Guide to the Identification of Safety-Critical Hardware Items for Reusable Launch Vehicle (RLV) Developers

(1 May 2005)

Prepared by

American Institute of Aeronautics and Astronautics

Abstract

This document provides guidelines for the identification of potentially safety-critical hardware items in RLV designs. Possible risk-mitigating design strategies that may be incorporated into designs are also included. Such risk reduction measures may be necessary if vehicle operation poses risk to the uninvolved public beyond established thresholds of acceptability.

Published by

American Institute of Aeronautics and Astronautics
1801 Alexander Bell Drive, Suite 500, Reston, VA 20191

Printed in the United States of America.

Contents

Figures

Tables

Foreword

Numerous Reusable Launch Vehicle (RLV) systems are currently under development and testing to serve a variety of markets, from sub-orbital personal spaceflight to remote sensing applications. As one part of its mission, the Federal Aviation Administration's Associate Administrator for Commercial Space Transportation (FAA/AST) has been tasked with protecting the uninvolved public from the risk inherent in commercial space launch. The second part of AST's mission involves "encouraging, facilitating, and promoting U.S. commercial space transportation." This project represents an attempt by AST to simultaneously protect public safety and promote the developing RLV industry.

With the support and participation of FAA/AST, the American Institute of Aeronautics and Astronautics (AIAA) formed an industry working group tasked with identifying reusable launch vehicle (RLV) potentially safety-critical systems in August 2003. This Guide is a result of that activity.

Developed through close cooperation between FAA/AST and commercial RLV developers, this document represents a systematic approach to identifying potentially safety-critical items on a vehicle. Possible risk mitigation strategies are currently listed for many of the items identified. It is intended that this list will be expanded in future editions of the document. As more experience is gained in the design and development of reusable launch vehicle systems, this Guide will be updated to reflect increased knowledge and changes in the state of the art.

The following individuals and their organizations were instrumental in the development of this Guide:

Paul Birkeland	Kistler Aerospace
Lyndon Bonaparte	FAA/AST-300 (Systems Engineering and Training)
Randall Clague	XCOR Aerospace
Ralph Ewig	Andrews Space, Inc.
Terry Hardy	FAA/AST-300 (Systems Engineering and Training)
Sri Iyengar	Lockheed Martin Corporation
Derek Lang, Pat Bahn	TGV Rockets
Richard Lee	AIAA Consultant
Dan Murray	FAA/AST-300 (Systems Engineering and Training)
Bob Peercy	The Boeing Company
Lorie Scheufule	Northrop Grumman Corporation
Yvonne Tran	FAA/AST-300 (Systems Engineering and Training)

This document represents a consensus of the RLV community represented above and was developed under the administration of AIAA. While this document is not an AIAA Standard, the process followed in the development of this Guide was in accordance with AIAA's Standards Program Procedures which have been accredited by the American National Standards Institute (ANSI).

Comments on the content of the document and suggested changes may be directed to Craig Day, AIAA Standards Program Manager, at craigd@aiaa.org.

1 Introduction

1.1 Purpose

This document provides guidelines for the identification of potentially safety-critical hardware items in RLV designs. Possible risk-mitigating design strategies that may be incorporated into designs are also included. Such risk reduction measures may be necessary if vehicle operation poses risk to the uninvolved public beyond established thresholds of acceptability.

The sole purposes of this document are to:

- assist developers by illustrating a systematic approach to identifying and mitigating the risk associated with safety-critical items;
- identify relevant and more in-depth documentation; and
- enhance understanding and communication.

It is expected that this document will be used by RLV developers in the design process to initiate the identification of potentially safety-critical items early in the development cycle. With this knowledge in mind, sufficient actions can be taken early in a program to bring the risk to the uninvolved public associated with a safety-critical item to an acceptable level.

1.2 Scope

The first iteration of this guide is limited in scope to cover only on-board RLV safety-critical hardware items. It is intended that future editions be expanded to cover other aspects of RLV design and operations (i.e., ground hardware, software, etc.).

2 Interpretation of Safety-critical

The *Commercial Space Transportation RLV and Reentry Licensing Regulations*, 14 CFR 401.5, provides the following definition of safety-critical.

"Safety-critical means essential to safe performance or operation. A safety-critical system subsystem, condition, event, operation, process or item is one whose proper recognition, control, performance, or tolerance is essential to system operation such that it does not jeopardize public safety."

For the purpose of this document, a definition derived from MIL-STD-882D and 14 CFR 401.5 was utilized to interpret "safety-critical" in the following ways:

A "potentially safety-critical" item is one, the failure of whose proper recognition, control, performance or tolerance could credibly pose a hazard to the uninvolved public.

A "developer's safety-critical" item is one the failure, as shown by analysis, of whose proper recognition, control, performance or tolerance does pose an unacceptable level of risk to the uninvolved public.

The differences in these terms are subtle, yet important. The 14 CFR 401.5 definition is intentionally broad to allow federal regulators necessary leeway in determining what is safety-critical on a given vehicle. For a new developer, it is important to realize that this does not mean that everything in a design is necessarily safety-critical. Rather, it is necessary to work through a systematic process to ensure that all items that could pose a threat to the uninvolved public are addressed in an appropriate manner.

The two interpretations, "potentially safety-critical" and "developer's safety-critical" are terms that are used in the process described in Section 7. "Potentially safety-critical" items are those that a developer has identified through a screening process using the guidelines and criteria outlined in this document. Using this list of potentially safety-critical items as a baseline, the developer applies quantitative and/or qualitative risk assessment techniques to evolve the list of safety-critical items specific to his vehicle.

The use of the process outlined in Section 7 should yield a list of items that meet the definition contained in the regulation.

3 Hazard Contributors

There are seven hazard contributors that add to the overall risk a system can pose to the uninvolved public. These hazard contributors are represented in Figure 1.

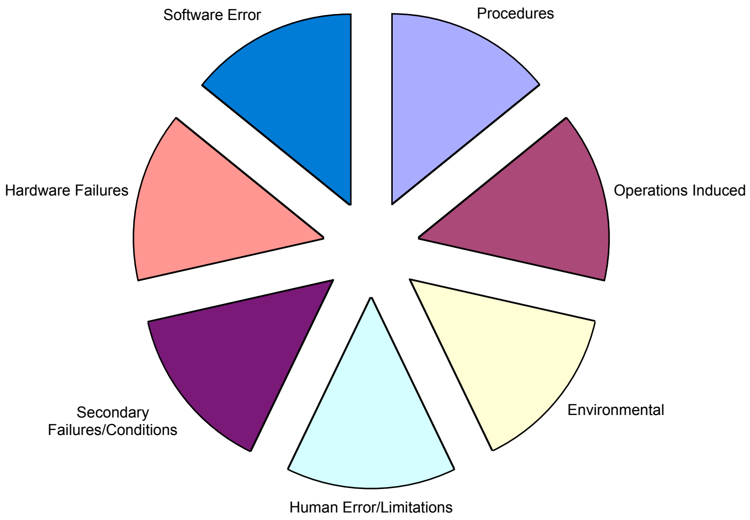

Figure 1 – Hazard Contributors

These seven hazard contributors can be generally categorized into the following higher level cause categories:

- Safety-critical hardware
- Safety-critical software functions
- Safety-critical procedures

Secondary failures/conditions can also occur as a result of problems with primary hardware, software or procedures.

The following table illustrates examples, for each hazard contributor, of a specific hazard, potential risk reduction measures for that hazard, and which higher level cause category that hazard falls into. Every hazard *contributor* can have hazards belonging to any cause category, but each specific *hazard* will belong to only one cause category.

Table 1 — Examples of Hazard Contributors, Potential Countermeasures, and Cause Categories

Contributor	Example(s)	Potential Countermeasures	Cause Category
Human Error/ Limitations	A. Accidental activation of a cockpit switch	1. Hooded switch cover 2. Mount switch recessed within panel 3. Pull circuit breaker (CB) until function is needed	Hardware
Procedural Problem	A. Incompatibilities or errors within Launch Commit Criteria (LCC), Flight Rules, etc.	1. Check hazard controls against procedures 2. Rigorous evaluation of each change to preclude "control erosion"	Procedures
Hardware Failure	A. Tank or fluid line rupture B. Loss of power bus	1. Apply rigorous safety factors 2. Multiple and/or redundant sources of power	Hardware
Secondary Failure/Condition	A. Loss of communication during an emergency	1. Alternate modes for each critical function 2. Ground intervention for emergencies	Hardware
Environmental	A. Crosswinds at landing site B. Lightning near launch site	1. Put constraints on crosswinds in Launch Commit Criteria (LCC) 2. Put constraints on lightning in LCC	Procedures
Software Error(s)	A. Data Corruption in Storage or Transfer B. Algorithmic Error	1. Error Correction Codes in Data Storage Units and Communication Systems 2. Software Development Review / Validation / Test Procedures	Software
Operations Induced	A. "Go Fever" B. Schedule pressure	1. Fully understand and document risk 2. Minimize exposures of this nature	Procedures

An RLV developer should consider all of these hazard areas, to ensure a comprehensive safety assessment of the vehicle and its mission. Each of these cause categories involving the RLV hardware, software and procedures can contribute to hazards that may result in injury to, or loss among, the uninvolved public.

This first iteration of these guidelines is limited in scope to cover only on-board RLV safety-critical hardware systems as hazard contributors. It is intended that future editions of this Guide will be expanded to cover the other hazard contributors.

4 A Three-Pronged Approach to Assessing Public Safety

The following approach to assessing system safety is based on proven aerospace industry practice and has been adapted by the FAA/AST for use in licensing commercially launched RLVs. The methodology has proven effective at assuring system safety and, as a result, the safety of the uninvolved public. It is recommended that vehicle developers utilize this approach in their vehicle development program. Figure 2 provides a graphical overview of the process.

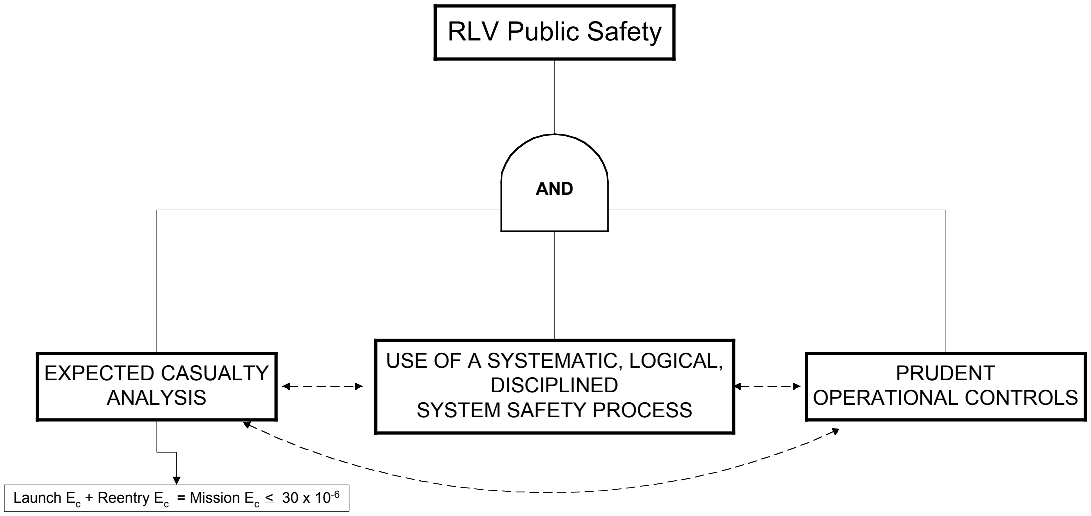
RLV Public Safety
AND
EXPECTED CASUALTY ANALYSIS
USE OF A SYSTEMATIC, LOGICAL, DISCIPLINED SYSTEM SAFETY PROCESS
PRUDENT OPERATIONAL CONTROLS
Launch E_c + Reentry E_c = Mission $E_c \leq 30 \times 10^{-6}$

Figure 2 — Three Pronged Approach to System Safety

The three prongs are inter-related throughout the system's development and operation. In particular, a preliminary Expected Casualty analysis will provide an idea of the depth of safety analysis required as part of the System Safety Process, as well as the extent of the Prudent Operational Controls. Section 5.3 presents three examples of different levels of risk and, consequently, levels of analysis for the identification of safety-critical items.

