assemblies/subassemblies which contain, control or monitor toxic, flammable, explosive, corrosive or cryogenic fluids; radiation or noise emitters or other power/energy sources.
- f. Training and certification/qualification requirements pertaining to hazardous operations and abatement; and safety operations, maintenance, control, supervision.

⁵ The PHL is converted to a System Hazard List (SHL) and is used as a device for tracking a hazard through the cycle of identification, classification, evaluation, analysis, elimination or mitigation, and elimination/mitigation verification and validation or residual risk acceptance.

- g. Essential safety related equipment, safeguards and the application of interlocks, redundancy, hardware/software fail safe design considerations, subsystem/assembly protection, fire suppression system, personal protective equipment, and noise or radiation barriers.

Some specialized safety analyses that may be employed in support of the PHA are:

2.3.2.1 Comparison-To-Criteria (CTC) Analysis The purpose of the CTC Analysis is to provide a formal and structured format that identifies all safety requirements for a system and ensures compliance with those requirements.

2.3.2.2 Environmental Risk Analysis The purpose of Environmental Risk Analysis is to assess the risk of environmental non-compliance that may be caused by a failure in a system.

2.3.2.3 External Events Analysis The purpose of this analysis is to focus the attention of the system safety analyst to those events outside the system under examination. It is to further hypothesize the range of credible events that may have an effect on the system being examined.

2.3.2.4 Fire Hazard Analyses There are multiple types of fire hazard analyses, four of which are described below:

2.3.2.4.1 Preliminary Fire-Hazard Analysis This type of analysis presents a listing of what are believed to be the primary fire hazards of concern, together with a qualitative estimate of the potential effects of these hazards on safety systems and the “best method” to control the hazard.

2.3.2.4.2 Barrier Analysis An analysis technique which describes fire severity in terms of total involvement of combustibles in a room and in terms of total involvement effect on the room’s structural integrity. Total involvement of combustibles is often referred to as “flashover.”

2.3.2.4.3 Fuel Load Analysis As described in the National Fire Protection Association (NFPA) Handbook, a fuel load analysis starts by adding up the weight of combustibles in a room and converting the weight to energy content of the fuel per unit floor area. The measured fuel load is then compared to a linear fire-duration scale.

2.3.2.4.4 National Fire Protection Association Decision Tree Analysis This method views fire events in a logical sequence leading to a predefined fire objective for life safety and property protection.

2.3.2.5 Health Hazard Assessment (HHA) The purpose of the HHA is to provide a detailed review of hazardous materials used in a facility or operation and to identify and evaluate potential hazards, eliminate or control the hazards, and to provide a verification of health-related requirements. The HHA uses the Material Safety Data Sheet (MSDS) as the

primary source and starting place for information on each material within the facility or operation, as well as each material that may be introduced.

2.3.2.6 Laser Safety Analysis The purpose of laser safety analysis is to provide a means to assess the hazards of non-ionizing radiation. As such, its intent is to also identify associated hazards and the types of controls available and required for laser hazards.

2.3.2.7 Management Oversight and Risk Tree (MORT) Analysis The purpose of the MORT technique is to systematically and logically analyze a system or an accident in order to examine and determine detailed information about the process inner-workings to include identification of hazards. It applies a pre-designed, systematized logic tree to the identification of total system risk, both those inherent in physical equipment and processes and those which arise from operational/management inadequacies. The pre-designed tree, intended as a comparison tool, generally describes all phases of a safety program and is applicable to systems and processes of all kinds. The technique is of particular value in accident/incident investigation as a means of discovering system or program weaknesses or errors which provide an environment conducive to mishaps.

2.3.2.8 Nuclear Safety/Cross-Check Analyses These analyses are applicable to reactor and non-reactor nuclear system.

2.3.2.8.1 Nuclear Safety Analyses The purpose of the nuclear safety analysis is to establish requirements for contractors responsible for the design, construction, operation, decontamination, or decommissioning of nuclear facilities or equipment to develop safety analyses that establish and evaluate the adequacy of the safety bases of the facility/equipment. The Department of Energy (DOE) requires that the safety bases analyzed include management, design, construction, operation, and engineering characteristics necessary to protect the public, workers, and the environment from the safety and health hazards posed by the nuclear facility or non-facility nuclear operations. The Nuclear Safety Analysis Report (NSAR) documents the results of the analysis.

2.3.2.8.2 Nuclear Safety Cross-Check Analyses (NSCCA) The NSCCA provides a technique that verifies and validates software designs. The NSCCA is also a reliability hazard assessment method that is traceable to requirements-based testing.

2.3.2.9 Probabilistic Risk Assessment (PRA) The PRA provides an analysis technique for low probability, but catastrophic severity type events. It identifies and delineates the combinations of events that, if they occur, will lead to an accident and estimates the frequency of occurrence for each combination of events, and then estimates the consequences. It involves developing models of the system, data bases giving competent failure rates, and baselines of the dominant risk sequences.

2.3.2.10 Single-Point Failure Analysis (SPFA) The purpose of a SPFA is to identify those failures that would produce a catastrophic event in terms of injury or monetary loss if they were to occur by themselves. The SPFA is performed by examining the system, element by element, and identifying those discrete elements or interfaces whose malfunction or failure,

taken individually, would induce system failure. The technique is equally applicable to hardware, software and formalized human operator procedures.

2.3.2.11 Explosive Safety Analysis The purpose of an explosive safety analysis is to provide an assessment of the hazards and potential explosive effects of the storage, handling or operations with various types of explosives from gram to ton quantities and to determine the damage potential.

An output of the PHA, SHA, and Safety Program Reviews is the Safety Assessment Report.

2.3.3 Safety Assessment Report (SAR).

The purpose of the SAR is to identify and document:

- a. The safety features of the hardware, software, and system design;
- b. The operational and procedural hazards that may be present including the specific controls and associated precautions;
- c. The safety criteria and methodology used to classify and rank hazards;
- d. The analyses and tests performed to identify hazards inherent in the system including:
 1. Hazards that still have residual risk, and the actions that have been taken to reduce the associated risk to specified acceptable levels.
 2. Results of tests conducted to verify and validate safety criteria requirements and analyses.
- e. The results of the safety program efforts;
- f. All significant hazards, the operating conditions (normal or abnormal) when they can be expected to occur, and specific recommendations or precautions required to ensure safety of personnel and property.
- g. All hazardous materials generated by or used in the system, including:
 1. Identification by type, quantity, and potential hazards.
 2. Safety precautions and procedures necessary during PHS&T).
 3. Explosives hazard classifications and Material Safety Data Sheets.
- h. The environmental impacts or hazards associated with the deployment, operation (including logistical support) and disposition of the system;
- i. A signed statement by the System Safety Program Manager attesting to the fact that all identified hazards have been eliminated or their associated risks controlled to levels specified as acceptable, and that the system is ready to test or operate or proceed to the next design/acquisition or life cycle phase.

2.4 DESIGN PHASE

The Design Phase of the System Engineering and Integration Process is subdivided into phases punctuated by Design Reviews. The purpose of the Design Reviews are primarily to assure management that the program is on schedule, that all critical issues have been identified and have either been resolved or that the proposed solutions are “workable”. The number and frequency of design reviews will vary according to the complexity of the system and the results of the previous review. A simple system or an “off-the-shelf” acquisition may have only one. Conversely, a “typical” three phase design review process, consisting of a conceptual, preliminary and critical design review, may have those reviews subdivided into phases, identified as Phase I, II, and III, as well.

During this phase of system development or acquisition, hazards identified by the PHA are evaluated and analyzed for inadequate safety features or induced hazards, and follow-on safety evaluations and analyses are conducted, and safety related design changes are recommended, documented, tracked, verified, and validated. The major follow-on safety analyses initiated, but not necessarily completed during this phase are the:

- a. System Hazard Analysis (SHA);
- b. Subsystem Hazard Analysis (SSHA);
- c. Software Hazard Analysis (SWHA); and
- d. Operating and Support Hazard Analysis (O&SHA).

2.4.1. System Hazard Analysis (SHA) The SHA, in many respects, is a continuation of the PHA in that most often the emphasis of the PHA is hazard identification which will include an intuitive estimate of the severity and probability of occurrence. The SHA will verify and validate the results of the PHA or eliminate some of the identified hazards as not being applicable to the design or as having been addressed and eliminated by design. It may also result in some of the PHA hazards being upgraded or downgraded in severity or probability of occurrence due to design considerations. However, since the design has reached a higher level of detail and sophistication, new hazards will be identified and rated as well.

Depending on the characteristics of the system, specialized analysis will be used to support or complement the SHA. Some of the most common specialized analysis are:

2.4.1.1. Bent Pin Analysis This analysis investigates the faults that can result from bent pins in electrical connectors and is applicable to the SHA, SSHA, and O&SHA during maintenance operations.

2.4.1.2 Change Analysis Change analysis examines the potential effects of modification from a starting point on baseline. The change analysis systematically hypothesizes worst-case effects from each modification from that baseline.

2.4.1.3 Checklist Analysis A list of specific items is used to identify known types of hazards, design deficiencies, and potential accident situations associated with common

equipment and operations. the identified items are compared to appropriate standards. The Checklist Analysis technique can be used to evaluate materials, equipment, or procedures.

2.4.1.4 Contingency Analysis A contingency analysis is a method of preparation for emergencies by identifying potential accident causing conditions and respective mitigating measures to include protective systems and equipment.

2.4.1.5 Cryogenic Systems Safety Analysis (CSSA) The purpose of the CSSA is to specifically examine cryogenic systems from a safety standpoint in order to eliminate or to mitigate the hazardous effects of potentially hazardous materials at extremely low temperatures.

2.4.1.6 Event/Fault Tree Analyses

2.4.1.6.1 Event Tree Analysis (ETA) The ETA is an analytical tool that can be used to organize, characterize, and quantify potential accidents in a methodical manner. An event tree models the sequence of events that results from a single initiating event.

2.4.1.6.2 Fault Tree Analysis (FTA) The purpose of the FTA is to assess a system by identifying a postulated undesirable end event and examining the range of potential events that could lead to that state or condition. The FTA can model the failure of a single event or multiple failures which lead to a single system failure. The FTA is a Top Down analysis versus the Bottom Up approach for the event tree analysis.

2.4.1.7 Facilities System Safety Analysis (FSSA) The purpose of the FSSA is to apply system safety analysis techniques to a facility and its operations. Safety analyses, within the FSSA, document the safety bases for and commitments to the control of subsequent operations. This includes staffing and qualification of operating crews; the development, testing, validation, and in-service refinement of procedures and personnel training materials; and the safety analysis of the person-machine interface for operations and maintenance. In safety analyses for new facilities and safety-significant modifications to existing facilities, considerations of reliable operations, surveillance, and maintenance and the associated human factors safety analysis are developed in parallel and integrated with hardware safety design and analysis. Once a facility or operation is in service, the responsible contractor and safety oversight activities use the report, which contains OSHA 1910.119 Program Requirements.

2.4.1.8 Fault Hazard Analysis (FHA) The FHA is very similar to a PHA. It is a subset of the Failure Modes and Effects Analysis (FMEA) technique. The FHA is a basic inductive analysis that is used to perform an evaluation that starts with the most specific form of the system and integrates individual examinations into the total system evaluation. The purpose of the FHA is to systematically examine a facility or system and to identify hazards and their effects. (See FMEA)

2.4.1.9 Material Compatibility Analysis Material Compatibility Analysis provides an assessment of materials utilized within a particular design. Any potential degradation that can occur due to material incompatibility is evaluated. System Safety is concerned with any

physical degradation due to material incompatibility that can result in contributory hazards or failures which can cause mishaps to occur.

2.4.1.10 Procedure Analysis Procedure Analyses are often designated by the procedure or activity to be analyzed, i.e., Test Safety Hazard Analysis, Operation Safety hazard Analysis, Maintenance Safety Hazard Analysis, Job Safety Analysis. The Procedure Analysis provides an analysis technique to perform step-by step reviews of procedures in operations to detect the possibilities of:

- harm to operations by the system/subsystems, or
- harm to the system/subsystems by the operators.

2.4.1.11 Process Hazard Analysis A Process Hazard Analysis is a requirement of OSHA 1910.199 (29 CFR 1910.199) for the management of highly hazardous chemicals. It is a means of identifying and analyzing the significance of potential hazards associated with the processing or handling of certain highly hazardous chemicals.

2.4.2 Subsystem Hazard Analysis (SSHA) The SSHA is performed to identify and document hazards associated with the design of subsystems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and assemblies within the subsystems as well as their external interfaces. It includes software whose performance, degradation, functional failure or inadvertent functioning could result in a hazard. It also includes a determination of the modes of failure including reasonable human errors, single point failures and the effects on safety when failures occur within subsystem components and assemblies.

As with the SHA, specialized analysis will be used to support or complement the SSHA. Some of the most common specialized analyses are:

2.4.2.1 Cable Failure Matrix Analysis (CFMA) The CFMA is a shorthand method used to concisely represent the possible combinations of failures that can occur within a cable assembly.