A systematic, logical, disciplined System Safety Process generally consists of analyses and procedures undertaken as part of the design and development effort to ensure system safety. This document is intended to support this aspect of a developer's effort. Such effort may include:

- Failure Modes and Effects Analysis (FMEA)
- Failure Modes, Effects and Criticality Analysis (FMECA)
- Fault Tree Analysis (FTA)
- Sneak Circuit Analysis
- Event Tree Analysis
- Failure Reporting, And Corrective Action System (FRACAS)
- Reliability testing
- Verification and Validation (V&V) testing

Prudent Operational Controls may consist of:

- Allowable weather conditions for operations
- Launch area security requirements
- Launch crew training and certification requirements
- Clearly articulated lines of communications and responsibilities
- Launch commit criteria
- “No Fly” zones
- Abort lines

5 Depth of Analysis Necessary to Identify Safety-Critical Items

The process and procedure for identifying safety-critical items outlined in Sections 6 and 7 below are intended to assist new developers throughout their vehicle design and development. This section represents a preliminary characterization of the level of effort that a developer may need to expend in order to identify their safety-critical systems by outlining three real-world vehicle examples of the process. The first two examples outline systems that lent themselves to a simplified analysis for identification of safety-critical items. The third example is one of a vehicle that requires extensive analysis to identify the safety-critical items.

Many factors such as the size of the vehicle, the history and heritage of vehicle systems, the flight profile, the launch site location, and the developer’s business plan’s risk tolerance must be considered. Industry experience demonstrates that early assessment of required safety analyses is greatly beneficial to a vehicle developers’ long-term design strategy. Should a developer wish to consult a regulatory body for approval to fly a commercial spacecraft in, or around, the vicinity of the uninvolved public, early identification of safety analyses, and the depth of those analyses, necessary to gain approval will allow for sound financial and resource planning.

The depth of analysis that a developer should undertake for safety purposes requires some amount of subjective judgment. Unlike regulations governing other aerospace-related endeavors, the current regulatory regime governing commercial space launch and reentry vehicles is intentionally broad and flexible. While this fact affords new vehicle developers the ability to work together with regulators, traditional aerospace organizations may find the lack of prescriptive regulatory requirements confusing. This section is an attempt to indicate by illustrative example how the developer might determine a sufficient depth of safety analysis early in his design process.

Many factors affect the degree of risk that a flight operation poses to the uninvolved public. However, the choice of launch site, the system’s operational scenario and vehicle configurations are fundamental drivers in all flight operations. The launch site is critical because the site’s proximity to populated areas strongly affects the level of risk posed. The operational scenario is critical because it determines how close the vehicle approaches that population and how long the hazard persists and, consequently, the level of risk. While the following examples may not apply to the developer’s specific vehicle configuration, the three separate examples will explore the effect of these risk drivers on the depth of analysis necessary.

5.1 Risk Assessment Definitions

Expected Casualty Analysis

The launch industry's fundamental method for assessing risk is called the Expected Casualty Analysis, or the Ec (E-sub-c) Analysis. This methodology was developed in the early days of launch system design to determine, through a set of conservative probabilistic models, the possibility of a given flight operation causing a casualty among the uninvolved public on the ground. Accepted industry practice allows no greater than 30 x 10^{-6} (30-in-a-million) probability of casualty among the uninvolved public on the ground.

Assumptions made in an Ec analysis could result in an oversimplification of the risk assessment, such oversimplification could make the risk assessment less conservative. To account for this, it is important that any assumptions made and their resultant effects on the overall risk be clearly documented in the analysis.

The reader should refer to FAA Advisory Circular 431.35-1, *Expected Casualty Calculations for Commercial Space Launch and Reentry Missions*, for a complete presentation of the Expected Casualty analysis.

Instantaneous Impact Point (IIP)

While risk assessment discussions often refer to the "overflight of populated areas," the physical location of the vehicle actually has less effect on the risk to the uninvolved public than the Instantaneous Impact Point.

The Instantaneous Impact Point (IIP) is the location on the earth's surface where the vehicle would impact if it were to stop thrusting at any given moment. The IIP is used in recognition of the fact that in the event of catastrophic failure, the vehicle is unlikely to impact at the point directly below where the failure occurred. Its energy will carry it away from that point.

In the case of a sub-orbital flight profile, the IIP will move away from the sub-vehicle point due to nominal thrust vectoring in the mission profile, atmospheric disturbances, and performance variations. The extent to which the IIP moves is dependent upon the vehicle's flight profile. Just before landing, of course, the IIP is once again directly beneath the vehicle.

In the case of an exo-atmospheric sub-orbital vehicle, the IIP will loiter in a Reentry Impact Zone (RIZ) during the ballistic portions of the vehicle flight above the atmosphere. During this period, the IIP will move very slowly or not at all. In the interest of public safety, the vehicle operator should operate the vehicle so as not to place the RIZ in a densely populated area.

In the case of an orbital flight profile, the IIP will move downrange ahead of the vehicle due to the vehicle's pitching over to build up lateral velocity to enter orbit. The IIP, which is a mathematical abstract, accelerates ahead of the vehicle and completes one circumnavigation of the earth before the vehicle becomes orbital. (Once a vehicle is orbital, by definition it has no IIP.)

When an orbital RLV is decelerating to return to the earth, its IIP races back toward the vehicle, gradually slowing and coming to rest at the landing site.

In practice, the IIP must be treated as a point with some degree of dispersions around it. Launch day winds, for example, will cause pieces of debris to move off the computed IIP by an uncertain amount. These dispersions are usually accounted for by extending the boundaries of any populated area outward, or by circumscribing a dispersion ellipse about the IIP itself. This provides margins for the unavoidable uncertainties inherent in this kind of analysis.

In any event, characterization of the IIP is critical to any flight risk assessment, and control of the location of the IIP is critical to operational flight safety.

IIP Trace

A plot of sequential IIPs as they move over time may be superimposed on a map of the launch area. Such a plot is called an IIP Trace.

Dwell Time

It takes a finite amount of time for the IIP trace to cross any given area on the earth's surface. The amount of time it takes to cross a given area of interest is known as the Dwell Time.

Population Density

The population density is the population of a given census block divided by the area of that block. The United States Census Bureau provides data (population, land area, and water area) for calculating population densities for each census block throughout the United States.

NOTE The U.S. Census Bureau does not generally calculate population densities.

Casualty Area

The casualty area of a given piece of debris is generally assumed to be the sum of the maximum possible area presented by the piece of debris and the area presented by the individual at risk. All other conditions being equal, the larger the casualty area, the greater the risk. In the simplest cases, these values may be assumed in some logical fashion. In more complex cases, there are several probabilistic models that will estimate these values. In either case, it is important to document assumptions and/or the models utilized for future reference. Figure 3 below (taken from FAA AC 431.3-1) is a graphical representation of the casualty area calculation for a piece of vertically falling debris.

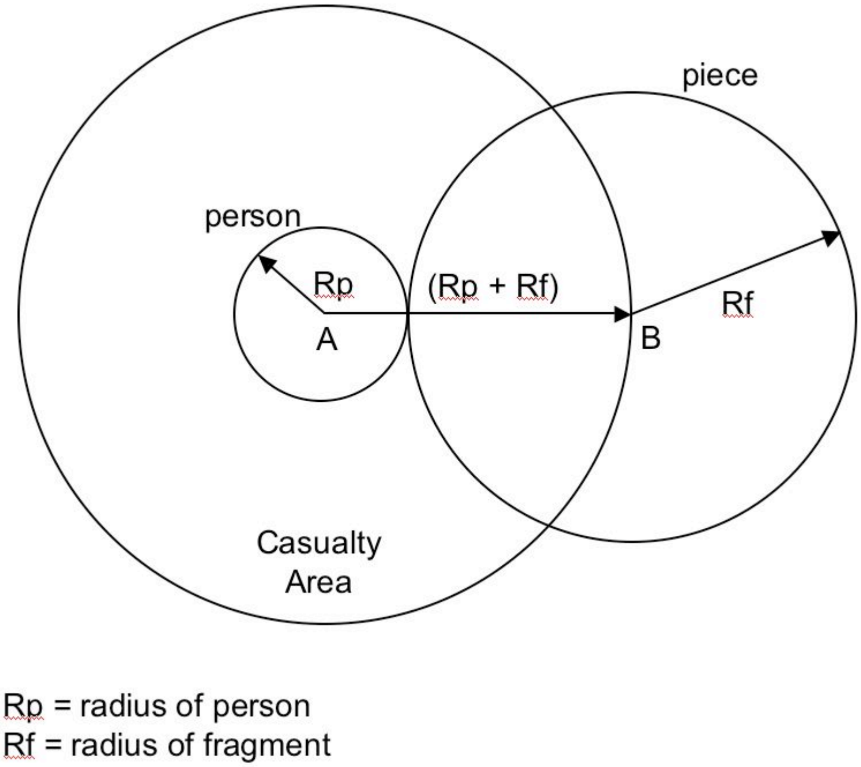

Figure 3 — Casualty area for vertically-falling debris (ref. FAA AC 431.35-1)

5.2 Depth of Analysis Examples

This section presents three flight scenarios that present distinctly different levels of risk to the uninvolved public. As such, one would expect that different depths of analyses would be applied in the design process to identify safety-critical items for different scenarios. The first, and simplest scenario, for example, presents a small, sub-orbital launch. There is no population beneath the dispersed IIP Trace at any time during flight. In this case, some simple system analyses were undertaken and some top-level operational restrictions were applied, the number of safety-critical systems was kept to a minimum.

The second case shows a sub-orbital launch in which its dispersed IIP intersects a small number of populated areas. In this case, one would anticipate that some additional analyses may be required, and, in fact, a simplistic Ec analyses was conducted. It is shown here. Again, however, the identification of safety-critical onboard hardware items as described in Sections 6 and 7 of this document was not required.

The third case presented here is that of NASA's X-33. The vehicle in this example is larger and more energetic, and its flight path more ambitious. As will be shown, the analysis required to identify safety-critical items of this system was quite extensive.

5.2.1 Sub-orbital Launch In Which the Dispersed IIP Does Not Intersect A Populated Area

The first case to be presented here is indicative of a situation where the vehicle size, operational profile, and operation site were such that the simplest analysis was adequate to identify the safety-critical items. The analysis itself does not ensure safety: the safety-critical systems, personnel, and operations do that. This historical example is presented to illustrate the process used by this developer to determine the depth of analysis required to adequately identify his safety-critical items. It involves a small, piloted, winged reusable launch vehicle executing a flight in which its dispersed IIP does not intersect a populated area.

The vehicle is approximately the size of a small airplane with the following characteristics:

- The vehicle is a piloted, winged, horizontally launched and recovered RLV
- Only non-toxic propellants are used in the vehicle
- Engine burns to propellant exhaustion
- Vehicle utilizes mechanical, unassisted flight controls
- The subsonic vehicle experiences moderate acceleration (2-3 g's) throughout the flight regime ensuring that the vehicle can be piloted using visual navigation to a demonstrated level of accuracy

In its operational scenario, it takes off under rocket power, climbs to 10,500 feet MSL (7700 feet AGL) while flying east away from the airport, burns until it has exhausted all of its propellant, spirals down to pattern altitude just east of the airport, enters the pattern, and lands.

In Figure 4, the black, crossed line segments to the left of center are the airport runways. The blue line is the vehicle ground track, climbing off the runway, up to altitude, spiraling back down, and returning to the runway. The red line shadowing the flight path is the vacuum IIP trace. The white irregular shapes west of the airport are populated U.S. Census Bureau census blocks.

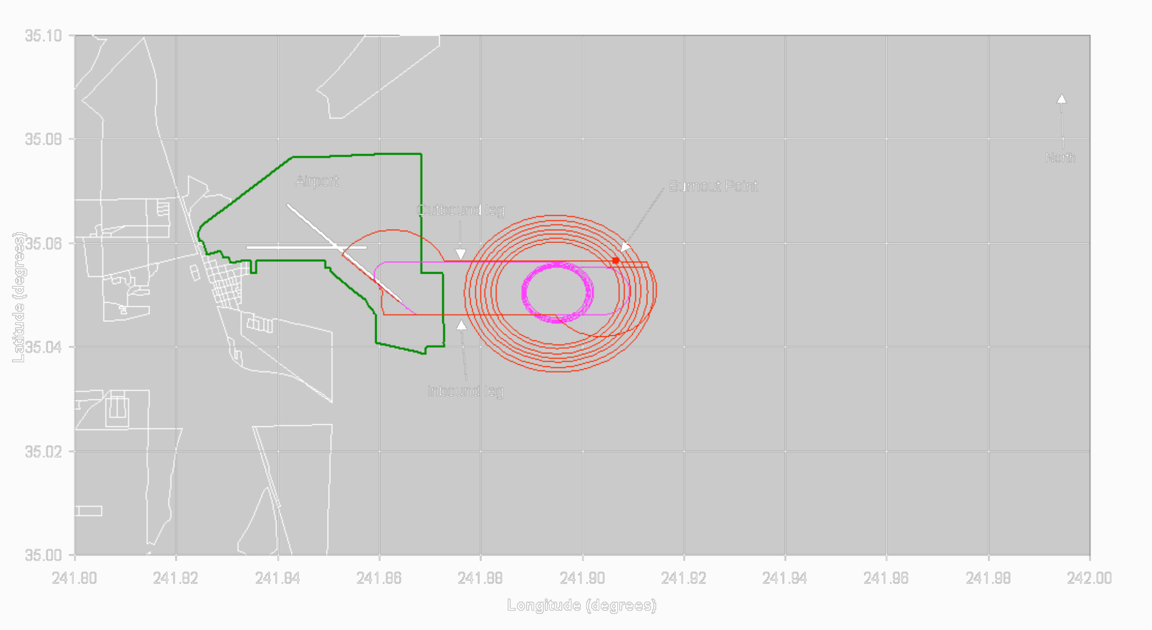

Figure 4 — Nominal Flight Path and IIP Trace Superimposed on a Map of Census Blocks

As the first step in determining the depth of analysis that would be required to identify the safety-critical items, the developer used his extensive knowledge of the vehicle subsystems and components, the vehicle operational concept, and engineering experience to identify any possible failure hazard conditions. The developer concluded in this preliminary assessment that the only components of the vehicle whose failure would result in any of the hazard conditions defined in section 7.2 were the pilot and vehicle flight controls.

The developer then undertook a preliminary risk assessment to determine the extent of the risks posed by the failure of systems other than the pilot or vehicle flight controls. The developer already knew from Figure 4 that the nominal flight profile did not overfly any populated areas. But the question remained as to whether or not another failure could cause sufficient perturbation in the trajectory so as to place populations at risk.

The developer then made the following assumptions:

1. The Probability of system failure (P_f) is 1.

   a. This assumption guarantees the maximum possible conservatism for likelihood of failure and is a good practice for an initial look with this simplified analysis. If the risk posed with this failure probability is unacceptably high, then analysis can be undertaken to more accurately bound the value.

   b. The reader should be aware that regardless of the level of analysis undertaken by the developer, the Federal Aviation Administration will require the assumption of Pf = 1.0 to determine operational restrictions for an unproven RLV at any time the IIP dwells over a populated area for a substantial amount of time. In such cases, the expected average number of casualties to members of the public shall still not exceed 30 x 10-6 (Ec < 30 x 10-6) over that populated area.

2. Worst-case wind conditions exist at the launch location

3. There is no debris detonation upon impact with the ground

4. The pilot will not become incapacitated.

Given the simple, sub-orbital nature of the flight profile and the remoteness of the operational area, the developer realized that the superposition of the vehicle's nominal vacuum IIP trace over the launch area, combined with a worst-case dispersion analysis, could demonstrate that no one on the ground is exposed to the risks associated with these operations, thus demonstrating compliance with the industry practice of a collective risk threshold of 30 x 10^{-6}.

The dispersion of the IIP of this vehicle, flown under visual flight rules, consists of visual navigation error and wind drift of any vehicle debris. The maximum navigation error for this vehicle for this flight path, derived from a visual navigation demonstration flight, is 1,740 feet. The maximum wind drift for this flight path on credible pieces of lethal inert debris, based on winds aloft data collected over a period of time at the launch site, is 1,845 feet. Their sum, the worst-case dispersion, is 3,585 feet.

The burnout point indicated on the figure represents a point where the vehicle becomes inherently safer due to a decreased level of potential energy.

Figure 5 is the dispersed IIP superimposed on the launch area.

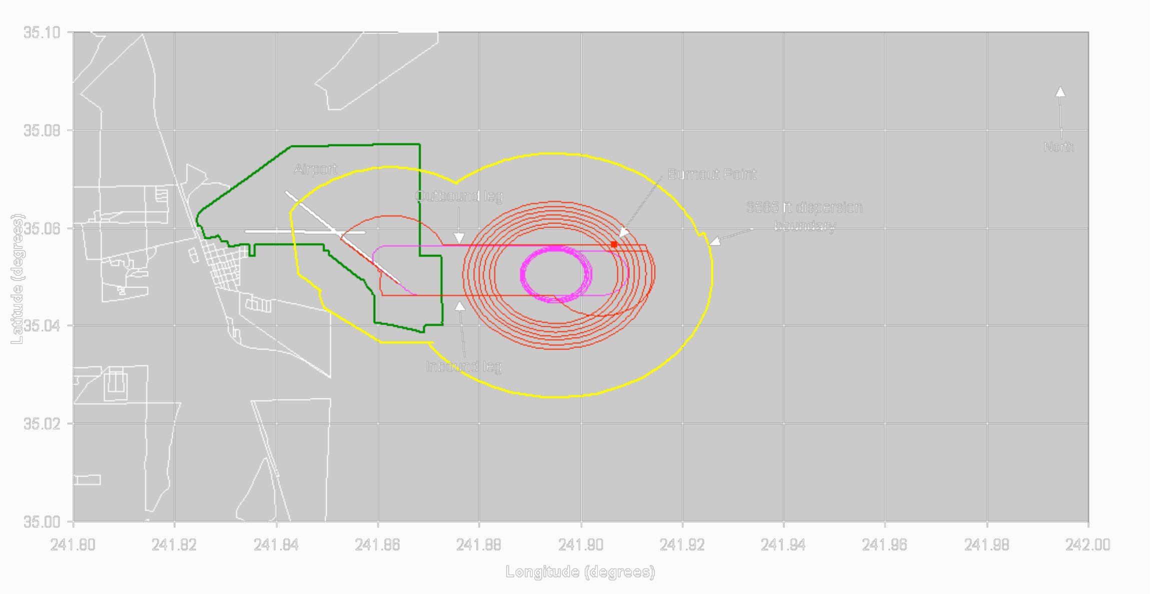

Figure 5 — Flight Path and IIP Trace With Dispersion

A visual inspection of the chart in Figure 5 reveals that the dispersed IIP does not encroach upon a populated census block. The only census block for which visual inspection does not obviously show its distance from the IIP trace to be more than the maximum dispersion is the block to the southwest of the active runway. The vehicle is only on or near the runway during takeoff and landing, during which its altitude, and thus its dispersion, is much lower than the maximum possible. Further, aerial photographs of the area show that the population within this block is clustered in its northeast corner, farthest away from the active runway.

Given the above analysis, the developer confirmed that no further analyses would be necessary to identify safety-critical items. However, it should be noted that any system, the failure of which causes violation of any of the above assumptions or renders the analyses invalid, may be safety-critical and require further analysis as outlined in the rest of the document.

The level of effort necessary to identify safety-critical systems in this example was relatively low since the hazards associated with this vehicle are readily identifiable and its operations can be contained within an area of no population. Given the lack of population overflight, the developer found it unnecessary to perform further analyses to identify safety-critical items. If the population of the area under which the vehicle is flown were greater, the complexity of this analysis would increase.

5.2.2 Sub-orbital Launch in Which the IIP Intersects a Small Number of Populated Areas

The second scenario is for a sub-orbital launch from an inland site in which the vehicle's dispersed IIP intersects a small number of populated areas. The risk posed is low, but obviously greater than the previous example, and one would expect a somewhat more detailed set of risk and safety analyses would be required to identify the vehicle's safety-critical items.

This vehicle was a traditional vertically-launched, fin-stabilized, unguided rocket. Figure 6 shows the computed hazard area (see below) overlying parts of two Census Blocks.