2.4.2.2 Common Cause Analysis The purpose of the common cause analysis is to identify any accident sequences in which two or more events could occur as the result of a common event or causative mechanism. If the probability of a common cause is significantly greater than the probability of two or more events occurring independently, then the common cause could be an important risk contributor. These single secondary cause/events may result from a common process, manufacturing defect, a common human operator error, or some common external event. This technique is very useful for accident reconstruction.

2.4.2.3 Petri Net Analysis The purpose of the Petri Net Analysis is to provide a technique to model systems components at a wide range of abstract levels. Once a Petri Net model has been developed, its mathematical representation can be analyzed by automated means. The analysis can be used to model an entire system, subsystems, or system components at a wide range of abstract levels all the way through conceptual, top level and detailed designs, down to actual implementation in hardware and software.

2.4.2.4 Human Error/Factors Analysis

2.4.2.4.1 Human Error Analysis This analysis is used to identify the systems and the procedures of a process where the probability of human error is of concern. The concept is to define and organize the data collection effort such that it accounts for all the information that is directly or indirectly related to an identified or suspected problem area. This analysis recognizes that there are, for practical purposes, two parallel paradigms operating simultaneously in any human/machine interactive system one comprising the human performance and the other, the machine performance. The focus of this method is to isolate and identify, in an operational context, human performance errors that contribute to output anomalies and to provide information that will help quantify their consequences.

2.4.2.4.2 Human Factors Analysis The Human Factors concept is the allocation of functions, tasks, and resources among humans and machines. The most effective application of the human factors perspective presupposes an active involvement in all phases of system development from design to training, operation and, ultimately, the most overlooked element, disposal. Its focus ranges from overall system considerations (including operational management) to the interaction of a single individual at the lowest operational level. However, it is most commonly applied and implemented, from a systems engineering perspective, to the system being designed and as part of the SHA.

2.4.2.5 Sneak-Circuit Analysis (SCA) The purpose of the SCA is to identify unintended paths or control sequences that may result in undesired events or inappropriate timed events. It is accomplished by examining circuits (or command/control functions), searching out unintended paths (or control sequences) which, without component failure, can result in undesired operations, or in desired operations at inappropriate times, or which can inhibit desired operations. SCA is applicable to control and energy-delivery circuits of all kinds, whether electronic/electrical, pneumatic, or hydraulic and is adaptable to software analysis.

2.4.2.6 Structural Safety Analysis Is used to validate mechanical structures. Inadequate structural assessment results in increased risk due to the potential for latent design problems causing structural failures, i.e., contributory hazards. Structural design is examined via mathematical analysis to satisfy two conditions:

- Equilibrium of forces, and
- Compatibility of displacements

The structure considered as a whole must be in equilibrium under the action of the applied loads and reactions; and, for any loading, the displacements of all the members of the structure due to their respective stress-strain relationships must be consistent with respect to each other.

2.4.2.7 The Human Error Rate Prediction (THERP) The purpose of THERP is to provide a quantitative measure of human operator error in a process and is a means of quantitatively estimating the probability of an accident being caused by a procedural error.

2.4.2.8 Test Safety Analysis (TSA) TSA is used to ensure a safe environment during the conduct of systems and prototype testing. It also provides safety lessons to be incorporated into the design, as applicable. Each test is evaluated to identify hazardous materials or operations.

2.4.2.9 Time/Loss Analysis (T/LA) for Emergency Response Evaluation is a system safety analysis-based process developed to semi-quantitatively analyze, measure and evaluate planned or actual loss outcomes resulting from the action of equipment, procedures and personnel during emergencies or mishaps. T/LA procedures produce objective, graphic time/loss curves showing expected versus actual loss growth during emergencies or mishaps. The expected versus actual loss data is used to describe the change in the outcome produced by intervention actions at successive states of the emergency response. Although it is a system level analysis, due to lack of design definition and maturity, it is not usually initiated until after the SSHA has begun and uses the SSHA data before it is integrated into the SHA.

2.4.3 Software Hazard Analysis (SWHA) The SWHA identifies hazardous conditions incident to safety critical operator information and command and control functions identified by the PHA, SHA, SSHA and other efforts. It is performed on safety critical software-controlled functions to identify software errors/paths which could cause unwanted hazardous conditions. The SWHA can be divided into two stages, preliminary and follow-on.

2.4.3.1 Preliminary SWHA The Preliminary SWHA is used to examine software design to identify unsafe inadvertent command/failure-to-command modes for resolution. It is accomplished by tracing safety critical operator information and commands through flow charts, storage allocation charts, software and hardware specifications and other applicable documentation.

2.4.3.2 Follow-on SWHA This phase of the SWHA examines software and its system interfaces for events, faults, and occurrences such as timing which could cause or contribute to undesired events affecting safety. It is accomplished by tracing safety critical operator information and commands through source/object code by system simulation. Safety critical programs/modules are analyzed for sensitivity to software or hardware failures which could cause the system to operate in a hazardous manner.

Specialized analysis used to support or complement the SWHA are:

2.4.4 Operating and Support Hazard Analysis (O&SHA) The purpose of the O&SHA is to examine procedurally controlled activities and to identify hazards and recommend risk reduction alternatives during all phases of intended system use. This analysis identifies and evaluates:

- a. Activities which occur under hazardous conditions, their time periods, and the actions required to minimize risk during these activities/time periods.
- b. Changes needed in functional or design requirements for system hardware/software, facilities, tooling, or S&TE to eliminate hazards or reduce associated risk.

- c. Requirements for safety devices and equipment, including personnel safety and life support and rescue equipment.
- d. Warnings, cautions, and special emergency procedures.
- e. Requirements for PHS&T and the maintenance and disposal of hazardous materials.
- f. Requirements for safety training and personnel certification.

While many of the analyses initiated during the PHA, SHA and SSHA are carried over and integrated into the O&SHA, the following specialized analysis are used to support or complement the O&SHA are:

2.4.4.1 Accident Analysis The purpose of the Accident Analysis is to evaluate the effect of scenarios that develop into credible accidents. Those that do not develop into credible accidents are documented and recorded to verify their consideration and validate the results.

2.4.4.2 Confined/Enclosed Space Safety Analysis The purpose of this analysis is to highlight the type of systematic examination of confined space hazards that should be conducted in order to preclude or at least minimize the potential for accidents.

2.5 DEPLOYMENT, AND OPERATIONAL PHASES

The SHA, SSHA, SWHA and O&SHA are all carried over into the Deployment and Operational Phases. Depending upon system complexity, the SHA, SSHA and SWHA may all be rolled into and carried forward as a single integrated O&SHA which will be initiated during the latter portion of the Design Phase. As the basic system is changed, modified and upgraded, various supporting analysis will be reapplied to ensure the integrity and currency of the existing Safety Risk Assessments.

2.6 DISPOSITION PHASE

Some or all of the previously discussed analyses may be carried forward and revised, initiated or reinitiated just prior to transitioning from the Operational to the Disposition Phase:

- Accident Analysis
- Common Cause Analysis
- Cryogenic Systems Safety Analysis
- Environmental Risk Analysis
- Fire Hazard Analysis
- Human Error/Factors Analysis
- Laser Safety Analysis
- Materials Compatibility Analysis

- Nuclear Safety/Cross-Check Analysis⁶
- Probabilistic Risk Assessment
- Process Hazard Analysis
- Structural Safety Analysis
- Change Analysis
- Confined/Enclosed Space Safety Analysis

However, the Deactivation Safety Analysis is specifically applicable to the Disposition Phase.

Deactivation Safety Analysis The purpose of the Deactivation Safety Analysis is to identify significant safety and health (S&H) concerns integral to the deactivation process. The S&H practices are applicable to all deactivation activities, particularly those involving systems or facilities that have used, been used for, or have contained hazardous or toxic materials. The deactivation process involves placing the system or facility into a safe and stable condition that can be economically monitored over an extended period of time while awaiting final disposition for reuse or disposal. The deactivation methodology emphasizes specification of end-points for cleanup and stabilization based upon whether the system or facility will be deactivated for reuse or in preparation for disposal. Specific guidance or procedures can be found in the following documentation:

- DOE Order 5480.23 Nuclear Safety Analysis Reports
- DOE Order 5481.1B Safety Analysis and Review System
- DOE Order 6430.1 A General Design Criteria

Supporting References include:

- DOE-STD- 1027-92
- DOE-STD-3009-94
- . DOE-STD-301 1-94
- DOE/EM-O3 18-96
- . DIE/EH-0486-92

Although these documents are primarily geared towards the Nuclear Power Industry, it should be remembered that Nuclear waste is, in fact, one among many hazardous materials and another form of toxic waste.

2.7 INPUT ANALYSIS

⁶ Nuclear powered systems only.

There are other evaluation procedures and system analyses which are routinely conducted by other Systems Design, Engineering, and Integration functions, such as Reliability & Maintainability Engineering, upon which system safety depends for vital input data. Conversely, some of those evaluations/analyses use data provided from system safety analysis. Some of these analyses are:

2.7.1 Failure Modes, Effects and Criticality Analysis (FMECA) The FMECA is an essential function in design from concept through development. The FMECA documents all probable failures of a system within specified ground rules, determines by failure modes analysis the effect of each failure on system operation, identifies single failure points, and ranks each failure according to a severity classification of failure effect. The methodology is the result of the following two analysis steps which, when combined, produce the FMECA:

2.7.1.1 Criticality Analysis The purpose of the criticality analysis is to rank each potential failure mode identified in a FMEA according to the combined influence of severity classification and its probability of occurrence based on the best available data.

2.7.1.2 Failure Modes and Effects Analysis (FMEA) The purpose of the FMEA is to determine the results or effects of sub-element failure on a system operation and to classify each potential failure according to its severity.

2.7.2 Damage Modes and Effects Analysis (DMEA) The purpose of the DMEA is to provide early criteria for survivability and vulnerability assessments. The DMEA provides data related to damage caused by specified threat mechanisms and the effects on system operation and mission essential functions.

2.7.3 Digraph Utilization Within System Safety Directional Graphs (digraphs) have been used to model failure effect scenarios within large complex systems, thereby modeling FMEA data. Digraphs can also be used to model hazardous events and reconstruct accident scenarios. As a result, both hazard analysis and accident investigation processes can be improved via modeling event sequences.

2.7.4 Electromagnetic Compatibility (EMC) Analysis and Testing EMC analysis is conducted to minimize/prevent accidental or unauthorized operation of critical safety functions within a system. The output of radio frequency (RF) emitters can be coupled into and interfere with electrical systems which process or monitor critical safety functions. Electrical disturbances may also be generated within an electrical system from transients accompanying the sudden operation of electrical devices. Design precautions must be taken to prevent electromagnetic interference (EMI) and electrical disturbances. Human exposure to electromagnetic radiation is also a concern.

2.7.5 Energy Trace and Barrier Analysis (ETBA) for Hazard Discovery and Analysis The ETBA method is a system safety-based analysis process developed to aid in the methodical discovery and definition of hazards and risks of loss in systems by producing a consistent, detailed understanding of the sources and nature of energy flows

that can or did produce accidental harm. Outputs support estimation of risk levels, and the identification and assessment of specific options for eliminating or controlling risk.

These analyses are routinely started in conjunction with the SHA and may be initiated when critical changes or modifications are made.

2.8 DECISION ANALYSES

The following decision analyses methodologies are analysis tools and techniques primarily used by System Safety Management:

2.8.1 Control Rating Code (CRC) Method The CRC method is a generally applicable system safety-based procedure used to produce consistent safety effectiveness rating of candidate actions intended to control hazards found during system safety analyses or accident investigations. Its primary purpose is to control recommendation quality. A secondary purpose is to require systematic application of accepted safety principles to the identification and selection of hazard controls intended to control system risk. Finally, it helps analysts identify priorities to support specific hazard control action plans.

2.8.2 Critical Path Analysis (CPA) The CPA and Program Evaluation Review Technique (PERT) are the two most commonly used forms of Network Modeling and Network Analysis Techniques (NATs) which are utilized to manage large Complex Programs and Projects. A program or project network is basically a graphical representation or description of activities or milestones, which are, needed in order to solve a problem. By employing NATs (e.g., logic diagrams) solutions can be obtained for a particular problem. PERT has been used to assist management in planning and controlling many programs and projects that consist of numerous specific tasks (activities), each of which must be completed in order to complete the entire project.

These analyses are routinely begun when the SSPP is initiated and revised throughout the system life cycle on an as needed as required basis.

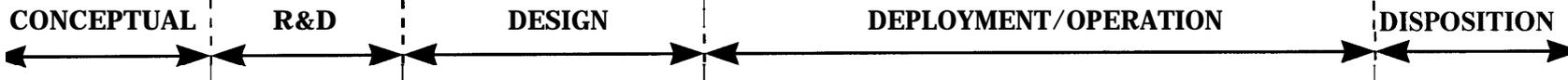
2.9 SUMMARY

All of the available analyses have not been identified and not all of those identified will be applied during a specific System Safety Analysis Process. Just as the design is tailored to meet operational and cost goals and constraints, so too will the Process and corresponding analyses.