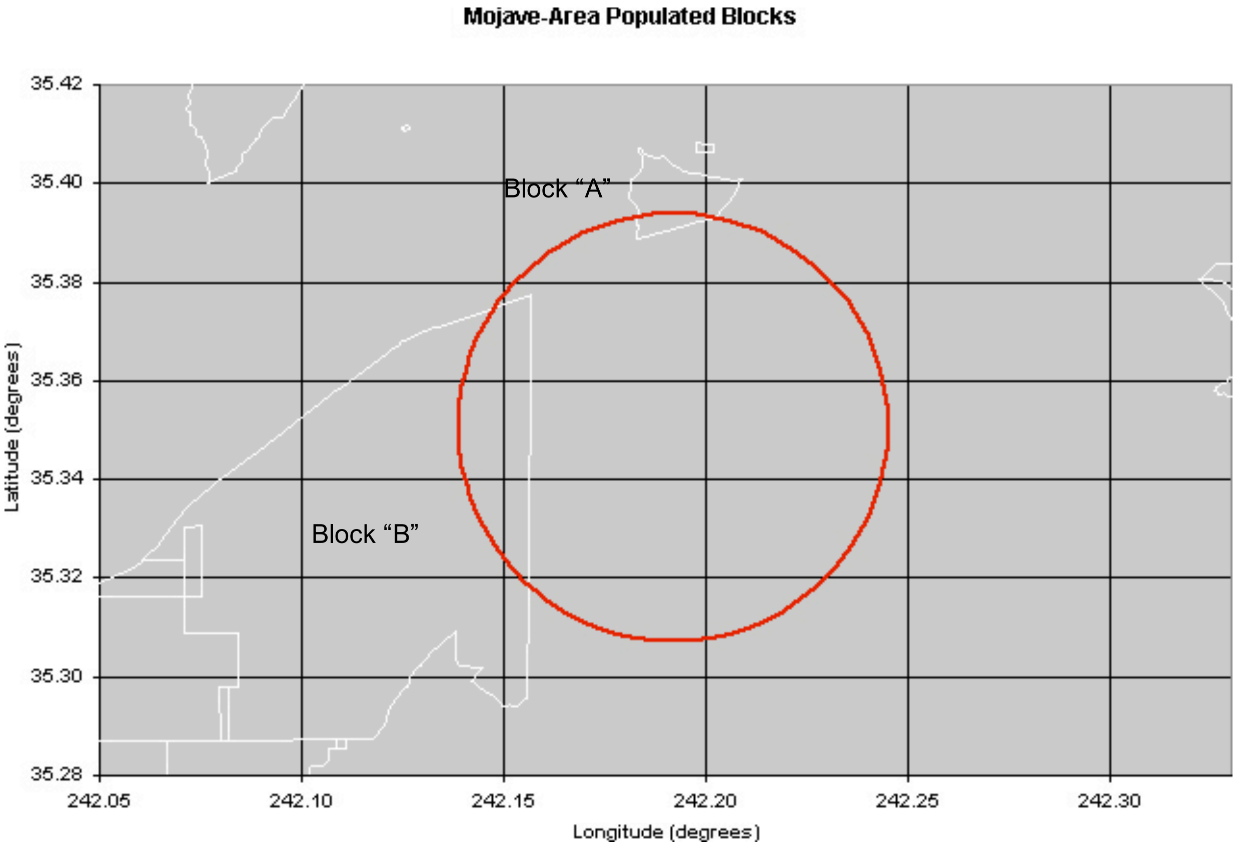

Figure 6 — Hazard Area Superimposed on a Map of Census Blocks

A review of the vehicle operations revealed that in order to contain the dispersed IIP within the identified hazard area, the propellant load on the vehicle at launch could not exceed 4 liters.

In order to approximate the depth of analysis that would be necessary to identify the vehicle's safety-critical items the developer used his knowledge of the vehicle subsystems and components, the vehicle operational concept, and solid engineering experience to identify any possible failure hazard conditions. The developer concluded in this preliminary assessment that the only component of the system whose failure would result in any of the hazard conditions defined in Section 7.2 was the operational control on the fuel load identified above.

The developer then performed a preliminary risk assessment on his vehicle making the assumption that it would fail catastrophically (Pf=1) but that the operational constraint was not violated.

Other assumptions made by the developer in performing the assessment included:

1. worst-case wind conditions (at launch location), and;

2. no debris detonation upon impact with the ground.

The following outline of the preliminary risk assessment is provided for illustrative purposes only.

As a first step, the developer needed to estimate the size of the area put at risk. As shown in column 1 of Table 2, the developer actually made two estimates here. The more conservative estimate is that the vehicle WILL come down inside one of the census blocks. In this case, the at risk area is simply the sum of the areas of each of the census blocks or 125,728,614 square feet.

Alternatively, the developer could make the more realistic assumption that the vehicle could come down anywhere within a hazard circle.

It should be noted here that, so long as the results are acceptable, the more conservative the modeling for the Ec analysis, the less depth of analysis on the system would be necessary. The goal of the Ec analysis is not to accurately predict the risk exposure, but to demonstrate that it is below the various thresholds of acceptability in the face of conservative assumptions and models.

Several probabilistic methodologies are available to determine the size of the hazard circle, but, for the purpose of simplicity, the developer simply calculated the maximum possible ballistic range for the vehicle. This represents a highly conservative estimate for this analysis. This led to an at Risk Area of 788,243,190 square feet as shown in the table.

The developer then overlaid that circle onto a Census map of population to determine the population of Census blocks overlain by the at risk circle.

As shown in Table 2, the developer then proceeded to compute a population density for the relevant Census blocks and At Risk Areas. The population of Block A was 2 persons. The population of Block B was 7 persons. The total population of 9 was divided by the two At Risk Areas to yield a conservative population density of 7.16 x 10^{-8}, and a nominal population density of 1.14 x 10^{-8}.

The developer then assumed, per FAA AC 431.35-1, that the radius of the space covered by a human is 1 foot, and that the radius of the crater is also 1 foot. Again, there are sophisticated probabilistic models to determine these values, and these models become rather more necessary with larger vehicles and more complex flight profiles. But for the case at hand, these simple assumptions were conservative.

The analysis then assumed a Probability of Failure (P_f) of 1.0, i.e. the developer made the assumption that the vehicle WILL fail.

These assumptions led to an estimated Casualty Area (AC) of 12.57 square feet as shown in Table 2.

Finally, multiplying the Population Density by the Casualty Area and by the Probability of Failure, the developer determined that the Expected Casualty probability for the conservative case was 9.00 x 10^{-7}. Likewise, for the nominal case the Expected Casualty probability was 1.43 x 10^{-7}. These values are both well below the industry accepted maximum of 30 x 10^{-6}. With the knowledge that the vehicle could not endanger the uninvolved public, further analyses were not performed.

Table 2 — Simplified Expected Casualty Analysis for Overflight of a Lightly Populated Area

	Risk Area (ft^2)	Fixed Pop. (persons)	Exp. Pop. (persons)	Pop. Density (persons/ft^2)	Human Radius (ft)	Crater Radius (ft)	AC Radius (ft)	AC (ft^2)	P_f	E_c(cas)
Block A	10,596,351	2								
Block B	115,132,283	7								
Total Pop. Area	125,728,614	9	9	7.16E-08	1	1	2	12.57	1	9.00E-07
Total Risk Area	788,243,190	9	9	1.14E-08	1	1	2	12.57	1	1.43E-07

Given the above analysis, the developer concluded that there were no on-board hardware items essential to ensuring that the risk to the uninvolved public remained acceptable. However, while not specifically covered by this guide, the operational control identified above was safety-critical in that its violation could put the uninvolved public at risk.

It is further noted that any system the failure of which causes violation of any of the above assumptions or renders the analyses invalid may be safety-critical and require further analysis as outlined in the rest of the document.

The effort necessary to perform this analysis was more complicated than the first example due to the need to account for the small population in the vicinity of the launch site. As this example illustrates, however, the simplified Ec analysis performed was sufficient to provide the developer with confidence that his system, with certain operational constraints implemented, was sufficiently safe to operate from the chosen launch location.

5.2.3 Sub-Orbital Launch In Which the IIP Intersects a Large Number of Populated Areas

Finally, the third scenario is for NASA's X-33 vehicle, a sub-orbital launch in which the vehicle's dispersed IIP intersects a large number of populated areas. The risk posed is more significant because of the flight path and the size of the vehicle, and one would expect a more comprehensive set of risk and safety analyses would be required to identify safety-critical items.

The X-33 was expected to fly from Southern California to Montana. Its IIP passed over a greater population than either of the above cases, and, consequently, a greater level of analysis would be expected. Lockheed Martin, in fact, undertook the entire regimen of safety and reliability analyses for the X-33 before it was cancelled. The following material was derived from X-33 Advanced Technology Demonstrator Program Final Environmental Impact Statement – Appendix G Flight Safety Analysis (NP-1997-09-02-MSFC)

X-33 documents reveal the extent of analyses required to ensure safe X-33 flights between Edwards AFB and sites in Utah, Montana, and Washington. Appendix G states:

"<Edwards Air Force Base> Range Safety, the organization responsible for flight safety, is chartered to protect life and property during vehicle launch, flight, and landing operations for all flights originating within their controlled airspace. In order to satisfy Range Safety's requirements to launch from Edwards Air Force Base and optimally land at one of three landing sites, the Program must provide:

Planning

- best estimate of trajectory
- establish nominal trajectory
- population density studies
- map generation
- launch and landing hazard analysis
- debris fragmentation patterns
- how to handle flight anomalies (deviations, accidents, etc.)
- establish nominal flight envelope
- determine vehicle discretes required for display
- best data source selection
- Range Safety Office and Range Operations Center (best data source) training

Launch

- activate ground support equipment
  - certify configuration
  - sub-system and end to end test
- weather data input
- launch risk analysis
- acoustic overpressure analysis if necessary

Post-Launch

- vehicle anomaly investigation if necessary
- support system anomaly investigation if necessary
- evaluate performance of:
  - support system anomaly investigation if necessary
  - evaluate performance of
    - instrumentation systems
    - communications systems
    - computer systems"

It is beyond the scope of this document to fully elucidate the X-33 safety analyses. And, in fact, Appendix G itself is only a topmost level perspective of the tasks required to better ensure safe operations. The full extent of required analyses will probably never be known since the program was terminated before many serious analyses were undertaken. The work presented in the referenced Environmental Impact Statement is merely a preliminary analysis. It was more to explore and get approval for modeling methods and identify the challenges that lay ahead.

It could be said that the developers of the vehicles in section 5.2.2 and 5.2.3 undertook the planning steps outlined above. However, the vehicles' concepts of operations and flight envelopes were such that the depth of the analyses that support these steps was substantially lower than for the X-33 flight. The effort necessary to perform these analyses for the X-33 flight would prove to be large due primarily to the population densities under the vehicle flight path. That being said, it is worth garnering an understanding of the preliminary Expected Casualty analysis planned for X-33. This analysis is presented in Annex A for reference.

While the level of effort that would be necessary to utilize the process outlined in sections 6 & 7 of this document for the X-33's given flight path is quite extensive, the methods would be applicable.

5.3 Depth of Analysis Summary

The identification of safety-critical items as outlined in this document may not be necessary for all developers and vehicles. There are many situations where such analyses may be inappropriate.

The developer does, however, need to make a conscious determination of the appropriate depth of analysis for his or her system as early as possible in his or her development program. Such a determination should take into account the developer's own risk tolerance and applicable laws and regulations.

The above three examples are intended to provide illustrations of situations that require:

- little additional analysis beyond a preliminary Casualty Expectation analysis;
- a moderate amount of additional analyses, and;
- and a significant amount of additional analyses.

While there are no firm rules governing the depth of analysis to undertake, the developer should now have some sense of where his or her specific system falls. Regardless of the depth of analysis found for a particular vehicle, the processes outlined below in sections 6 & 7 for identifying safety-critical items may be used.

6 Risk Assessment Methodologies

As has been discussed earlier, RLV developers should identify the safety-critical items aboard their vehicles. Industry in general, and the aerospace industry in particular, have developed various systematic approaches to identifying safety-critical systems.

The methods referenced below represent a portion of methodologies that have been developed. The developer should select the approach most appropriate to their vehicle and its concept of operations.