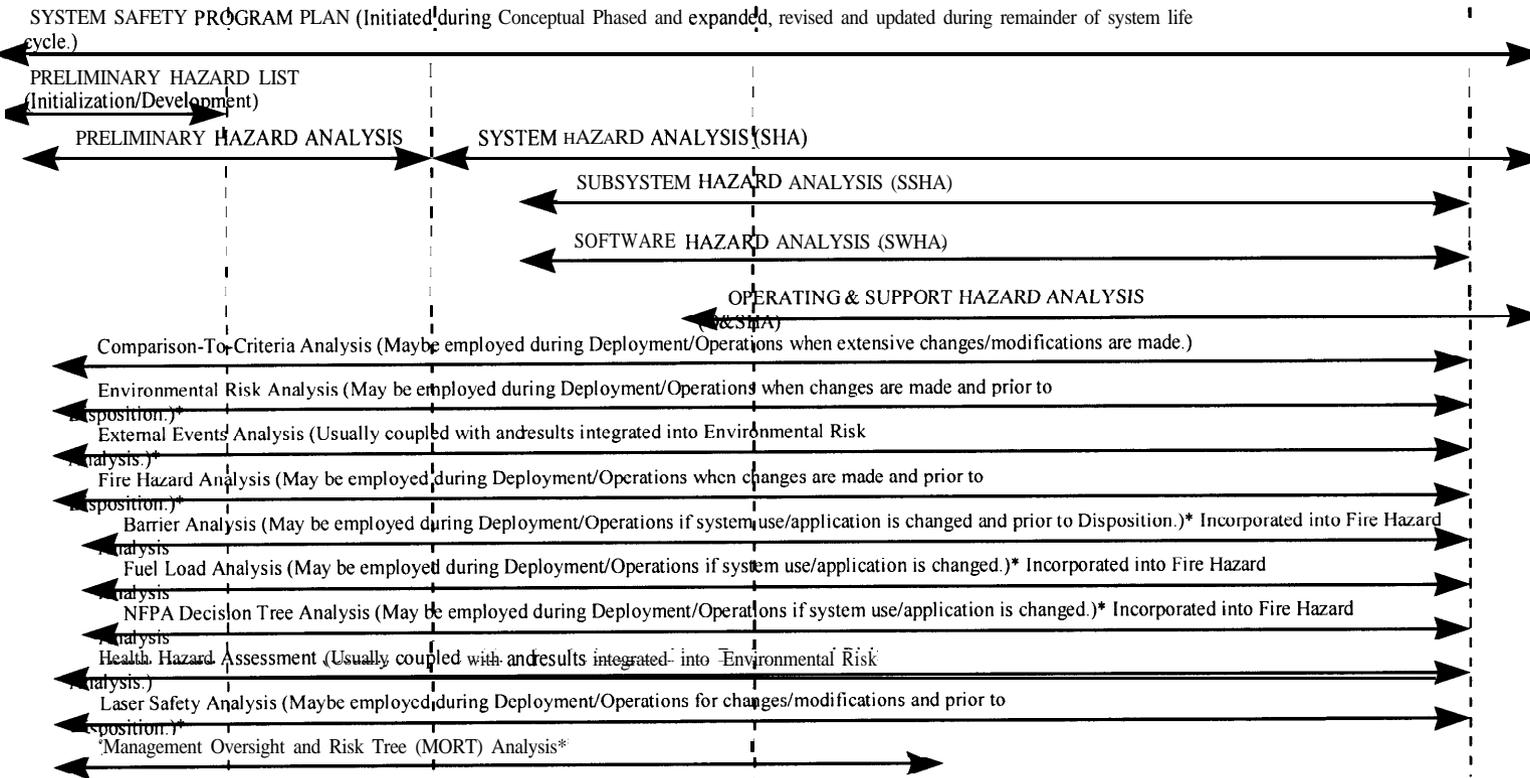
Figure 1

SYSTEM SAFETY ENGINEERING PROCESS

SYSTEM DESIGN, ENGINEERING AND INTEGRATION PROCESS

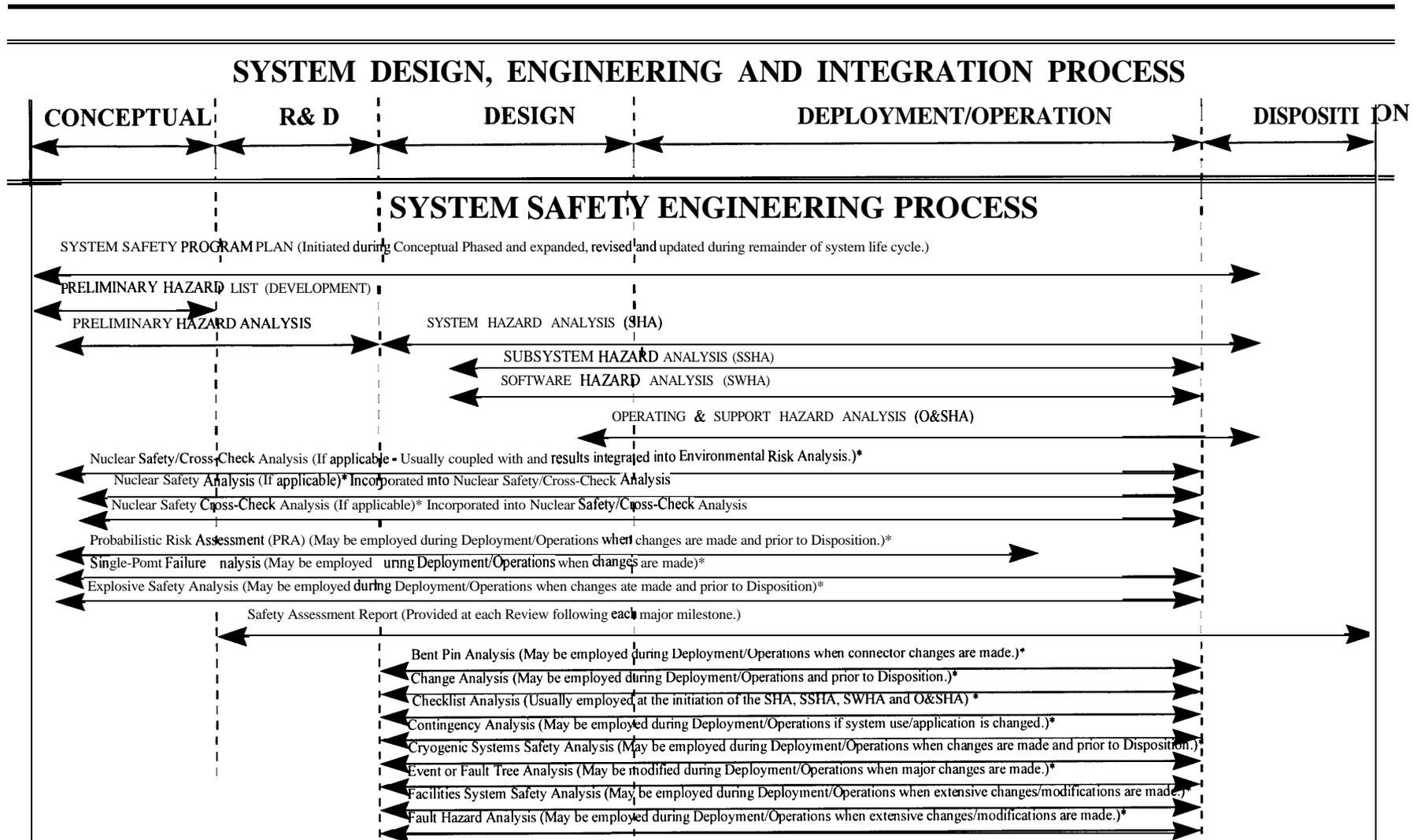


SYSTEM SAFETY ENGINEERING PROCESS



Subordinate to and incorporated into PHA, SHA, SSHA or O&SHA

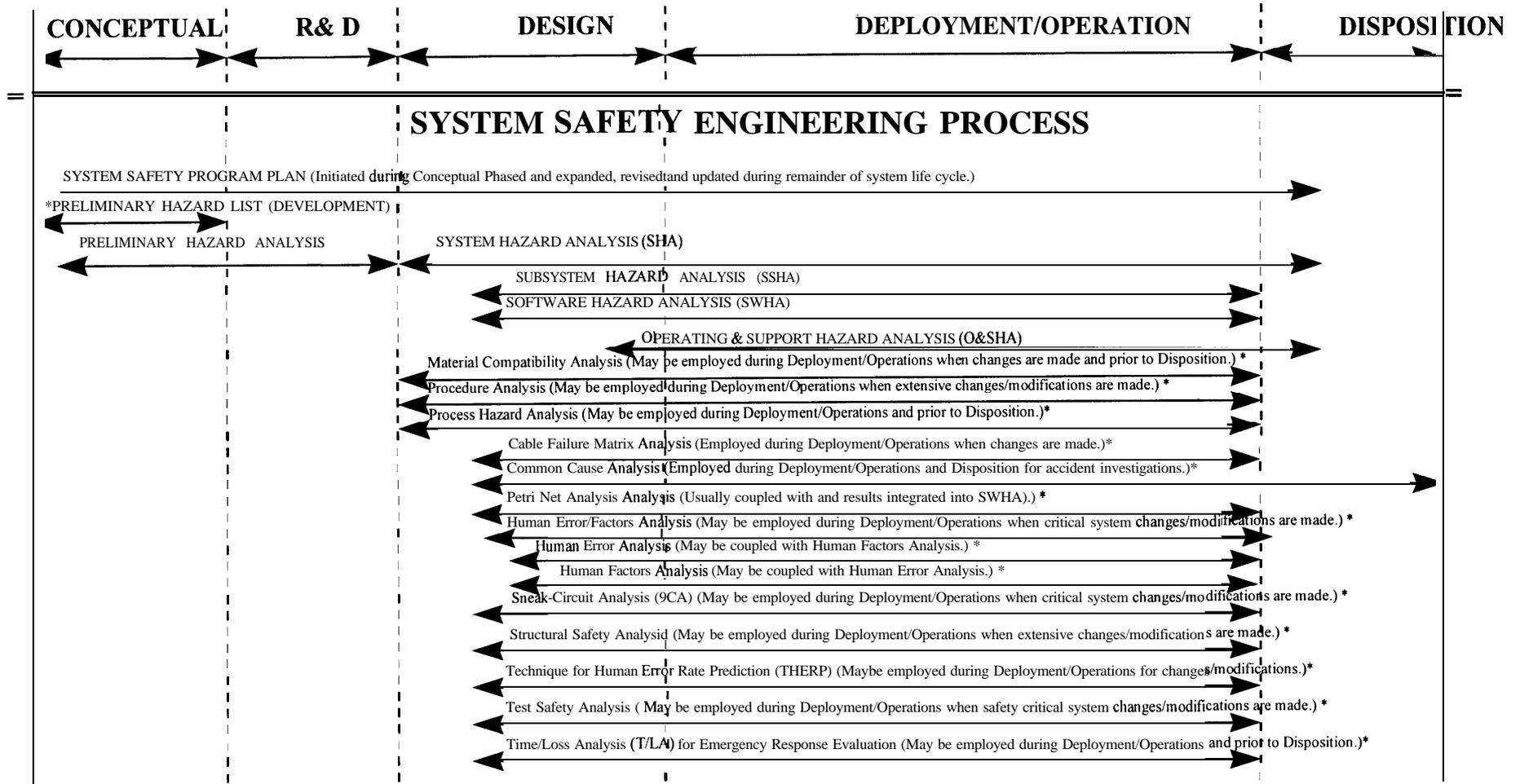
SYSTEM SAFETY ENGINEERING PROCESS



* Subordinate to and incorporated into PHA, SHA, SSHA or O&SHA.

SYSTEM SAFETY ENGINEERING PROCESS

SYSTEM DESIGN, ENGINEERING AND INTEGRATION PROCESS



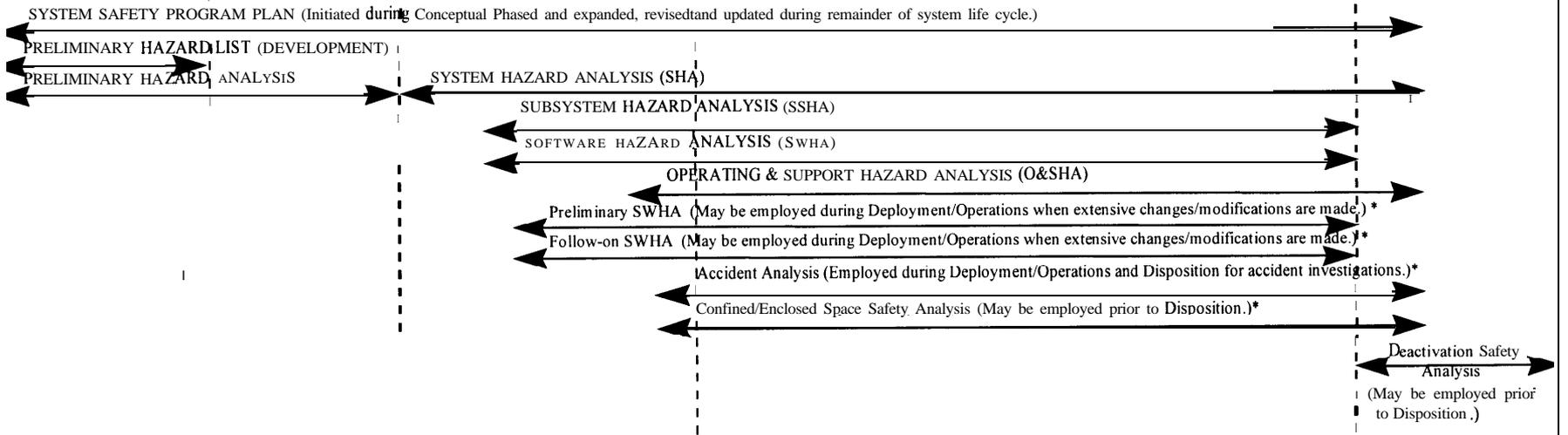
* Subordinate to and incorporated into PHA, SHA, SSHA or O&SHA.