6.1 Methodologies

FAA Advisory Circular AC 431.35-2 Reusable Launch and Reentry Vehicle System Safety Process (http://ast.faa.gov/files/pdf/Ac4312a5.pdf) outlines various methodologies for assessing systems safety. Some of the more commonly utilized methodologies include Failure Modes and Effects Analyses (FMEA), Failure Modes, Effects and Criticality Analyses (FMECA), and Event/Fault Tree Analyses. A number of other methodologies exist and developers are encouraged to review AC 431.35-2 in its entirety for a greater understanding of the system safety process, especially as it may be phased in during the vehicle development program.

6.2 Appropriateness of Various Methodologies

As stated in AC 431.35-2 Reusable Launch and Reentry Vehicle System Safety Process, a system's life cycle may be divided into six (6) distinct phases.

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

The identification of safety-critical systems should be undertaken as early as practical in the system life cycle. The developer should determine the appropriate methodology to use for each given stage of development. Among the considerations in this determination should be:

1. the appropriateness of the methodology to the depth of technical detail available;
2. the appropriateness of the methodology to the type of system or operation being analyzed;
3. the appropriateness of the level of rigor in relation to the severity of the consequences of failure; and
4. the best use of available resources.

7 Guidelines for Identifying Potentially Safety-Critical RLV Items

7.1 Introduction

This section contains a set of tools that RLV developers may use to screen their vehicles and concept of operations to identify potentially safety-critical items. These tools include:

— a set of guidelines that may be used to evaluate a specific hardware item or system to determine if it may jeopardize the safety of the uninvolved public;

— an assessment process that may be followed to return a list of a developer's safety-critical items; and

— a representative list of potentially safety-critical items.

7.2 Safety-Criticality Guidelines

The following guidelines may be used by developers to perform an initial screening of their vehicle to make a preliminary assessment of safety-criticality. This screening is performed independent of a structured risk assessment.

In general, if BOTH of the following conditions are true for a particular item, the item is potentially safety-critical and may require further analysis.

(1) If the vehicle is over/in a populated area, or may reach a populated area as a result of failure, and

(2) the system could credibly fail, with the failure resulting in one or more of the five described hazard conditions below.

List of Hazard Conditions

- Failure causes vehicle breakup:
  The vehicle is broken into fragments.

- Failure causes vehicle loss of control:
  The vehicle can no longer be controlled by the crew (may be onboard crew or ground crew) or by autonomous means.

- Failure causes uncontrolled debris:
  The failure leaves the vehicle intact and controllable, but debris is ejected, without any means of controlling where the debris will impact. For example, an engine failure leaves the vehicle intact and in control, but may cause a fan blade to be ejected from the vehicle; or a structural failure may lead to the separation of a aerodynamic control surface. The intentional jettison of a component (e.g. drop tank) in a designated area during normal or emergency operations is not considered a failure.

- Failure causes uncontrolled discharge of hazardous material:
  The failure leaves the vehicle intact and controllable, but leads to the discharge of hazardous material (toxic, flammable, cryogenic, etc.)[1]. The controlled dumping of propellants in a designated area during normal or emergency operations is not considered a failure.

- Failure prohibits safe landing:
  The failure leaves the vehicle intact and controllable in flight, but prohibits the vehicle from either reaching a designated landing location where the public is not endangered (e.g. a missile range), or prevents the vehicle from performing a controlled emergency landing without endangering the uninvolved public (e.g. at a public airport).

[1] As defined by Table contained in 49 CFR 172.101

7.3 Safety-criticality Assessment

This section presents a step-by-step process that an RLV developer may use to generate a list of safety-critical items specific to his vehicle configuration. This process utilizes the guidelines presented in section 7.2. There are five steps in this process.

1. List the subsystems and operations of the RLV.

2. List hardware elements of each subsystem.

3. Question each component to determine if its failure presents a hazard to the uninvolved public.

4. If it does, designate it as "potentially safety-critical."

5a. Perform a preliminary risk assessment. If it meets the allowable criteria, no further analysis may be required.

5b. Otherwise, apply risk reduction measures and iterate until risks are within acceptable limits.

6. Using the results of this assessment, determine which items must function correctly in order to ensure an acceptable level of risk to the uninvolved public.

7. Prepare a list of the developer's safety-critical items.

Figure 6 is a graphical representation of this process.

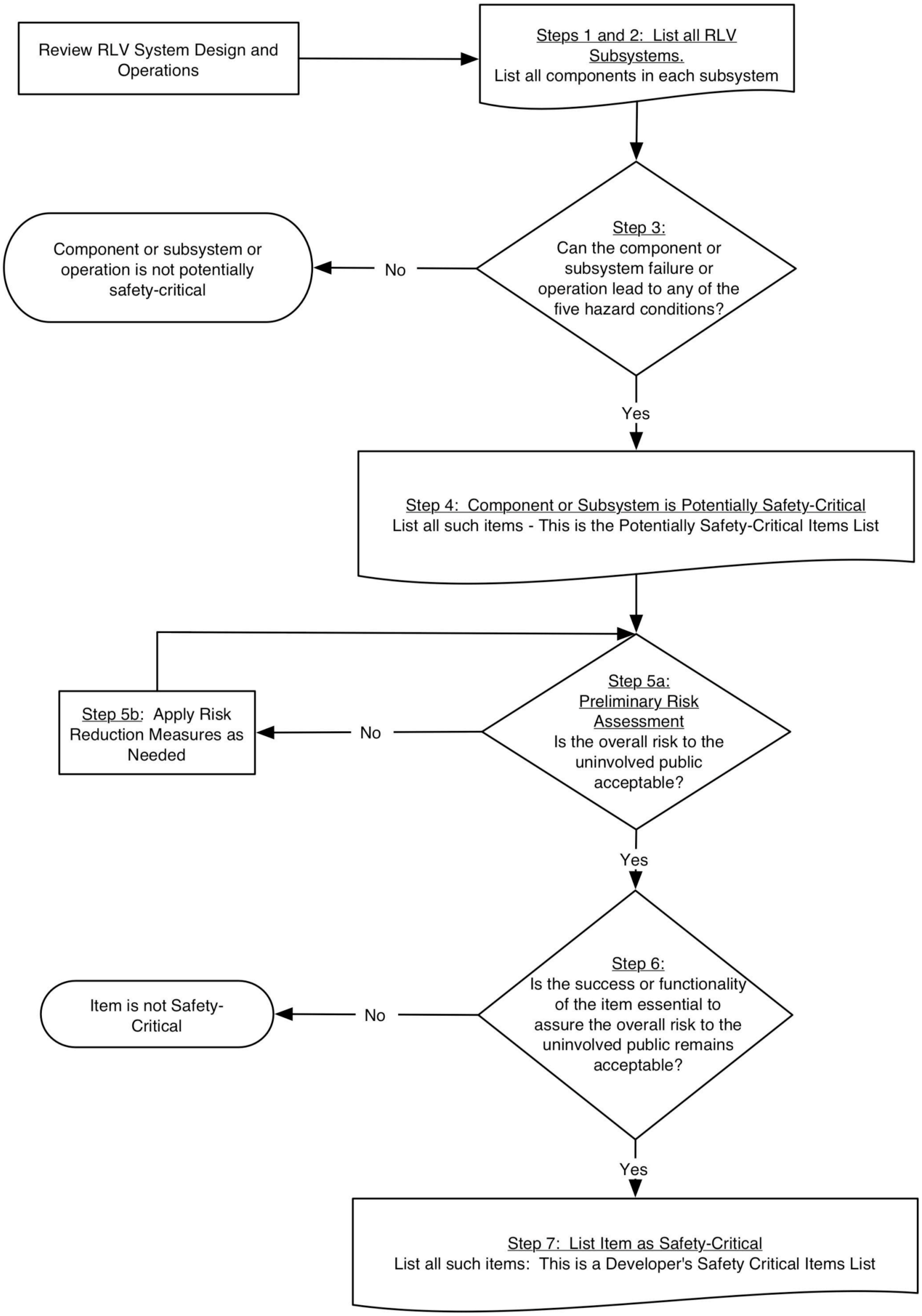
Review RLV System Design and Operations
Steps 1 and 2: List all RLV Subsystems.
List all components in each subsystem
Step 3:
Can the component or subsystem failure or operation lead to any of the five hazard conditions?
No
Component or subsystem or operation is not potentially safety-critical
Yes
Step 4: Component or Subsystem is Potentially Safety-Critical
List all such items - This is the Potentially Safety-Critical Items List
Step 5a:
Preliminary Risk Assessment
Is the overall risk to the uninvolved public acceptable?
No
Step 5b: Apply Risk Reduction Measures as Needed
Yes
Step 6:
Is the success or functionality of the item essential to assure the overall risk to the uninvolved public remains acceptable?
No
Item is not Safety-Critical
Yes
Step 7: List Item as Safety-Critical
List all such items: This is a Developer's Safety Critical Items List

Figure 6 – Flowchart of Safety-Criticality Assessment Methodology

7.3.1 STEP 1: List RLV Subsystems and Operations

A typical RLV may involve some or all of the following systems. This list is included simply as a starting point for developers. Some RLVs may incorporate systems not included in the list below. Therefore, a first step would be the identification of various systems. Add or delete systems as applicable to the systems and operations of the subject RLV.

a. Structures

b. Thermal Protection Systems

c. Propulsion

d. Pneumatics and Hydraulics

e. Operational Ordnance

f. Flight Safety

g. Flight Controls (Mechanical)

h. Flight Controls (Electrical/Electronic)

i. Environmental Control and Life Support Systems (ECLSS)

j. Recovery hardware

7.3.2 STEP 2: List Subsystem Components

The second step in the process involves the identification of key elements in each system. Add or delete components as applicable to the systems and operations of the subject RLV.

a. Structures

    1. Fuselage
    2. Wings
    3. Stabilizers
    4. Doors
    5. Landing Gear
    6. Propellant/Pressurant Tanks (if also used as load bearing structures)

b. Thermal Protection

    1. Ceramic Tiles
    2. Ablative Materials
    3. Composite Panels

c. Propulsion

    1. Engines
    2. Propellant Tanks
    3. Propellant Dumping Systems

d. Pneumatics and Hydraulics

    1. Pressure Vessels
    2. Piping (Rigid and Flexible)
    3. Valves (Flow Control, Directional Control, Check Valves)
    4. Regulators
    5. Relief Devices (Valves and Burst Discs)
    6. Pressure Gauges and Transducers
    7. Temperature Probes
    8. Pumps
    9. Accumulators
    10. Electrical Motors and Solenoids
    11. Interlocks
    12. Logic Devices

e. Operational Ordnance

    1. Parachute Deployment Devices
    2. Parachute Reefing Devices
    3. Drogue Release Devices
    4. Stage Separation Arming Devices
    5. Stage Separation Charges

f. Flight Safety

    1. Propellant Dumping System
    2. Pilot
    3. Flight/Thrust Termination Systems
    4. Ejection Seats

g. Flight Controls (Mechanical)

    1. Elevators
    2. Ailerons
    3. Rudders
    4. Spoilers
    5. Flaps
    6. Brakes
    7. Drag Devices

h. Flight Controls (Electrical/Electronic)

    1. Antenna
    2. Data Receiver/Transmitter
    3. GPS Hardware
    4. Computer
    5. Voice Communications
    6. Active Sensors and Vehicle Position Transducers
    7. Displays
    8. Wiring/Connectors

i. Environmental Control and Life Support Systems (ECLSS)
    1. Cabin Materials
    2. Cabin Atmosphere Regulation Hardware
    3. Pressurized Cabin
    4. Cabin Atmosphere Controls
    5. Cabin Temperature Control System

j. Recovery Hardware
    1. Parachutes
    2. Airbags
    3. Landing Gear

7.3.3 STEP 3: Identify Failure Hazard Conditions

The third step involves assessing each component to determine if its failure can result in any of the hazard conditions defined in section 7.2:

1. Vehicle breakup
2. Loss of vehicle control
3. Uncontrolled debris
4. Uncontrolled release of hazardous materials
5. Prohibits safe landing

7.3.4 STEP 4: Potentially Safety-Critical Items

If the answer is yes to any of the conditions in Step 3, the items are included on the potentially safety-critical items list.

7.3.5 STEP 5(a and b): Preliminary Risk Assessment and Risk Reduction Measures

The fourth step involves performing a Preliminary Risk Assessment assuming failures of the above potential safety-critical items and the consequences and likelihood of failure.

If the Preliminary Risk Assessment shows the risk to be below the acceptable limits, no further analysis may be required. If not, Risk Reduction Measures (RRMs) may be needed

Section 7.4 provides a number of generic risk reduction approaches that may be applied to RLV systems. In addition, the table in Section 7.4 identifies specific RRMs for a number of items. Please note that the implementation of these RRMs is an iterative process. Multiple RRMs may need to be applied repeatedly to reduce the risk to an acceptable level.

7.3.6 STEP 6: Item-Level Risk Analysis

Utilizing the results of this preliminary analysis, the developer identifies those systems on his vehicle which must function correctly to ensure that the level of risk to the uninvolved public remains acceptable. These are the developers' safety-critical items. The items on this list should meet the definition of safety-critical published in 14 CFR 401.5.

Industry practice encourages developers to focus their resources on items that provide the greatest reduction in risk to the uninvolved public. As a general rule, only a small percentage of system failures may contribute to a significant portion of the risk.

7.3.7 STEP 7: List of Developers' Safety-Critical Items

The final step in the process is simply the creation of a list containing the items identified by the developer as safety-critical. In addition to this list, the developer should have a set of documentation that details his process, the analyses performed, the results of those analyses, and any conclusions reached by the developer concerning any item's inclusion on this list. Alteration of a vehicle design and/or operational concept subsequent to the identification of safety-critical items may necessitate subsequent analyses to ensure proper recognition of all safety-critical items.

7.4 Potential Safety-Critical Hardware Items

The following table does not present a list of systems, subsystems, components, equipment or items that will always be safety-critical; it simply provides a point of departure for additional analysis. The safety-criticality of each item on the list is highly dependent on the vehicle design and concept of operations. It is impossible to conceive of all possible RLV configurations; therefore, the following table should not be considered an all-inclusive list. However, the guidelines and process outlined above are also applicable to any RLV system or hardware item that may not be included in the table.

As mentioned above, risk reduction measures are often applied to vehicle systems and hardware components to reduce the risk to the uninvolved public to an acceptable level. The table below identifies specific risk reduction measures for some of the components; however there are a number of general risk reduction measures that are applicable to most space transportation systems. These include, but are not limited to:

- increasing safety factors to provide adequate design margins;
- incorporating flight proven design concepts and materials;
- incorporating special design features;
- incorporating manufacturing and processing improvements;
- testing components to maximum limit loads and environments (for nominal and off-nominal conditions);
- isolating critical components from each other and other critical parts;
- conducting subsystem development and qualification tests to demonstrate system performance and verify design analyses; and
- modifying vehicle flight parameters (trajectory, velocity, etc.) to reduce operating loads, avoid populated areas, etc.

For each item indicated in Table 3, the primary hazard condition that could result from a failure of the item is indicated by an “X”. In some cases there are secondary hazard conditions that occur as a direct result of the initial hazard; these are noted as well. The majority of the hazard conditions identified are followed by explanations as to why they were included. Some of these explanations utilize examples of real-world vehicles, most notably the X-15, the Space Shuttle, Soyuz, and the Armadillo Aerospace project. The information contained in these examples was taken from the open, publicly available sources identified below.

Space Shuttle *Columbia: The Columbia Accident Investigation Board (CAIB) Report*, Volume I-VI, August – October 2003 (http://www.caib.us/news/report/default.html)

X-15: Jenkins, Dennis R. and Landis, Tony R., *Hypersonic: The Story of the North American X-15,* Specialty Press, North Branch, MN, 2003.

Soyuz, X-15: http://www.astronautix.com/

Armadillo Aerospace: http://www.armadilloaerospace.com/n.x/Armadillo/Home/News

Table 3 — Potential Safety-Critical Hardware Items

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	**Vehicle Loss of Control**	**Uncontrolled Release of Debris**	**Uncontrolled Release of Hazardous Material[2]**	**Prohibits Safe Landing**
Structures						
Fuselage	Loss of structural integrity	X[a]	X (secondary condition)	X (secondary condition)	X (secondary condition)	X (secondary condition)
	Loss of control surface	X (secondary condition)	X[b]	X[c]	X (secondary condition)	X (secondary condition)

Specific RRMs:

- Incorporate redundant flight control system to allow a level of control following loss of a control surface
- Use of adequate design margin for control surface strength and attachment

Hazard Condition Explanation:

[a]Design flaw in deHavilland Comet I (square windows) airliner led to metal fatigue and caused structure to fail in flight.
[b]Obvious to most casual of observers (OMCO)
[c]A detached control surface can become uncontrolled debris.

Item	Failure Mode	Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[2]	Prohibits Safe Landing
Wings	Loss of structural integrity	X[a]	X (secondary condition)	X (secondary condition)	X (secondary condition)	X (secondary condition)
	Loss of control surface	X (secondary condition)	X[b]	X[c]		X (secondary condition)

Specific RRMs:

- Incorporate redundant flight control system to allow a level of control following loss of a control surface
- Use of adequate design margin for control surface strength and attachment

Hazard Condition Explanation:

[a]During the final reentry of Space Shuttle *Columbia*, a puncture in the left wing allowed superheated gas into the wing cavity causing a loss of structural integrity of the wing. As a result, the vehicle yawed left and subsequent aerodynamic loads led to vehicle breakup.
[b]OMCO
[c]A detached control surface can become uncontrolled debris.

[2] See Hazardous Materials Table, 49 CFR 172.101

<table>
<tr><th>Item</th><th>Failure Mode</th><th colspan="5">Hazard Condition/Suggested Risk Reduction Measures (RRMs)</th></tr>
<tr><th></th><th></th><th>Vehicle Breakup</th><th>Vehicle Loss of Control</th><th>Uncontrolled Release of Debris</th><th>Uncontrolled Release of Hazardous Material[3]</th><th>Prohibits Safe Landing</th></tr>
<tr><td colspan="7"><b>Structures</b></td></tr>
<tr><td rowspan="2">Stabilizers</td><td>Loss of structural integrity</td><td>X[a]</td><td>X
(secondary condition)</td><td>X
(secondary condition)</td><td>X
(secondary condition)</td><td>X
(secondary condition)</td></tr>
<tr><td>Loss of control surface</td><td>X[a]</td><td>X[b]</td><td>X[c]</td><td></td><td>X
(secondary condition)</td></tr>
<tr><td colspan="7"><u>Specific RRMs:</u>
• Incorporate redundant flight control system to allow a level of control following loss of a control surface
• Use of adequate design margin for control surface strength and attachment

<u>Hazard Condition Explanation:</u>
[a]If stabilizers are necessary for stable flight, loss of a stabilizer could lead to vehicle tumbling and subsequent break-up.
[b]OMCO
[c]On X-15 flight 2-53-97, a shock impingement from the scramjet motor melted part of the ventral stabilizer, sending debris from the aircraft.</td></tr>
<tr><td rowspan="3">Doors (landing gear, drag chute, etc. doors)</td><td>Premature/Unintended deployment</td><td></td><td>X[a]</td><td></td><td></td><td>X
(secondary condition)</td></tr>
<tr><td>Detachment from vehicle</td><td></td><td></td><td>X[b]</td><td></td><td></td></tr>
<tr><td>Failure to function</td><td></td><td></td><td></td><td></td><td>X[c]</td></tr>
<tr><td colspan="7"><u>Specific RRMs:</u>
• Add safety latches requiring two independent commands (or mechanisms) to “full open”
NOTE: Adding redundancy may add risk to the vehicle in order to reduce risk to the uninvolved public.
• Design two doors, inner & outer, with the inner door taking structural loads and the outer door taking aero loads
• Design control system to handle off-nominal loads from door failure

<u>Hazard Condition Explanation:</u>
[a]On X-15 flights 3-15-25, 1-35-56, 2-33-56, and 2-36-63, landing gear doors opened in supersonic or hypersonic flight. Resultant asymmetric drag made control difficult.
[b]OMCO
[c]The failure of a drag chute door to function could prohibit a safe landing.</td></tr>
</table>

[3] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	**Vehicle Loss of Control**	**Uncontrolled Release of Debris**	**Uncontrolled Release of Hazardous Material[4]**	**Prohibits Safe Landing**
Structures						
Propellant/Pressurant Tanks (if used as a load bearing structure)	Tank burst	X[a]	X[b]	X[c]	X[d]	X (secondary condition)

Specific RRMs:

- Add redundant relief mechanisms (i.e., burst discs in parallel with a relief valve, typically with a lower setting); consider use of non-propulsive venting (i.e., a “T” orifice that provides a neutral thrust)
- Avoid the use of a hazardous media as a pressurant.

Hazard Condition Explanation:

[a]Historic launch vehicles have utilized a design in which the vehicle structural rigidity is attained largely from its pressurized tanks. Loss of pressure in the structure causes the vehicle to crumple, rather than breakup. This loss of structural integrity could lead to a decreased ability to sustain aerodynamic loads which could cause the vehicle to breakup.

[b]In the above configuration, a loss of pressure alone would cause the vehicle to crumple rather than breakup. Such crumpling could lead to a loss of the propulsion, guidance, or other control systems.

[c]In the event of a tank burst with sufficient energy to rupture the vehicle skin, tank and/or other structural debris could be shed.

[d]In the above configuration, a tank containing a hazardous media (e.g., MMH, N2O4) could be damaged as the vehicle crumples.