SYSTEM SAFETY ENGINEERING PROCESS

SYSTEM DESIGN, ENGINEERING AND INTEGRATION PROCESS

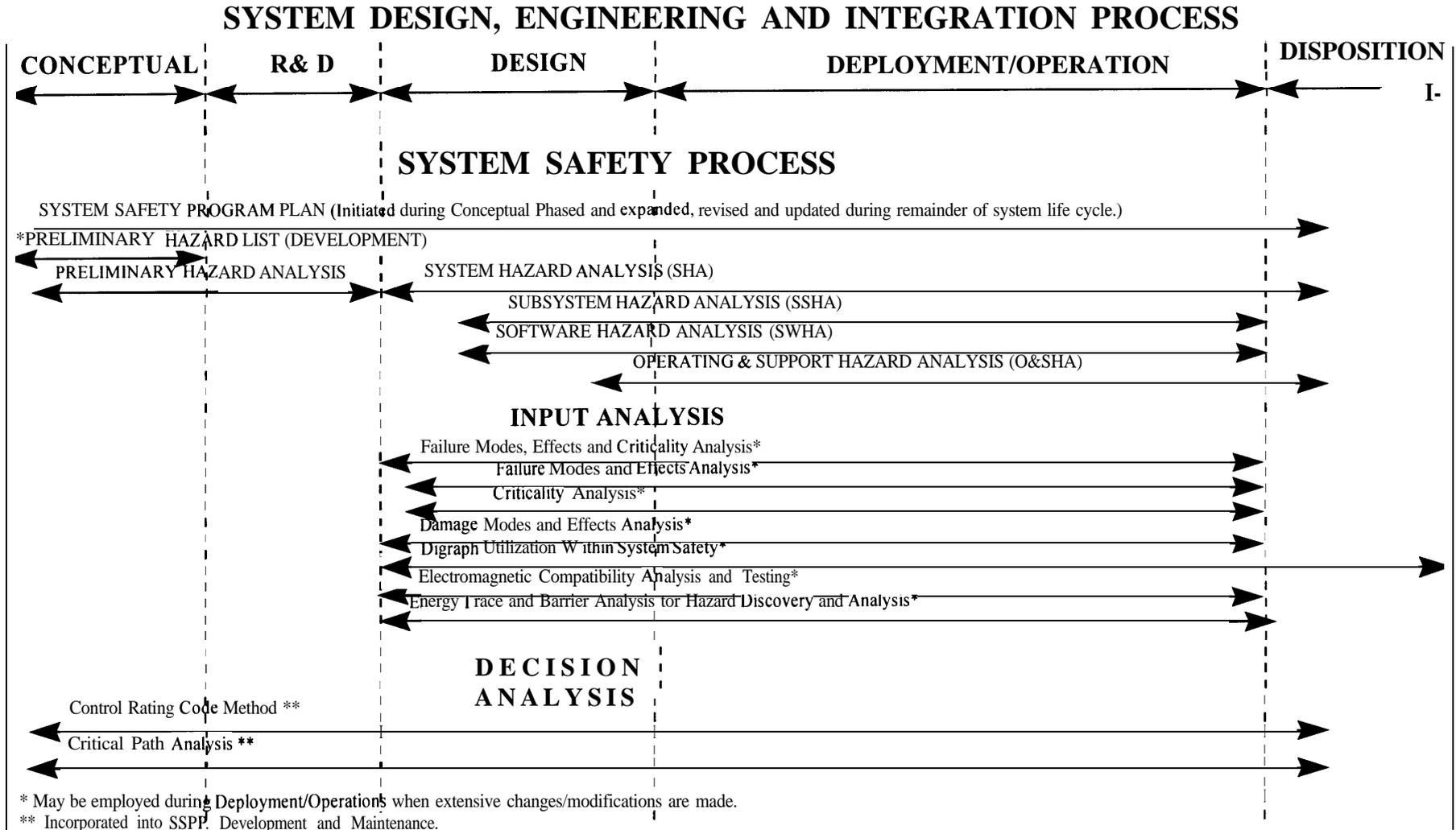
← CONCEPTUAL! → R&D → DESIGN → DEPLOYMENT/OPERATION → DISPOSITION

SYSTEM SAFETY ENGINEERING PROCESS



* Subordinate to and incorporated into PHA, SHA, SSHA or O&SHA.

SYSTEM SAFETY ENGINEERING PROCESS



Attachment 2

DRAFT

Sample

Reusable Launch Vehicle

SYSTEM SAFETY PROGRAM PLAN

Preface

The following sample System Safety Program Plan (SSPP) is based on a hypothetical applicant creating its own System Safety Program by tailoring MIL- STD- 882C “System Safety Program Requirements” to a commercial RLV Program. MIL-STD-882 was selected for this example because of likelihood of greater familiarity within industry with this standard, however, other similar standards exist that could be effectively tailored to this task. This material was created only for illustration purposes. It is intended to demonstrate a systematic, logical, and disciplined approach for early hazard identification, and elimination or reduction, during the overall design and development and operation of a Reusable Launch Vehicle system. This material demonstrates one means of developing an SSPP, and is not a regulatory requirement.

Format: In addition to the sample SSPP text, which is indicated by plain text, the document includes applicable excerpts from MIL-STD-882C in *Italics* at the beginning of selected sections. There are also additional notes and observations included where applicable in reduced font bold text.

TABLE OF CONTENTS

Section	Title	Page
	Preface	ii
1.0	INTRODUCTION	1
2.0	PURPOSE OF SYSTEM SAFETY PROGRAM	1
3.0	PROGRAM SCOPE AND OBJECTIVES	2
3.1	TASKS AND ACTIVITIES	3
3.1.1	SAFETYRELATEDTASKS	4
4.0	SYSTEM SAFETY ORGANIZATION	5
5.0	SYSTEM SAFETY PROGRAM MILESTONES	6
6.0	REQUIREMENTS AND CRITERIA	7
6.1	RISK ASSESSMENT	10
6.1.1	HAZARD SEVERITY	11
6.1.2	HAZARD PROBABILITY	11
6.2	RISK ACCEPTABILITY CRITERIA	12
6.3	SAFETY ACTION TRACKING	13
6.4	HAZARD TRACKING	13
7.0	HAZARD ANALYSIS	14
7.1	PRELIMINARY HAZARD ANALYSIS (PHA)	16
7.2	SAFETY REQUIREMENTS/CRITERIA ANALYSIS(SRCA)	18
7.3	SUBSYSTEM HAZARD ANALYSIS (SSHA)	20
7.4	SYSTEM HAZARD ANALYSIS (SHA)	21
7.5	OPERATING AND SUPPORT HAZARD ANALYSIS	22
7.6	SOFTWARE SAFETY	24
8.0	SYSTEM SAFETY DATA	24
9.0	SAFETY VERIFICATION	25
9.1	REUSED / REFLOWN HARDWARE	25
10.0	AUDIT PROGRAM	25
11.0	MISHAP AND HAZARDOUS MALFUNCTION ANALYSIS AND REPORTING	26
12.0	INTEGRATION AND MANAGEMENT OF ASSOCIATE CONTRACTORS AND SUBCONTRACTORS	26
ANNEX 1	HAZARD REPORT AND ANALYSIS FORMAT	28

1.0 INTRODUCTION:

NOTE: This sample System Safety Program Plan (SSPP) is provided for guidance and information on developing a Reusable Launch Vehicle System Safety Program Plan that addresses public safety considerations. The methods and procedures described herein illustrate one acceptable SSPP but are not the only ones acceptable to the Federal Aviation Administration. It is recognized that many applicants will also use this same process to identify and control other RLV program safety hazards such as ground crew and flight crew hazards. It is acceptable to address all the RLV safety related activities in a System Safety Program Plan even if they do not relate to public safety. However, the FM will only assess the activities that may impact public safety.

This is the ABC Space Systems Company's System Safety Program Plan (SSPP) for the XYZ Program. It covers the design and fabrication of the XYZ vehicle, its ground operations, launch facilities, support equipment, flight tests, and subsequent operations of the vehicle system.

The purpose of the SSPP is to describe the tasks and activities of system safety management and engineering required during the XYZ program to identify, evaluate, and eliminate hazards, or reduce the associated risk to a level acceptable to Program Management and the FAA. This plan provides direction and guidance between ABC Space Systems and all its associated contractors as to how the system safety program will be accomplished.

The XYZ System Safety program described in this plan will be conducted jointly by the System Safety organizations of ABC Space Systems, Reliable Rocket Engines Inc., Guidance to the Stars Inc., Technical Operations Limited, Structures R Us, McNozzle's, etc.

The system safety organizations of each company will provide the necessary resources and coordinate and accomplish the tasks, activities, and data preparation required by the XYZ Team Statement of Work (*or equivalent*) in accordance with this plan. ABC Space Systems will provide direction to the associated contractors to integrate the System Safety Program and provide a single point of contact for program management on system safety issues.

2.0 PURPOSE OF SYSTEM SAFETY PROGRAM:

The System Safety Program Plan (SSPP) should describe in detail tasks and activities of system safety management and system safety engineering required to identify, evaluate, and eliminate/ control hazards, or reduce the associated risk to a acceptable level throughout the system life cycle. The approved plan provides a formal basis of understanding on how the system safety program will be executed to meet all requirements.

The purpose of the XYZ System Safety Program is to help ensure that safety, consistent with ABC Space Systems Company and FAA requirements, is designed into the XYZ system, including its subsystems, supporting equipment, operations and interfaces. During development of the XYZ program, the emphasis will be on assuring the safety of the XYZ vehicle and associated personnel, the public, and private and public property.

3.0 PROGRAM SCOPE AND OBJECTIVES:

*The SSPP should describe, as a minimum, the four elements of an effective system safety program: a planned approach for task accomplishment, **qualified** people to accomplish tasks, authority to implement tasks through all levels of management, and appropriate commitment of resources (both **staffing** and funding) to assure tasks are completed. The SSPP should define a program to satisfy the public safety-related system safety requirements. This section should:*

- a. Describe the scope of the overall program and the related system safety program.*
- b. List the tasks and activities of system safety management and engineering. Describe the interrelationships between system safety and other functional elements of the program. List the other program requirements and tasks applicable to system safety and identify where they are specified or described.*
- c. Account for all FAA required safety tasks and responsibilities. A matrix should be provided to correlate the requirements to the location in the SSPP where the requirement is addressed.*

The XYZ vehicle is scheduled to start flight tests on July 04, 1999. The objectives of the tests are to obtain flight data on the XYZ Reusable Launch Vehicle (RLV). Specific objectives of the tests include verification of vehicle performance, validation of the design, identification of system deficiencies, and demonstration of safe operations. Following the successful completion of the flight test program the vehicle will become operational and begin to carry cargo into space.

The principal System Safety objective is to protect public safety, and to ensure safe and successful flight operations can be conducted within minimum acceptable risk limits. Other objectives of the System Safety Program are:

- To identify hazards and implement safety features and requirements during the design phase which provide the optimum degree of system safety consistent with mission requirements;
- To ensure that system safety issues are properly considered with respect to conducting ground tests, ground servicing, initial flight tests, and the flight and reentry operations of the XYZ;
- To maximize the safety of the public and property during all phases of the XYZ program;
- To provide lessons learned for application to the design and operation of the XYZ RLV.

3.1 TASKS AND ACTIVITIES:

The tasks and activities listed in Figure 3-1 will be accomplished by the system safety organizations of the companies that make up the XYZ Team in the conduct of the System Safety Program. The approaches to individual tasks or activities are described in the paragraphs of this plan referenced in Figure 3-1. The tasks listed in Figure 3- 1 will be shared by system safety organizations of the XYZ Team as they support the basic tasks assigned. For example, each contractor will perform a subsystem hazard analysis on the subsystems for which they have design responsibility, and prepare the corresponding portions of the Subsystem and System Hazard Analysis Reports. Unless otherwise stated, the approaches to the tasks and activities listed below apply to all phases of the program, including design, manufacture, and operations (which includes ground and flight test, launch, recovery, and maintenance).

TASK	SSPP Paragraph	MIL-STD-882 Task
System Safety Program	All	100
System Safety Program Plan	All	101
Hazard Tracking	6.4	105
Test & Evaluation Hazard Analysis	7.0	302
Preliminary Hazard Analysis	7.1	202
Safety Requirements / Criteria Analysis	7.2	203
Subsystem Hazard Analysis	7.3	204
System Hazard Analysis	7.4	205
Operating & Support Hazard Analysis	7.5	206
Safety Verification	9.0	401
Audit Program	10.0	104
Integration/management of Subcontractors	12.0	103

Figure 3-1. Safety Tasks and Activities

3.1.1 Safety Related Tasks:

Many of the scheduled tasks and activities of organizations other than System Safety are safety related or have System Safety imbedded within them. The tasks and activities usually performed by other organizations or disciplines which are the most directly applicable to the System Safety tasks listed in Figure 3-1 are summarized in Figure 3-2.

ORGANIZATION/DISCIPLINE	SAFETY RELATED TASK
Quality Assurance (QA)	Establish a Quality Program suitable to XYZ System Safety objectives, QA Program Management, Vehicle/Hardware acceptance, QA Engineering, supplier selection, supplier quality surveillance and audits, production quality performance and evaluation, verification, configuration assurance, calibration /metrology, test assurance, material reviews, nonconformance reviews, process review and corrective action identification, quality data collection and reporting.
Reliability	Perform Reliability analysis, failure mode, effect, and criticality analysis (FMECA), reliability predictions, reliability critical item identification, reliability testing and demonstration, develop parts selection and derating criteria. Identify and resolve reliability issues on safety critical systems.
Maintainability	Provide a maintainability program that addresses safety critical system and subsystem maintenance and refurbishment considerations. Identify and track limited life items.
Design	Provide design hazard mitigation. Define verification/test requirements for design features.
Flight Test	Provide test procedures and hazard mitigation.
Subcontractors/Vendors	Provide reliability/quality, and safety data on components designed or supplied.

Figure 3-2 Safety Tasks Performed by other Organizations

4.0 SYSTEM SAFETY ORGANIZATION:

The SSPP should describe:

- a. *The system safety organization or function within the organization **of** the total program using charts to show the organizational and functional relationships, and lines **of** communication. **The** organizational relationship between other functional elements having responsibility **for** tasks with system safety impacts and the system safety management and engineering organization should be shown. Review and approval authority **of** applicable tasks by system safety.*
- b. *The responsibility and authority **of** system safety personnel, other organizational elements involved in the system safety effort, subcontractors, and system safety groups. The methods by which safety personnel may raise issues **of** concern directly to the program manager or the program manager's supervisor within the corporation. Organizational unit responsible **for** executing each task. Authority in regard to resolution **of** all identified hazards.*
- c. ***The staffing of** the system safety organization **for** the duration **of** the project to include manpower loading, control **of** resources and a summary **of** the qualifications **of** key system safety personnel assigned to the effort, including those who possess coordination/approval authority **for** documentation.*
- d. ***The procedures by which the developer will integrate and coordinate the system safety efforts including assignment of** the system safety requirements to action organizations and subcontractors, coordination **of** subcontractor system safety programs, integration **of** hazard analyses, program and design reviews, program status reporting, and system safety groups.*
- e. *The process through which management decisions will be made including timely notification **of** unacceptable risks, necessary action, incidents or malfunctions, waivers to (ABC Space Systems and/or FAA) safety requirements, program deviations, etc.*
- f. *Details **of** how resolution and action relative to system safety will be **effected** at the program management level possessing resolution authority.*

The XYZ System Safety Program will be conducted jointly by the system safety organizations of the XYZ team associates. ABC Space Systems will act as integrator and will assign tasks to appropriate team members to accomplish the System Safety Program. The system safety tasks assigned to each associate team member will support the work agreed to by their respective organizations and take advantage of their safety expertise in specific areas. Program format, mutually agreed to between ABC Space Systems and each associate will be used.

Qualifications TBD.

XYZ Program System Safety personnel will generally report directly to the applicable company's XYZ Program Manager. Key personnel are:

<u>COMPANY</u>	<u>NAME</u>	<u>WORK PHONE</u>
ABC Space Systems	John Doe, XYZ Program System Safety Manager	(800) 123-4567
Reliable Rocket Engines	Jane Doe	(123) 987-6543
Etc.		

5.0 SYSTEM SAFETY PROGRAM MILESTONES:

The SSPP should:

- a. *Define system safety program milestones. Relate these to major program milestones, program element responsibility, and required inputs and outputs.*
- b. *Provide a program schedule of safety tasks including start and completion dates, reports, and reviews.*
- c. *Identify subsystem, component, software safety activities as well as integrated system level activities (Le., design analyses, tests, and demonstrations) applicable to the system safety program but specified in other engineering studies and development efforts to preclude duplication.*
- d. *Provide the estimated manpower loading required to complete each task.*

Note: To facilitate the FAA's review and assessment activities, it is recommended that an applicant implement a process whereby the FM is (in the loop) continuously informed of safety critical design, manufacture, integration, test and verification activities. In order for the FAA to support the design and safety review milestones proposed by an RLV system developer, the FM will need to have access to the detailed review data well in advance of the review so that it may perform analysis and assessment activities. This type of a process will aid in providing thorough and timely reviews and will expedite identification of significant issues early in the process and avoid significant schedule impacts.

The XYZ RLV is a new vehicle development program and as a result the System Safety Program Milestones are scheduled to coincide with the traditional design review milestones. Major events and dates are as follows:

- Preliminary Design Review/Preliminary Hazard Analysis, December 1, 1999.
 - Preliminary Hazard Review, December 5, 1999
- Critical Design Review/Subsystem Hazard Analysis (SSHA), November 1, 2000.
 - Subsystem Hazard Review, December 5, 2000.
- System Hazard Review, March 25, 2002.
 - First Flight Teat Readiness Review/ System Hazard Analysis (SHA) complete, April 28, 2002 (Approximately 90 days prior to First Flight)

- First Flight Test, July 4, 2002.

Note: In this example the PDR is scheduled approximately 3.5 years in advance of the expected first flight test. The earlier the system safety process is started in the development cycle the more likely safety considerations will be designed into the system and operational concepts thus avoiding costly and potentially ineffective design changes and retrofits.

6.0 REQUIREMENTS AND CRITERIA:

The SSPP should:

- Describe general engineering requirements and design criteria for safety. Describe safety requirements for support equipment and operational safety requirements for all appropriate phases **of the life cycle up to, and including, disposal.** List the safety standards and system specifications containing safety requirements that are to be complied with by the team members. Include titles, dates, and where applicable, paragraph numbers.*
- Describe the risk assessment procedures. **The hazard severity categories, hazard probability levels, and the system safety precedence that is to be followed to satisfy the safety requirements of the program.** State any qualitative or quantitative measures **of safety to be used for risk assessment including a description of the acceptable/unacceptable risk levels.** Include system safety definitions.*
- Describe closed-loop procedures **for taking action to resolve identified unacceptable risk including those involving nondevelopmental items.***

Safety requirements and design criteria for the XYZ Program are identified through FAA Regulations and Guidance Material, and additionally, will be established as a result of hazard analyses performed, the Safety Requirements and Criteria Analysis, use of lessons learned from similar programs, and company design safety requirements. In general, safety requirements will be established to control the safety risk associated with individual hazards to levels acceptable to the XYZ Program Management and the FAA.

For the XYZ Program, the order of precedence for establishing recommended hazard control measures is:

- (a) Design to eliminate hazard/risk
- (b) Incorporate Safety Devices
- (c) Provide Warning Devices
- (d) Develop Procedures and Training

In addition to the hazard reduction precedence all XYZ public safety critical systems and functions will incorporate the following ABC Space Systems-required fault tolerance and risk mitigation approaches.

Failure Tolerance: The XYZ vehicle must tolerate a minimum number of credible failures and/or operator errors. This criterion applies to the XYZ operations when loss of a function or inadvertent occurrence of a function results in a hazardous event (risk to public safety).

The XYZ Vehicle safety critical command and control functions will be designed to be at least two fault tolerant. (i.e. No combination of two failures or operator errors shall result in the potential for loss of control of the vehicle or, death or injury to the public.)

A function that could lead to death or injury to the public shall be controlled by a minimum of three independent inhibits, whenever the hazard potential exists.

Monitoring of these inhibits shall be available to verify that at least two of the three inhibits are in place.

Figure 6.1 “XYZ Public Safety Strategy” depicts the integrated elements of the public safety strategy applied to the XYZ program. The XYZ public safety strategy incorporates the system safety process outlined in this System Safety Program Plan in combination with Expected Casualty Analysis and the use of prudent Operational Controls (objectives) specified by the FAA and ABC Space Systems.

XYZ Public Safety Strategy

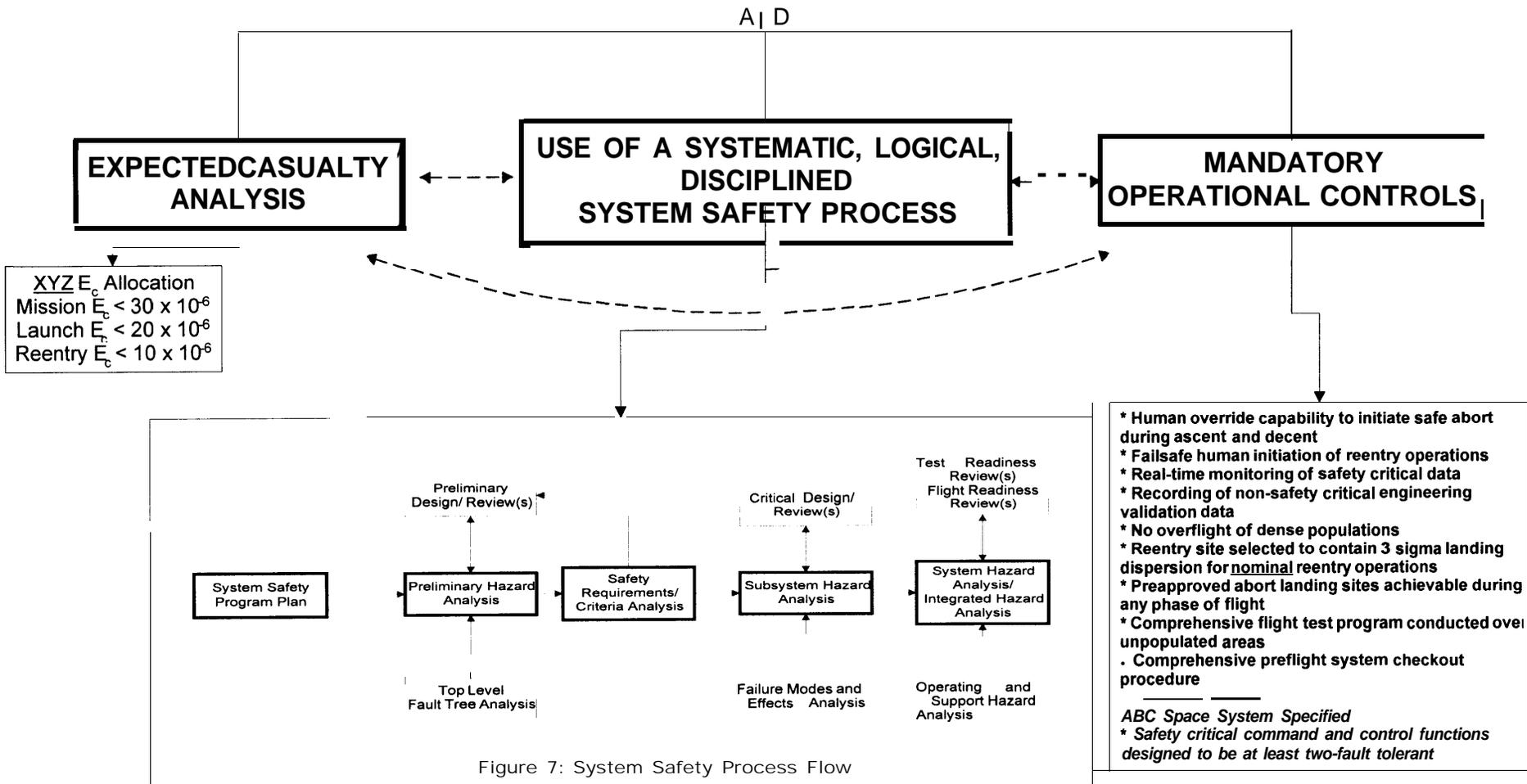


Figure 7: System Safety Process Flow

Figure 6.1 XYZ Public Safety Strategy

6.1 RISK ASSESSMENT:

Risk is a function of the combination of the severity (consequences) and the probability (frequency of occurrence) categories. The risk assessment will generally be qualitative. The qualitative measures of severity and probability are described in sections 6.1.1 and 6.1.2 respectively.

NOTE: Quantitative measures are provided with the Hazard Probability Levels to provide the applicant with a basis for assigning probability categories. It is recognized that for most of the subsystems that make up new RLV systems there will not be sufficient performance and reliability data supported by flight history to perform a credible quantitative analysis. Even when a system, subsystem or component is known to have an extensive and favorable flight history in the same or more severe environment, the interfaces and integration with other systems will likely be dissimilar enough to make any quantitative analysis suspect and provide results with very low confidence levels.