[4] See Hazardous Materials Table, 49 CFR 172.101

<table>
<tr><th>Item</th><th>Failure Mode</th><th colspan="5">Hazard Condition/Suggested Risk Reduction Measures (RRMs)</th></tr>
<tr><th></th><th></th><th>Vehicle Breakup</th><th>Vehicle Loss of Control</th><th>Uncontrolled Release of Debris</th><th>Uncontrolled Release of Hazardous Material[5]</th><th>Prohibits Safe Landing</th></tr>
<tr><td colspan="7"><b>Thermal Protection System (TPS)</b></td></tr>
<tr><td>Ceramic Tiles</td><td>Detachment from vehicle</td><td>X[a]</td><td>X
(secondary condition)</td><td>X[b]</td><td>X
(secondary condition)</td><td>X
(secondary condition)</td></tr>
<tr><td colspan="7"><u>Specific RRMs:</u>
• Incorporate standard inspection process before and after each flight

<u>Hazard Condition Explanation:</u>
[a]Loss of TPS tiles could allow superheated reentry gases to enter the vehicle and melt the structural elements.
[b]Current operational ceramic TPS tiles are so small as to not pose a serious debris threat, however future technology may make this condition a concern.</td></tr>
<tr><td>Ablative Materials</td><td>Premature degradation of material</td><td>X[a]</td><td>X
(secondary condition)</td><td>X
(secondary condition)</td><td>X
(secondary condition)</td><td>X
(secondary condition)</td></tr>
<tr><td colspan="7"><u>Specific RRMs:</u>
• Conduct degradation test program to determine heat flux vs. ablation loss data
• Incorporate sufficient design margin in material thickness
• Incorporate standard inspection process before and after each flight

<u>Hazard Condition Explanation:</u>
[a]If ablative TPS material erodes completely prior to completion of high-temperature reentry phase, superheated gases could melt vehicle structural elements.</td></tr>
</table>

[5] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[6]	Prohibits Safe Landing
Thermal Protection System (TPS)						
Composite Panels	Detachment from vehicle	X[a]	X (secondary condition)	X[b]	X (secondary condition)	X (secondary condition)
	Puncture in panel	X[c]	X[c]	X (secondary condition)	X (secondary condition)	X[d]
	Multi-panel seam degradation	X[e]		X (secondary condition)		

Specific RRMs:

- Incorporate standard inspection process before and after each flight

Hazard Condition Explanation:

[a] Detachment of a composite panel at a critical location could allow reentry plasma to enter vehicle and melt structural elements, leading to vehicle breakup.

[b] If composite panels are of sufficient size to cause concern for the uninvolved public on the ground, this becomes a concern. Note that this hazard is also a secondary condition resulting from vehicle breakup.

[c] During the final reentry of Space Shuttle *Columbia*, a puncture in the left wing allowed superheated gas into the wing cavity causing a loss of structural integrity of the wing. As a result, the vehicle yawed left and subsequent aerodynamic loads led to vehicle breakup.

[d] During the final Space Shuttle *Columbia* reentry, had the vehicle not been destroyed, unanticipated drag could have been sufficient to prohibit a safe landing.

[e] Degradation of a seam between panels could allow reentry plasma to enter the vehicle and melt structural elements, leading to vehicle breakup.

[6] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	**Vehicle Loss of Control**	**Uncontrolled Release of Debris**	**Uncontrolled Release of Hazardous Material[7]**	**Prohibits Safe Landing**
Propulsion System						
Engine (Rocket & Air Breathing)	Engine explosion	X[a]	X[b]	X[c]	X[d]	X[e]
	Loss of propulsive capability		X[f]			X[g]
	Combustion instability		X[h]	X[i]	X[j]	X[k]

Specific RRMs:

- Isolate engines from other vehicle critical systems
- Isolate engines from each other, and design for engine-out capability (nominal throttle < 100%, multiple smaller engines, etc.)
- Incorporate a parachute system to minimize impact energy
- Incorporate a steerable parachute system to avoid densely populated areas
- Incorporate debris containment into engine / airframe design
- Incorporate risk reduction design features to minimize impact (automatic cut-off valves, etc.)

Hazard Condition Explanation:

[a]OMCO

[b]In the case of a Vertical Take-off, Vertical Landing (VTVL) vehicle configuration, a loss of propulsion could result in the inability to control the vehicle's IIP.

[c]In the absence of debris containment, an explosion could result in engine fragments being shed from the vehicle.

[d]If the vehicle utilizes hazardous materials as propellants, an engine explosion could destroy the shutoff valves and allow release of the HAZMAT.

[e]Engine explosion could prevent the vehicle from reaching its destination and/or an abort site.

[f] Loss of propulsion could cause the vehicle to lose control

[g]Loss of propulsion could prevent the vehicle from reaching its destination and/or an abort site

[h]A combustion instability can impose side loads and torques greater than the vehicle was designed to tolerate. This can lead to vehicle loss of control if the loads are high enough.

[i]Combustion instabilities can cause structural failure of a rocket nozzle extension which could become debris.

[j]Combustion instabilities can lead to a catastrophic engine failure, which could destroy shutoff valves and allow release of a hazardous material (if used as a propellant).

[k]Combustion instabilities can destroy a propulsion system which could prevent the vehicle from reaching its destination and/or an abort site.

[7] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[8]	Prohibits Safe Landing
Propulsion System						
Propellant Tanks	Tank burst	X[a]	X[b]	X[c]	X[d]	X[e]

Specific RRMs:

- Incorporate heritage data into tank design
- Design tank to accepted industry standards
- Ensure that tank mount is sufficient for expected operating loads
- Qualify tank to loads expected in non-nominal operation
- Incorporate adequate design safety factors
- Perform structural (qualification) testing to verify design margins
- Perform proof testing at adequate factors
- Incorporate a parachute system to minimize impact energy
- Incorporate a steerable parachute system to avoid densely populated areas

Hazard Condition Explanation:

[a] Pressure-fed rocket propellant tanks typically operate at full system pressure. In this scenario, a tank burst could easily release sufficient energy to destroy the vehicle.

[b] If the tank burst does not destroy the vehicle, the loss of propellant in a VTVL vehicle would lead to loss of vehicle control, as in the 8 August 2004 Armadillo Aerospace test flight.

[c] In the absence of debris containment, a tank burst could lead to the release of debris.

[d] If the vehicle utilizes hazardous materials as propellants, a tank burst will lead to the release of a HAZMAT.

[e] A burst propellant tank will quickly lead to a loss of propellant, leading to the possibility of the vehicle not being able to make it back to its landing and/or abort site.

Propellant Dumping Systems	Premature/unintentional activation		X[a]		X[b]	X[c]

Hazard Condition Explanation:

[a] During the 8 August 2004 Armadillo Aerospace test flight, control of the VTVL vehicle was lost when propellant was exhausted.

[b] If the vehicle uses hazardous materials as propellant, a premature or unintentional activation would be an uncontrolled release of the HAZMAT.

[c] A loss of propulsive capability due to lack of propellant could prevent the vehicle from reaching its landing and/or abort site.

[8] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[9]	Prohibits Safe Landing
		Pneumatics and Hydraulics				
Pressure Vessels	Tank burst	X[a]	X[b]	X (secondary condition)		X[c]
	Pressurant leakage		X[b]			X[c]

Specific RRMs:

- Adequate design safety factors for strength, leak before burst design, testing, pressure reduction in an emergency

Hazard Condition Explanation:

[a]During an X-15 ground test on 8 June 1960, an overpressurization of an ammonia tank caused the tank to rupture. The tank shot backward and damaged the hydrogen peroxide tank; the mixing of ammonia and hydrogen peroxide caused an explosion and the vehicle was essentially blown in half.

[b]A pressure-fed VTVL vehicle would lose propulsive capability in the event of a pressure loss. As mentioned above, loss of propulsion in a VTVL translates to loss of control.

[c]In a pressure-fed propulsion system vehicle configuration, a loss of pressure would lead to a loss of propulsive capability. This could lead to an inability to reach a landing and/or abort site.

Item	Failure Mode	Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[9]	Prohibits Safe Landing
Piping (Rigid and Flexible)	Rupture/Leakage		X[a]		X[b]	X[c]

Hazard Condition Explanation:

[a]Loss of hydraulic pressure or pneumatic pressure for control surface actuators could lead to a vehicle loss of control.

[b]A ruptured or leaking pipe could allow a hazardous hydraulic fluid to be released. The leak would have to be large to affect the uninvolved public.

[c]A loss of hydraulic and/or pneumatic pressure for control surface actuators could impair performance enough to prevent the vehicle from reaching its destination and/or an abort site.

[9] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[10]	Prohibits Safe Landing
Pneumatics and Hydraulics						
Valves (Flow Control, Directional Control, Check Valves)	Rupture/Leakage		X[a]		X[b]	X[c]
<u>Hazard Condition Explanation:</u> [a]Loss of hydraulic pressure or pneumatic pressure for control surface actuators could lead to a vehicle loss of control. [b]A ruptured or leaking valve could allow a hazardous hydraulic fluid to be released. The leak would have to be large to affect the uninvolved public. [c]A loss of hydraulic and/or pneumatic pressure for control surface actuators could impair performance enough to prevent the vehicle from reaching its destination and/or an abort site.						
Regulators	Rupture/Leakage	X (secondary condition)	X[a]	X[b]	X[c]	X[d]
	Improper pressure regulation (failure to provide correct pressure; either over or under design value)	X[e]	X[a]	X (secondary condition)	X	X[d]
<u>Hazard Condition Explanation:</u> [a]Loss of hydraulic pressure or pneumatic pressure for control surface actuators could lead to a vehicle loss of control. [b]A ruptured or leaking regulator could allow the release of debris [c]A ruptured or leaking regulator could allow a hazardous hydraulic fluid to be released. The leak would have to be large to affect the uninvolved public. [d]A loss of hydraulic and/or pneumatic pressure for control surface actuators could impair performance enough to prevent the vehicle from reaching its destination and/or an abort site. [e]Historic launch vehicles have utilized a design in which the vehicle structural rigidity is attained largely from its pressurized tanks. Loss of pressure due to a regulator malfunction in the structure causes the vehicle to crumple, rather than breakup. This loss of structural integrity could lead to a decreased ability to sustain aerodynamic loads which could cause the vehicle to breakup.						

[10] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[11]	Prohibits Safe Landing
Pneumatics and Hydraulics						
Pressure Gauges and Transducers	Rupture/Leakage	X	X	X	X	X
	No or faulty data return	X	X[a]	X	X	X
Hazard Condition Explanation: [a]Loss of or faulty data could lead to erroneous guidance data that may affect vehicle control. (See Flight Control/Electrical Category)						
Temperature Probes	No or faulty data return	X[a]	X[a]		X[a]	X (secondary condition)
Hazard Condition Explanation: [a]Loss of/faulty data could cause a component to thermally fail						
Pumps	Rupture	X (secondary condition)	X[a]	X	X	X[b]
	Freeze-up or Oscillation (Pogo Effect)		X	X (secondary condition)	X (secondary condition)	X (secondary condition)
Hazard Condition Explanation: [a]A loss of hydraulic and/or pneumatic pressure for control surface actuators due to a pump malfunction could lead to a vehicle loss of control. [b]A loss of hydraulic and/or pneumatic pressure for control surface actuators due to a pump malfunction could impair performance enough to prevent the vehicle from reaching its destination and/or an abort site.						
Accumulators	Rupture/Leakage	X (secondary condition)	X	X	X	X

[11] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[12]	Prohibits Safe Landing
Pneumatics and Hydraulics						
Electrical Motors and Solenoids	Mechanical/Electrical Malfunction (loss of control)	X (secondary condition)	X	X	X	X
Interlocks	Unplanned change of state	X (secondary condition)	X	X	X	X
Logic Devices	Improper command, corrupt signal, etc.	X (secondary condition)	X	X	X	X
Operational Ordnance						
Parachute Deployment Devices	Failure to deploy			X	X	X[a]

Notes:

- Failure of deployment mortars to fire could lead to impact outside the intended landing zone
- Premature or unintended parachute deployment could damage parachute and/or damage vehicle near parachute attach points

Specific RRMs:

- Designate and control a safety zone outside the intended landing zone.
- Redundant mortar firing mechanism
- Separate controls for arming mortar and firing mortar

Hazard Condition Explanation:

[a]During the Soyuz 1 reentry, the main parachute failed to deploy. The reserve parachute tangled with the drogue chute and the capsule crashed. A similar failure of a parawing could lead to an impact outside the landing zone.