NOTE: All (risk) assessment methodologies are subjective to some extent. By using the severity and probability categories contained on tables 6.1.1 and 6.1.2, the analyst has a basis for assigning a designation. However, the frequency and severity designations do require a level of engineering judgement. If, in the analyst's judgement, the severity or frequency of a hazard is on the borderline between two categories, the analyst should select the more conservative designation. (i.e. If a hazard severity is judged to be between critical and catastrophic, the analyst should designate the hazard as catastrophic. If the probability is borderline between occasional and remote the analyst should designate the hazard as occasional. It is almost always more desirable to err on the conservative (safe) side and perhaps achieve a system design that is more robust than is necessary than to discover late in the development or during operations that an expensive and potentially ineffective redesign or retrofit is required.

6.1.1 Hazard Severity:

The hazard severity categories defined below are used.

DESCRIPTION	CATEGORY	MISHAP DEFINITION
Catastrophic	I	Death or system loss
Critical	II	Severe injury, <i>severe occupational illness</i> , or major system damage
Marginal	III	Minor injury, <i>minor occupational illness</i> , or minor system damage
Negligible	IV	Less than minor injury, <i>occupational illness</i> , or system damage

Table 6.1.1: Hazard Severity

6.1.2 Hazard Probability:

The hazard probability categories defined below are used.

DESCRIPTION	LEVEL	INDIVIDUAL ITEM
Frequent ($X > 10^{-1}$)	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.
Probable ($10^{-1} > X > 10^{-2}$)	B	Will occur several times in the life of an item with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.
Occasional ($10^{-2} > X > 10^{-3}$)	C	Likely to occur some time in the life of an item with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.
Remote ($10^{-3} > X > 10^{-6}$)	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.
Improbable ($10^{-6} > X$)	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.

Table 6.1.2: Hazard Probability

6.2 RISK ACCEPTABILITY CRITERIA:

The acceptability of risk will be determined for individual hazards by comparing the hazard risk index (HRI) with the HRI acceptability criteria. The HRI is a number from 1 to 20, which ranks the risk, with 1 representing the highest risk. The hazards with the highest HRIs will receive priority for corrective action. Figure 6- 1 a shows HRI values corresponding to the qualitative severity and probability categories, which were described in the previous sections. The HRI acceptability criterion is listed below in Figure 6-1b.

FRE- QUENCY OF OCCURRENCE	HAZARD SEVERITY	I CATASTROPHIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
	(A) Frequent		1	3	7
(B) Probable		2	5	9	16
(C) Occasional		4	6	11	18
(D) Remote		8	10	14	19
(E) Improbable		12	15	17	20

Level	Index	Acceptability Criteria
High	1 - 6	Corrective/controlling actions must be taken to reduce the hazard severity below "III" or reduce the probability/frequency of occurrence below "C".
Medium	7 - 10	If not corrected, must be presented to XYZ Program Management and FAA as accepted risk.
Low	11 - 20	Project Management decision on actions.

Figure 6.2. Hazard Risk Index Matrix

6.3 SAFETY ACTION TRACKING

Note: A closed loop safety action tracking system may be useful to help assure that all risk resolution activities required and undertaken by one of the system/subsystem developers is communicated, understood, and assessed for potential effects on the other critical RLV systems.

ABC Space Systems has instituted a closed loop safety action tracking system to help assure that all risk resolution activities required and undertaken by one of the system/subsystem developers is communicated, understood, and assessed for potential effects on the other critical XYZ systems. This closed loop safety action tracking function will be accomplished through the use of XYZ Safety Action Tracking Records (SATR). SATRs will be used for all system safety written correspondence on XYZ program safety issues including the following:

- Transmittal of safety requirements that result from the hazard analysis activities and the Safety Requirements/Criteria Analysis
- System Safety Actions that result from Safety Reviews or Design Reviews.
- Safety Guidance or explanation of system safety position on safety related issues
- Transmittal of mishap and lessons learned data
- Transmittal of significant parts, manufacturing or process alerts
- Requests for data or analysis necessary to resolve safety issues

Any company's System Safety Organization may originate XYZ SATR's. As the XYZ system integrator, ABC Space Systems will be addressed or copied on all SATR's and will determine which other XYZ Team companies will be notified. In addition, ABC Space Systems will maintain a complete file of all XYZ SATR's and responses. In the event a response is not acceptable, the issue will be referred to progressively higher management levels until acceptable actions are taken or an appropriate management level has accepted the risk. FAA/AST should be provided copies of all accepted XYZ SATR's that are related to ensuring public safety.

6.4 HAZARD TRACKING:

Hazard Report forms (HRs) will be used to track identified hazards to assure that the actions taken to control the risks are acceptable to System Safety and to the XYZ Program Management. The signatures of the ABC Space Systems System, Safety Manager and Program Manager will be required to close all hazards discovered and resolved during analysis by XYZ Team members. All hazards discovered (including those resolved "informally") shall be recorded on an HR form, as well as in the analyses described in paragraph 7.0 below. See Annex 1 for HR form sample and details.

7.0 HAZARD ANALYSIS:

The SSPP should describe:

- a. The analysis techniques and formats to be used in qualitative or quantitative analysis to identify hazards, their causes and **effects**, hazard elimination, or risk reduction requirements and how those requirements are met.
- b. The depth within the system to which each technique is used including hazard identification associated with the system, subsystem, components, software, hazardous materials, personnel, ground support equipment, nondevelopmental items, facilities, and their interrelationship in the logistic support, training, maintenance, operational and disposal (including render safe and emergency disposal) environments.
- c. The integration of subcontractor hazard analyses with overall system hazard analyses.
- d. Efforts to identify and control hazards associated with materials used during the system's life cycle.

Hazard analyses will be performed to identify hazards, their causes and effects, controls to eliminate or mitigate the hazards, risk assessment, and status of hazard resolution. The time phasing of the actual work being done to perform the system safety analysis of the total system leads to the labeling of the analyses produced by traditional names; Preliminary Hazard Analysis, Subsystem Hazard Analysis, and System Hazard Analysis. (See Figure 7.0) For the XYZ program, the intent is to have a database containing all of the hazards involved with the total system throughout its life cycle. Within this database, individual hazards will be identified as relating to the areas normally covered in the traditional hazard analyses discussed below.

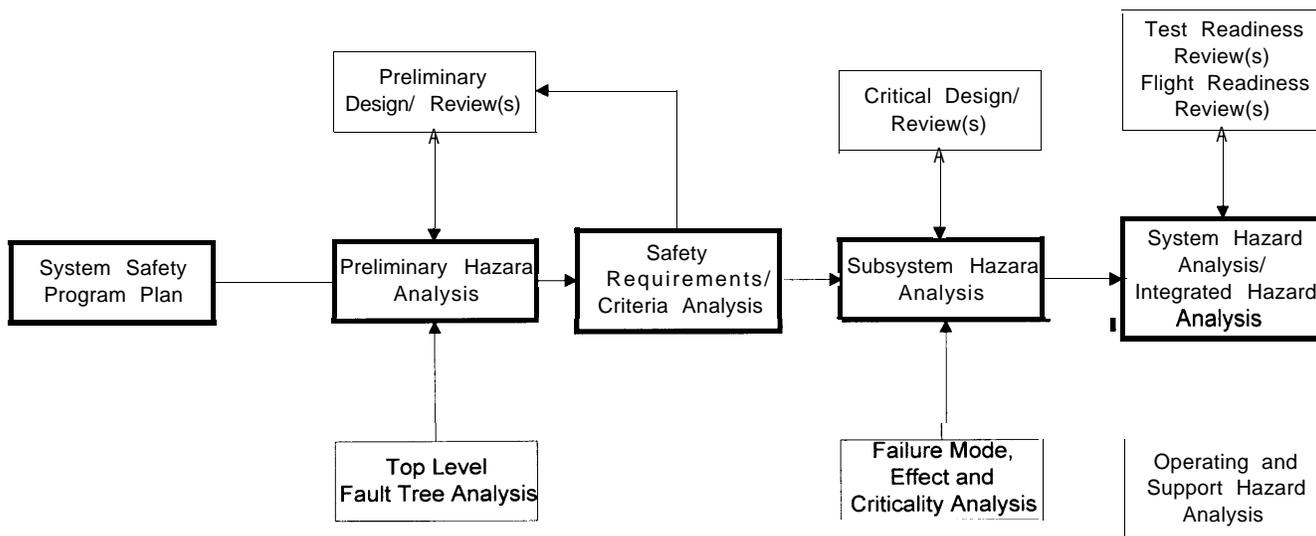


Figure 7: System Safety Process Flow

The Safety Requirements/Criteria Analysis (SRCA) will use the hazards identified by the PHA and the safety criteria specified by ABC Space Systems and the FAA, to develop vehicle system and subsystem design requirements to eliminate or reduce the risk of identified hazards to an acceptable level. Requirements that result from the SCRA will be transferred to the appropriate system/subsystem developers using the Safety Action Tracking Record (SATR) process described in section 6.3.

Operating and Support Hazard Analyses (O&SHA) cover hazards that arise during the use and or maintenance of a system. Hardware failure may be involved in these hazards, but often is not a factor at all. Normal procedures for operation and maintenance, emergency procedures to cope with failures, and the effect of system design on operators and maintainers and their ability to perform properly are considered part of an O&SHA. These types of hazards shall be covered and included in the database as they are discovered.

Note: In this example the Program Management has elected to use a single hazard data base for tracking all safety related issues, not just public safety related hazards. For many programs, the safety of their ground and flight crews will be of the same level of importance as public safety. In those cases it will likely be more efficient to track all safety hazards (public, flight and ground crews, and protection of the asset [vehicle]) using a single hazard tracking mechanism such as the hazard data base described in this example. In addition, safety of the vehicle is often directly or indirectly tied to safety of the public such that it is hard to draw the distinction.

Software (and Firmware) Safety shall be included in all analyses in that the software imbedded in or necessary to the operation of a component, subsystem or operation shall be included in the analysis of the area the same as a piece of hardware. Software involvement is also identified specifically in each Hazard Report. For the purposes of this analysis firmware will be addressed in the software portion of the Hazard Report.

Test Hazard Analyses are performed to identify hazards during ground and flight tests. They include the hazards in the equipment, procedures, hardware and software necessary to complete safe and successful tests in all areas of testing (development, qualification, and acceptance). These types of hazards are included in the database.

The approach discussed above allows for review of the database with an emphasis on any desired area; Test, Maintainability, Software, *etc.*. The specific analyses to be performed are as follows.

7.1 PRELIMINARY HAZARD ANALYSIS:

***PURPOSE.** To perform and document a Preliminary Hazard Analysis (PHA) to identify safety critical areas, to provide an initial assessment of hazards, and to identify requisite hazard controls and follow-on actions.*

TASK DESCRIPTION. Perform and document a preliminary hazard analysis to obtain an initial risk assessment **of** a concept or system. Based on the best available data, including mishap data (if assessable) from similar systems and other lessons learned, hazards associated with the proposed design or function should be evaluated **for** hazard severity, hazard probability, and operational constraint. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to the FAA should be included. The **PHA** should consider the following **for** identification and evaluation **of** hazards as a minimum:

- a. Hazardous materials and components (e.g., **fuels**, propellants, lasers, explosives, toxic substances, hazardous construction materials, pressure systems, and other energy sources).
- b. Safety related **interface** considerations among various elements **of** the system (e.g., material compatibility's, electromagnetic interference, inadvertent activation, fire/explosive initiation and propagation, and hardware and **software** controls). This should include consideration **of** the potential contribution by software (including **software** developed by other sources) to subsystem/system mishaps. Safety design criteria to control safety-critical **software** commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, inappropriate magnitude, or other undesired events) should be identified and appropriate action taken to incorporate them in the **software** (and related hardware) specifications.
- c. Environmental constraints including the operating environments (e. g., drop, shock, pressure, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and non-ionizing radiation including laser radiation).
- d. Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures (e.g., human factors engineering, human error analysis **of** operator-functions, tasks, and requirements; effect **of** factors such as equipment layout, lighting requirements, potential exposures to toxic materials, effects **of** noise or radiation on human performance; explosive ordnance render safe and emergency disposal procedures; life support requirements and their safety implications in manned systems, crash safety, egress, rescue, survival, and salvage). Those test unique hazards which will be a direct result **of** the test and evaluation **of** the vehicle.
- e. Facilities, real property installed equipment, support equipment (e.g., provisions **for** storage, assembly, checkout, **prooftesting** **of** hazardous systems/assemblies which may involve toxic, flammable, explosive, corrosive or cryogenic materials/wastes; radiation or noise emitters; electrical power sources) and training (e. g. training and certification pertaining to safety operations and maintenance).
- f. Safety related equipment, safeguards, and possible alternate approaches (e. g., interlocks; system redundancy; fail safe design considerations using hardware or software controls; subsystem protection; fire detection and suppression systems;

personal protective equipment; heating, ventilation, and air-conditioning; and noise or radiation barriers).

- g. Malfunctions to the system, subsystems, or software. Each malfunction should be specified, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and/or design changes developed.*

The preliminary hazard analysis (PHA) will be started as soon as design work has begun so that safety considerations are used to evaluate design alternatives and trade studies. The PHA should be used to identify hazards and assist in establishing safety requirements as early in the program as possible. A common format for the PHA will be used to facilitate tracking and transfer of Hazard Reports between companies where necessary. The PHA will be used as the baseline for performing future analyses, such as the SSHA, SHA, and O&SHA. See Annex 1 for details and examples of the Hazard Report forms and format (data fields). The XYZ Description Documents, such as the Baseline System Description, and Avionics Systems Description, Propellant Feed/Pressurization System Description, Flight Safety System *et al.*, will serve as the System Descriptions for the PHA and all subsequent analyses. ABC Space Systems recommends a Functional Hazard Assessment (FHA) technique for the PHA.

The PHA will be presented at the Preliminary Design Review. Each company is responsible for performing the analysis and submitting the analysis to ABC Space Systems for that portion of the XYZ design and/or operation for which they have accepted responsibility. ABC Space Systems will consolidate all inputs and keep them available for Program Management and FAA review.

Note: The safety analyst must be familiar with the conceptual system and its planned functions and interfaces. The analyst will need to use data such as preliminary systems and mission descriptions, flow diagrams, design drawings, operational concepts, and other technical data as may be available.

7.2 SAFETY REQUIREMENTS/CRITERIA ANALYSIS

PURPOSE. To perform and document the safety design requirements/design criteria for a system under development/design.

TASK DESCRIPTION. The Safety Requirements/Criteria Analysis (SRCA) relates the hazards identified to the system design and identifies or develops design requirements to eliminate or reduce the risk of the identified hazards to an acceptable level. The SRCA uses the Preliminary Hazard Analysis as a basis. The SRCA is also used to incorporate design requirements that are safety related but not tied to a specific hazard. The analysis includes the following efforts:

Determine applicable generic system safety design requirements and guidelines for facilities; hardware and software from federal, military, national and industry regulations, codes, standards, specifications; and other documents for the vehicle system under development. Incorporate these requirements and guidelines into the high level system specifications and design documents as appropriate.

Analyze the System Design Requirements, System/Segment Specifications, Preliminary Hardware Configuration Item Development Specification, Software Requirements Specifications, and the Interface Requirements Specifications, or equivalent documents as appropriate, to include the following sub-tasks:

- a. Ensure that the system safety design requirements and guidelines are developed; refined; correctly and completely specified; properly translated into system hardware and software requirements and guidelines where appropriate; and implemented in the design and development of the system hardware and associated software.*
- b. Identify hazards and relate them to the specifications or documents listed above and develop design requirements to reduce the risk **of** those hazards.*
- c. Identify safety critical computer software components and place them under configuration control.*
- d. Analyze the preliminary system design to identify potential hardware/ software interfaces at a gross level that may cause or contribute to potential (**public safety**) hazards. Interfaces identified should include control functions, monitoring functions, safety systems and functions that may have indirect impact on safety. These interfaces and the associated software should be designated as safety critical.*
- e. Perform a preliminary hazard risk assessment on the identified safety critical software functional requirements using the hazard risk index matrix.*
- f** Ensure that System Safety design requirements are properly incorporated into the operator, user, and diagnostic manuals.*

Develop safety related design change recommendations and testing requirements and incorporate them into Preliminary Design Documents and the hardware, software and system test plans. The following sub-tasks should be accomplished:

- a. Develop safety-related change recommendations to the design and specification documents and include a means **of** verification **for** each design safety requirement.*
- b. Develop safety related test requirements **for** incorporation into the test documents. Tests should be developed **for** hardware, software and system integration testing.*
- c. Support the System Requirements, System Design and Software Specification development from a system safety viewpoint. Address the system safety program, analyses performed and to be performed, significant hazards identified, hazard resolutions or proposed resolutions, and means **of** verification.*

The Safety Requirements/Criteria Analysis (SRCA) will be performed by ABC Space Systems (with input from the entire XYZ Team) in conjunction with, or immediately following the Preliminary Hazard Analysis. The SRCA will use the hazards identified by the PHA and the safety criteria specified by ABC Space Systems and the FAA, to develop vehicle system and subsystem design requirements to eliminate or reduce the risk of identified hazards to an acceptable level consistent with the system safety strategy applied.

The ABC System Safety Manager and the XYZ Program Manager will assure that all necessary system safety design requirements, criteria, and guidelines are developed, refined, and correctly and completely specified and translated into system hardware and software requirements and guidelines. In addition, the ABC System Safety Manager and the XYZ Program Manager will assure that all these requirements, criteria, and guidelines are flowed down to the subsystem developers. The subsystem System Safety and Program Managers will assure that all of these system safety requirements, criteria, and guidelines are adhered to in the subsystem design and verification activities.

Top level system safety requirements specified by ABC space systems includes:

Failure Tolerance: The XYZ vehicle must tolerate a minimum number of credible failures and/or operator errors. This criterion applies to the XYZ operations when loss of a function or inadvertent occurrence of a function results in a hazardous event (Risk to the public safety).

The safety critical command and control functions will be designed to be at least two fault tolerant. (i.e. No combination of two failures or operator errors shall result in the potential for loss of control of the vehicle or, death or injury to the public.)

A function that could lead to death or injury to the public shall be controlled by a minimum of three independent inhibits, whenever the hazard potential exists.

Monitoring of these inhibits shall be available to verify that at least two of the three inhibits are in place.

7.3 SUBSYSTEM HAZARD ANALYSIS:

***PURPOSE.** Perform and document a Subsystem Hazard Analysis (SSHA) to: verify subsystem compliance with safety requirements contained in subsystem specifications and other applicable documents; identify previously unidentified hazards associated with the design **of** subsystems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem; recommend actions necessary to eliminate identified hazards or control their associated risk to acceptable levels.*

***TASK DESCRIPTION.** Perform and document a subsystem hazard analysis to identify all components and equipment that could result in a hazard or whose design does not satisfy safety requirements. Areas to consider are performance, **performance** degradation, functional failures, timing errors, design errors or defects, or inadvertent functioning. **The** human shall be considered a component within a subsystem, receiving both inputs and initiating outputs, during the conduct **of** this analysis.*

The analysis should include a determination:

- a. Of the modes **of** failure including reasonable human errors as well as single point and common mode failures, and the effects on safety when failures occur in subsystem components.*
- b. Of potential contribution **of** hardware and software (including that which is developed by other contractors/sources) events, faults, and occurrences (such as improper timing) on the safety **of** the subsystem.*
- c. **That** the safety design criteria in the hardware, software, and facilities specification (s) have been satisfied.*
- d. That the method **of** implementation **of** hardware, software, and facilities design requirements and corrective actions has not impaired or decreased the safety **of** the subsystem nor has it introduced any new hazards or risks.*
- e. Of the implementation **of safety** design requirements from top level specifications to detailed design specifications **for** the subsystem. The implementation **of safety** design requirements developed as part **of** the PHA and SRCA shall be analyzed to ensure that it satisfies the intent **of** the requirements.*
- f. Of test plan and procedure recommendations to integrate safety testing into the hardware and software test programs.*
- g. **That** system level hazards attributed to the subsystem are analyzed and that adequate control **of** the potential hazard is implemented in the design.*

*When software to be used in conjunction with the subsystem is being developed under other development documents; the developer performing the SSHA shall monitor, obtain, and use the output **of** each phase **of** the formal software development process in*

evaluating the software contribution to the SSHA. Problems identified which require the reaction of the software developer shall be reported to the system manager in time to support the ongoing phase of the software development process.

Update the SSHA as a result of any system design changes, including software design changes, which affect system safety.

The Subsystem Hazard Analysis (SSHA) shall be started immediately after the Preliminary Design Review. Each company shall perform the analysis on the portion of the system for which they are responsible, in the format outlined in Annex 1. The analysis will be based on detailed subsystem design data, PHA results, Failure Modes and Effects Analysis results, and safety design requirements for the subsystem. The SSHA must be complete by the Critical Design Review to the point that all subsystem hazards have been identified, mitigating actions planned, and verification requirements for these hazards identified. The SSHA will be briefed at the CDR and made available to XYZ Program management and the FAA. ABC Space Systems will coordinate the consolidation of inputs for the SSHA.

7.4 SYSTEM HAZARD ANALYSIS:

PURPOSE. Perform and document a System Hazard Analysis (SHA) to: verify system compliance with safety requirements contained in system specifications and other applicable documents; identify previously unidentified hazards associated with the subsystem interfaces and system functional faults; assess the risk associated with the total system design, including software, and specifically of the subsystem interfaces; and recommend actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels.

TASK DESCRIPTION. Perform and document a system hazard analysis to identify hazards and assess the risk of the total system design, including software, and specifically the subsystem interfaces.

This analysis shall include a review of subsystems interrelationships for:

- a. Compliance with specified safety design criteria.
- b. Possible independent, dependent, and simultaneous hazardous events including system failures; failures of safety devices; common cause failures and events; and system interactions that could create a hazard or result in an increase in mishap risk.
- c. Degradation in the safety of a subsystem or the total system from normal operation of another subsystem.
- d. Design changes that affect subsystems.
- e. Effects of reasonable human errors.

f. Determination:

- (1) Of potential contribution of hardware and software (including that which is developed by other contractors/sources, or Commercial Off-The-Shelf hardware or software) events, faults and occurrences (such as improper timing) on safety of the system.*
- (2) That the safety design criteria in the hardware, software, and facilities specification (s) have been satisfied.*
- (3) That the method of implementation of the hardware, software, and facilities design requirements and corrective actions has not impaired or degraded the safety of the system nor has introduced any new hazards.*

The SHA may be combined with and/or performed using similar techniques to those used for the SSHA.

When software to be used in conjunction with the system is being developed, the contractor performing the SHA shall monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SHA.

The system developer shall update the SHA as a result of any system design changes, including software design changes, which affect system safety.

The System Hazard Analysis (SHA) will be performed by ABC Space Systems with the support and assistance of all other Contractors and Team members. It will incorporate each company's SSHA into a system level analysis, with emphasis on system interfaces and interactions. Note that there is no formal start of the SHA. Hazards may be identified as SHA applicable at any time during the Program. Each Company shall ensure that all hazards discovered since the Critical Design Review have been added to their respective SSHA's and transmitted to ABC Space Systems. The SHA will be presented at the First Flight Readiness Review. Work on the analysis will continue past this time, however, until all actions required on identified hazards have been completed.

The purpose of the SHA is identical to the SSHA, but at the system level. (Once the subsystem levels have been established, combinations of subsystems make up a system. In turn, a group of systems may comprise another system until the top level is identified. Consequently, a system to one project may be a subsystem to another project.) In general, for a SHA the previous analyses are extended to encompass the total system. The unique aspect of the SHA is its consideration of the interfaces between subsystems that make up a system. In other words, it is a form of an integrated hazard analysis.

7.5 OPERATING AND SUPPORT HAZARD ANALYSIS:

Purpose. Perform and document an Operating and Support Hazard Analysis (O&SHY), both to evaluate activities for hazards or risks introduced into the system by operational and support procedures and to evaluate adequacy of operational and support procedures used to eliminate, control, or abate identified hazards or risks.

Task description. The developer should perform and document an O&SHA to examine procedurally controlled activities. The O&SHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons, considering: the planned system configuration or state at each phase of activity; the facility interfaces; the planned environments (or ranges thereof); the supporting tools or other equipment, including software-controlled automatic test equipment, specified for use; operational task sequence, concurrent task effects, and limitations; biotechnological factors; regulatory or contractually specified personnel safety and health requirements; and the potential for unplanned events including hazards introduced by human errors. The human should be considered an element of the total system, receiving both inputs and initiating outputs during the conduct of this analysis. The O&SHA must identify the requirements (or alternatives) needed to eliminate or control identified hazards, or to reduce the associated risk to a level that is acceptable under either regulatory or contractually specified criteria.

The analysis should identify:

- a. Activities that occur under hazardous conditions, their time periods, and the actions required to minimize risk during these activities/time periods. .
- b. Changes needed in functional or design requirements for system hardware, software, facilities, tooling, or support or test equipment to eliminate or control hazards or reduce associated risks.
- c. Requirements for safety devices and equipment, including personnel safety and life support equipment.
- d. Warnings, cautions, and special emergency procedures (e.g., egress, rescue, escape, render safe, explosive ordnance disposal, or back-out procedures), including those necessitated by failure of a computer software-controlled operation to produce the expected and required safe result or indication.
- e. Requirements for packaging, handling, storage, transportation, maintenance, and disposal of hazardous materials.
- f. Requirements for safety training and personnel certification.
- g. Effects of nondevelopmental hardware and software across any interface with other system components or subsystems.
- h. Potentially hazardous system states under operator control.
- i. Federal laws regarding the storage and handling of hazardous materials.

The O&SHA should document system safety assessment of procedures involved in system production, deployment, installation, assembly, test, operation, maintenance, servicing, transportation, storage, modification (including programming, and disposal.

For the XYZ program the Operating and Support Hazard Analysis (O&SHA) is conducted in parallel with the development of procedures for manufacturing, processing, and operation. The O&SHA will be used to examine procedurally controlled activities to identify hazards. For the XYZ program the hazard Report format included in Annex 1 incorporates the intent of the O&SHA into the PHA (and SCRA), SSHA, and SHA hazard analysis by incorporating human error considerations as potential hazard causes and incorporating safety devices, warning devices, and procedures/training as potential hazard controls for all the three phases of the hazard analysis.

7.6 SOFTWARE SAFETY

Software/Firmware hazard analysis is imbedded in the XYZ Program Hazard Analysis process through the PHA, SRCA, SSHA, and the SHA. Potential software causes for all potential hazards are to be addressed on each hazard Report see Hazard Report format in Annex 1. Additional or detailed software hazard analysis requirements may be identified through the PHA, Fault Tree analysis, and the Failure Modes and Effects and Criticality Analysis

8.0 SYSTEM SAFETY DATA:

The SSPP should:

- a. *Describe the approach **for** collecting and processing pertinent historical hazard, mishap, and safety lessons learned, data.*
- b. *Identify deliverable data by title and number, and means **of** delivery (e.g. hard copy, electronically, etc.).*
- c. *Identify non-deliverable system safety data and describe the procedures **for** accessibility and retention **of** data.*

System Safety data will be prepared and available for the scheduled Safety Reviews. Updates will be provided as necessary by each Company and coordinated by ABC Space Systems. All analyses generated during the program will be available to all participants. By using the data fields as specified in Annex 1 the XYZ Program safety data will be searchable by many different parameters or combinations of parameters including analysis phase, system, subsystem, component, risk level, risk severity, hazard risk index, mission phase, and hazard status.

9.0 SAFETY VERIFICATION:

The SSPP should describe:

- a. *The verification (test, analysis, inspection, etc.) requirements for making sure that safety is adequately demonstrated. Identify any certification requirements for software, safety devices or other special safety features (e.g., render safe and emergency disposal procedures).*
- b. *Procedures for making sure safety-related verification information is transmitted to the FAA for review and analysis.*
- c. *Procedures for ensuring the safe conduct of all tests*

Tests, demonstrations, analysis or inspection shall verify safety critical hardware, software, and procedural safety requirements. Safety critical hardware, software, and procedures are defined as those subsystems, systems, safety devices, and procedures necessary to preclude a catastrophic or critical hazard from occurring or whose failure or degradation can result in a catastrophic or critical hazard. The XYZ Hazard Report Database will have electronic copies (or linkages) of all verification data referenced in Hazard Reports. All XYZ program participants and the FAA will be provided remote access (read only) to the database. Data manipulation access will be controlled by ABC Space Systems.

9.1 REUSED/REFLOWN HARDWARE

XYZ Systems, Subsystems, components or elements that are to be reused or reflowed as part of another XYZ mission will be reviewed for the following:

1. Correction of any safety deficiency encountered during a previous mission
2. Safety impact of any changes made to hardware or operating procedures.
3. Any maintenance and / or refurbishment affecting safety.
4. Appropriate design and verification features for reuse.
5. Safety of reuse in view of gradual hardware degradation (including fatigue) from previous use.
6. Any limited life items that may affect safety.

Note: Each applicant will need to define a systematic, logical, disciplined and thorough process for the identification and evaluation of reuse issues involving their system.

10.0 AUDIT PROGRAM:

The SSPP should describe the techniques and procedures to be employed by the developers to make sure the objectives and requirements of the system safety program are being accomplished.

An audit program will be initiated to ensure that the objectives and requirements of the system safety program are being accomplished. Safety Reviews for the XYZ Program will be conducted per section 5.0. System Safety issues will be addressed during Technical Reviews throughout the program. System Safety will perform technical audits as necessary to insure that critical items are being properly controlled during manufacturing, assembly, transportation, storage, and use. Assembly and check out of the XYZ system will be monitored by the System Safety Organization to identify and control hazards.

11.0 MISHAP AND HAZARDOUS MALFUNCTION ANALYSIS AND REPORTING:

*The contractor shall describe in the SSPP the mishap/incident alerting/notification, investigation and reporting process including notification **of** the FAA.*

A mishap response plan is a requirement and responsibility of ABC Space Systems for the XYZ Program flight test. All participants in the Program will provide engineering and system safety support as required.

Hazardous malfunctions will be documented on HRs and reviewed during Program Reviews and technical meetings.

12.0 INTEGRATION AND MANAGEMENT OF ASSOCIATE CONTRACTORS AND SUBCONTRACTORS:

The SSPP should identify, in detail:

- a. *The **interface** between system safety and all other applicable safety disciplines such as: nuclear safety, range safety, explosive and ordnance safety, chemical and biological safety, laser safety and any others.*
- b. *The interface between system safety, systems engineering, and all other support disciplines such as: maintainability, quality control, reliability, software development, human factors engineering, medical support (health hazard assessments), and any others.*
- c. *The **interface** between system safety and all system integration and test disciplines.*

Subcontractors and suppliers will perform significant portions of the XYZ Program. They will provide subsystems and components that are critical to the XYZ System. System Safety requirements for subcontractors and suppliers will generally be imposed through statements of work (SOW), equipment specifications, and contractor data

requirements lists (CDRL). Because of the widely varied nature of the products and services provided, the safety requirements will be tailored on a case-by-case basis. Specific equipment safety requirements will be identified and included in equipment specifications. System Safety Program and task requirements will be specified in the SOW to ensure that safety is addressed in the equipment design and that subcontractor efforts are integrated into the system safety program described in this plan. CDRL requirements will specify data required to document compliance with specification requirements, track hazards, and provide inputs to the hazard analysis process.

ANNEX 1

HAZARD REPORT AND ANALYSIS FORMAT

This annex describes the Hazard Report database and Hazard analysis format to be used by all XYZ Team members. It is designed to allow for ease of hazard tracking, flexibility in analysis presentation, and reduction of time and effort in report preparation. The information on the individual HRs can then be selectively extracted and formatted to provide data for the hazard analysis reports.

Hazard Report Data Entry Forms:

Examples of the Hazard Report data entry form follows. The fields are completed in accordance with the fields that would normally be specified for each type (phase) of the analysis. Individual data fields are standardized as to content where necessary so that data searches will come up with consistent and complete results. In these examples, something has been entered in the fields to demonstrate their usage.

Hazard Report

Company: Sample XYZ

Title: Premature shut down of Main Engine	Analysis Phase: PHA
System: Propulsion Subsystem: Main Engine	Report Number: XYZ-001
Function: _____	Risk Level: High
Mission Phase: Ascent Flight Operations, Autosafing/Safe Abort Sequence	Hazard Status: Open

	Severity	Probability	HRI	Open Date:	
Initial:	I	B	2	Close Date:	
Closeout:				Originator:	John Doe

Hazard Description:

Failure/Premature shutdown of the main engine during ascent

Effect:

Inability to achieve orbital velocity.

Failure Mode/Cause:

Hardware Cause:

- 1. Failure of the LH2 Fuel Feed System or the LO2 Lox feed system (Tank, feed lines, valves, pump)
 - 1a. Due to design deficiency.
 - 1 b. Due to environmental stress including drop, shock, thermal, acoustic, and vibration.
 - 1c. Due to workmanship
 - 1d. Clogged LH2 or LO2 tank filter
 - 1e. LH2 or LO2 isolation valve failure

Software Cause:

- 1. Premature main engine shutdown inadvertently initiated by software

Human Error:

- 1. Operator error causes inadvertant commanded shutdown of main engine

Interface Description:

Controls:

Hardware Controls:

- 1a. Design LH2 and LO2 fuel feed system including tanks, plumbing, valves, pumps, etc to worrst case pressures for 50 reuse launch and landing cycles with a factor of safety > 1.5. Design pressure vessels to meet ASME or Mil-Std 1522. Design pressurized lines and fittings with less than 1.5 inch inside diameter to a factor of safety > 4.0. Design those with a 1.5 inch or greater inside diamater to an ultimate factor of safety greater than 1.5.
- 1b. Design LH2 and LO2 fuel feed system including tanks, plumbing, valves, pumps to expected worst case environmental stress including, shock, thermal, acoustic, and vibration.
Defined using methodology described in MIL-STD XXXX, or Industry STD- XXXX.
- 1c. Manufacture and test LH2 and LO2 feed system using ASME standards and ISO 9000 certified processes.
- 1d. Develop preassembly cleaning process and post assembly contamination controls procedures to assure that no FOD or

particulates large enough to clog system filters of valves can be introduced into the system.

le. TBD

Software Controls:

la. Design failsafe software that interrogates main engine performance and automatically initiates Safe Abort sequence in the event of a premature main engine shutdown.

lb. Design and test software to TBD certified process

lc. Perform complete software Independent verification and validation

Safety Device:

la. Design failsafe software that interrogates main engine performance and automatically initiates Safe Abort sequence in the event of a premature main engine shutdown.

lb. Design and test software to TBD certified process

lc. Perform complete software Independent verification and validation

Warning Device:

Design command control system such that each of the three independent commands required to initiate main engine shutdown trips a Warning in Mission Control Center.

Procedures/Training:

Flag this operation as safety critical in the operations training procedures and require simulation training and certification for Mission control center operators.

Verification (Method & Status):

Hardware Design:

la. i. Main Engine LH2 and LO2 fuel feed system tanks, plumbing, valves, pumps designed for worst case pressure and 50+ total mission cycles per PDR action item closure ABC XYZ MAQ344-tyt 11/29/96

1 b.i Worst case Qualification Environments incorporated into ABC XYZ MA-344 TYT Preliminary Qualification Test Requirements. (To be closed upon completion of Qual testing.) OPEN

1c.i. ABC Space Systems ISO Certification process underway. ISO certification of XYZ Team members TBD. OPEN

1d.i XYZ Safety Action Tracking Record (XYZ -ME-2- 001) sent to all XYZ main propulsion system component system suppliers directing preassemble contamination controls and FOD controls. OPEN

1d.ii TBD

le. i. TBD

Software Design:

1a.i & 1c.i XYZ Safety Action Tracking Record (XYZ-ME-SW-002) adding safe abort sequence initiation and IV&V requirement to software design initiated. Design and verification in work. OPEN

1b.i TBD

Safety Device:

XYZ Safety Action Tracking Record (XYZ-ME-MCC-005) Transmits requirement for three independent operator commands to initiate main engine shutdown. MCC design behind schedule. (OPEN)

Warning Device: TBD
Procedure/Training TBD

Remarks:

--

Closure

Signatures:

Originator:

--

System Safety Manager:

--

Program Management:

--

EXAMPLE SYSTEMS AND SUBSYSTEMS

The following table shows the relationship of XYZ systems and subsystems.

System:	Subsystem:
Propulsion	Main Auxiliary Re-entry/de-orbit
Primary Structure	Wings Landing Gear Attachment Thrust System Attachment Aero-shell Control Surfaces Doors Fuel Tank Oxidizer Tank
Propellant Feed/Pressurization	GO2 Pressurization GH2 Pressurization LOX Feed LH2 Feed
Thermal Protection	Carbon Carbon Metallics Composite Aeroshell
Electrical Power	Power Control Power Distribution Power Generation
Landing and Recovery	Nose Landing Gear Main Landing Gear Parachutes Airbags Landing struts Nose Wheel Steering
Flight Control Actuation	Rudder Assemblies Body Flap Assemblies
Environmental Control	Active Thermal Control Leak/Fire Detection Purge and Vent
Reaction Control	Thruster Modules Propellant Supply Electronics & Instrumentation
Telemetry, Tracking, and Command	Avionics Comm. Receivers/Transmitters INS/GPS Radar Altimeter Software Vehicle Computer

Flight Safety System	Vehicle Health Monitoring Flight Termination System Thrust Termination system Safe Abort System
Vehicle Health Monitoring / Management	Avionics Comm. Receivers/Transmitters INS/GPS Radar Altimeter Software Vehicle Computer
Ground Support Equipment	Propulsion Umbilical Mechanical Hold-Down Launch Structure Lifting/Hoist/ Landing Accessories Test Instrumentation
Facilities	Umbilicals Vehicle Erection Vehicle Shelter Utilities Control Center
Payload	
Other	

EXAMPLE STANDARD HR DATA FIELD ENTRIES.

Consistency in selected data fields throughout all analysis phases and techniques is beneficial for performing future data searches.

Analysis:	PHA SRCA SSHA SHA
Risk Level:	Low Medium High
Hazard Status:	Open Closed Transferred
Phase:	Maintenance Launch Processing Launch Countdown Ascent Flight Operations On-Orbit Operations Reentry Countdown Reentry Flight Operations Autosafing Sequence Post Landing Safing All
Severity:	I II III IV
Probability:	A B C D E
HRI:	Numbers from 1 to 20 corresponding to the severity and probability of the hazard as shown in Table 6.2, Hazard Risk Index Matrix, of the SSPP.

Closing a Hazard Report:

The closure of the Hazard Report will require the signature of the System Safety Manager, the Program Manager, and the Hazard Report Originator. When a Hazard Report has been approved for closure, an “XYZ Program Hazard Analysis - Closed Hazard Report” document will be prepared and released. This document and its revisions will identify all the Hazard Reports that have been closed as of that date. Within the database, closed HRs will be identified by the presence of the date in the Date Closed field