[12] See Hazardous Materials Table, 49 CFR 172.101

<table>
<tr><th>Item</th><th>Failure Mode</th><th colspan="5">Hazard Condition/Suggested Risk Reduction Measures (RRMs)</th></tr>
<tr><th></th><th></th><th>Vehicle Breakup</th><th>Vehicle Loss of Control</th><th>Uncontrolled Release of Debris</th><th>Uncontrolled Release of Hazardous Material[13]</th><th>Prohibits Safe Landing</th></tr>
<tr><td colspan="7"><b>Operational Ordnance</b></td></tr>
<tr><td>Parachute Reefing Devices</td><td>Failure to deploy</td><td></td><td></td><td></td><td></td><td>X[a]</td></tr>
<tr><td></td><td>Premature activation</td><td></td><td></td><td></td><td></td><td>X[b]</td></tr>
<tr><td colspan="7">Specific RRMs:
• Designate and control a safety zone outside the intended landing zone.
• Redundant disreefing mechanism.

Hazard Condition Explanation:
[a]Parachute reefing mechanism (cutter) failure could lead to hard landing, possibly outside intended landing zone
[b]Premature activation of the device could lead to torn or non-functional parachutes</td></tr>
<tr><td>Drogue Release Devices</td><td>Failure to release properly or releases prematurely</td><td></td><td></td><td></td><td></td><td>X[a]</td></tr>
<tr><td colspan="7">Specific RRMs:
• Designate and control a safety zone outside the intended landing zone.
• Redundant drogue release mechanism

Hazard Condition Explanation:
[a] Drogue release failure could cause interference with later parachute stages, degraded performance, and/or a hard landing possibly outside the intended landing zone. The reentry of Soyuz 1 resulted in a similar situation when the reserve parachute became tangled with the drogue chute and resulted in a hard landing outside the intended landing zone.</td></tr>
<tr><td>Stage Separation Arming Devices</td><td>Failure to arm or arms inadvertently</td><td>X
(secondary condition)</td><td>X[a]</td><td></td><td></td><td>X[a]</td></tr>
<tr><td colspan="7">Specific RRMs:
• Multiple “either/or” arming paths (timer, altimeter, sequencer, etc.)
• Arming circuitry and mechanisms feedback

Hazard Condition Explanation:
[a]During Soyuz 18-1 launch, the third stage failed to separate. Control of the vehicle was lost and the crew capsule was separated from the booster. This led to an uncontrolled landing in which the crew experienced a 20+ g reentry and landed thousands of km from the intended landing site.</td></tr>
</table>

[13] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
[redacted]	[redacted]	**Vehicle Breakup**	**Vehicle Loss of Control**	**Uncontrolled Release of Debris**	**Uncontrolled Release of Hazardous Material[14]**	**Prohibits Safe Landing**
Operational Ordnance						
Stage Separation Charges	Failure to fire/initiate	X (secondary condition)	X[a]			X[a]
<u>Specific RRMs:</u> • Incorporate redundant firing system into design <u>Hazard Condition Explanation:</u> [a]During Soyuz 18-1 launch, the third stage failed to separate. Control of the vehicle was lost and the crew capsule was separated from the booster. This led to an uncontrolled landing in which the crew experienced a 20+ g reentry and landed thousands of km from the intended landing site.						
Flight Safety Systems						
Propellant Dumping System	Failure to unload propellant prior to landing					X[a]
	Premature or unintended unloading during normal flight		X[b]		X[c]	X[a]
<u>Hazard Condition Explanation:</u> [a]Propellant dumping system failure may lead to inability to off-load propellant (and thus reduce vehicle mass) for a safe landing. [b]Unintentional dumping of propellant could cause unexpected loads and forces (loss of vehicle mass) on the vehicle, leading to loss of control. [c]OMCO if a hazardous propellant is used.						

[14] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[15]	Prohibits Safe Landing
		Flight Safety Systems				
Pilot	Incapacitated	X (secondary condition)	X[a]	X (secondary condtion)	X (secondary condtion)	X[a]

Notes:

- Pilot can become safety-critical if his incapacitation leaves the vehicle with no other means of control
- Pilot may not be on-board vehicle
- Circumstances which could lead to pilot incapacitation include:
    - Injury/illness
    - Human factors/human limitations issues
    - Contaminated cabin atmosphere or breathing media

Specific RRMs:

- Procedures of contingency operations are identified and incorporated into system prior to launch
- Multiple fault tolerance in flight control systems
- Caution and Warning (C&W) available to pilot and ground support
- Alternate sources of coolant for the pilot suit pressure (redundancy)
- Appropriate safety factors of suit oxygen and coolant lines
- Human limitation considerations integrated into design solutions
- Crew procedure(s) readiness
- Pre-launch monitoring of vehicle flight systems (thermal, atmosphere, controls) by ground crew
- Launch commit criteria well-defined

Hazard Condition Explanation:

[a]OMCO if the pilot is the only means of vehicle control.

[15] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[16]	Prohibits Safe Landing
Flight Safety Systems						
Flight/Thrust Termination System	Failure to initiate when commanded		X[a]			X (secondary condition)
	Premature or unintended operation	X[b]	X[a]			X[c]
Notes: • The flight/thrust termination system does not necessarily have to be a destructive system. Hazard Condition Explanation: [a]In the case of a non-destructive thrust termination system, a failure to initiate could lead to unanticipated loads on the vehicle, causing a loss of control. [b]OMCO for a destructive flight termination system. [c]An unanticipated loss of thrust could prevent a powered descent vehicle from safely reaching its intended landing and/or abort site.						
Ejection Seats	Unintentional activation	X (secondary condition)	X[a]	X (secondary condition)	X (secondary condition)	X (secondary condition)
Notes: • Unintentional activation could incapacitate the pilot and/or lead to cabin fire Specific RRMs: • Use of proven ordnance, electrical circuitry and ejection seat technology with dual fault tolerance in control loop. Hazard Condition Explanation: [a]An unintentional activation could incapacitate an onboard pilot. OMCO if the pilot is the only means of vehicle control.						

[16] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[17]	Prohibits Safe Landing
Flight Controls (Mechanical)						
Elevators	Detachment from vehicle	X (secondary condition)	X[a]	X[b]		X (secondary condition)
	Mechanical/Electrical/Pneumatic Malfunction (to perform proper operation)	X (secondary condition)	X[a]	X (secondary condition)		X (secondary condition)
Hazard Condition Explanation: [a]Loss of a control surface could lead to loss of vehicle control. [b]Detached control surface becomes debris.						
Ailerons	Detachment from Vehicle	X (secondary condition)	X[a]	X[b]		X (secondary condition)
	Mechanical/Electrical/Pneumatic Malfunction (Failure to perform Failure proper operation)	X (secondary condition)	X[a]	X (secondary condition)		X (secondary condition)
Hazard Condition Explanation: [a]Loss of a control surface could lead to loss of vehicle control. [b]Detached control surface becomes debris.						
Rudders	Detachment from Vehicle	X (secondary condition)	X[a]	X[b]		X (secondary condition)
	Mechanical/Electrical/Pneumatic Malfunction (Failure to perform proper operation)	X (secondary condition)	X[a]	X (secondary condition)		X (secondary condition)
Hazard Condition Explanation: [a]Loss of a control surface could lead to loss of vehicle control. [b]Detached control surface becomes debris.						

[17] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	**Vehicle Loss of Control**	**Uncontrolled Release of Debris**	**Uncontrolled Release of Hazardous Material[18]**	**Prohibits Safe Landing**
Flight Controls (Mechanical)						
Spoilers	Detachment from Vehicle	X (secondary condition)	X[a]	X[b]		X (secondary condition)
	Mechanical/Electrical/Pneumatic Malfunction (Failure to perform proper operation)	X (secondary condition)	X[a]	X (secondary condition)		X (secondary condition)
Hazard Condition Explanation: [a]Loss of a control surface could lead to loss of vehicle control. [b]Detached control surface becomes debris.						
Flaps	Detachment from Vehicle	X (secondary condition)	X[a]	X[b]		X (secondary condition)
	Mechanical/Electrical/Pneumatic Malfunction (Failure to perform proper operation)	X (secondary condition)	X[a]	X (secondary condition)		X (secondary condition)
Hazard Condition Explanation: [a]Loss of a control surface could lead to loss of vehicle control. [b]Detached control surface becomes debris.						
Brakes	Mechanical Malfunction (Failure to stop vehicle)					X[a]
Hazard Condition Explanation: [a]Failure of the brakes at landing could cause the vehicle to leave the runway, possibly endangering the uninvolved public.						

[18] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[19]	Prohibits Safe Landing
Flight Controls (Mechanical)						
Drag Devices	Failure to deploy	X[a]	X (secondary condition)	X (secondary condition)	X (secondary condition)	X[b]
<u>Specific RRMs:</u> • Incorporate redundant release system, one component of which is possibly an ordnance or manual back-up <u>Hazard Condition Explanation:</u> [a]Vehicle breakup could be caused by high aerodynamic an/or g loads on a vehicle resulting from the failure of a drag device to deploy. [b] During the Soyuz 1 reentry, the main parachute failed to deploy. The reserve parachute tangled with the drogue chute and the capsule crashed. A similar failure of a parawing could lead to an impact outside the landing zone.						
Flight Controls (Electrical/Electronic)						
Antenna	Failure to receive/transmit correct data		X[a]			X[b]
<u>Hazard Condition Explanation:</u> [a]The identified failure mode could result in a loss of, and/or corrupt, guidance and control data which could lead to a loss of control, especially in autonomous systems. [b]Loss of, and/or corrupt, vehicle position data could prevent a vehicle from safely reaching its landing and/or abort site.						
Data Receiver/ Transmitter	Failure to receive/transmit correct data		X[a]			X[b]
<u>Hazard Condition Explanation:</u> [a]The identified failure mode could result in a loss of, and/or corrupt, guidance and control data which could lead to a loss of control, especially in autonomous systems. [b]Loss of, and/or corrupt, vehicle position data could prevent a vehicle from safely reaching its landing and/or abort site.						

[19] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[20]	Prohibits Safe Landing
Flight Controls (Electrical/Electronic)						
GPS Hardware	Failure to provide correct position information		X[a]			X[b]
	Loss of Signal		X[a]			X[b]
Hazard Condition Explanation: [a]GPS malfunction (such as faulty or no signal) could lead to loss of vehicle control if the GPS input is required for vehicle guidance and control functions [b]Loss of, and/or corrupt, position data could prevent a vehicle from safely reaching its landing and/or abort site.						
Computer	Mechanical malfunction		X[a]			X[a]
Notes: • Computer malfunction could lead to an inability to accurately process vehicle performance data • Computer malfunction could lead to an inability to accurately monitor vehicle health • Computer malfunction could lead to an inability to accurately process telemetry data to determine correct vehicle position and orientation Specific RRMs: • Incorporate redundant distributed signal for command processing • Ensure that configuration is multiple-fault tolerant (can sustain any two failures) • Incorporate autonomous auto-land or attitude hold sequence • Incorporate user error correction protocols • Ensure ground uplink backup • Require positional backup with redundant feedback Hazard Condition Explanation: [a]During an Armadillo Aerospace test flight, vehicle vibration caused an electronics connector to be pulled from the power bus; the vehicle immediately went out of control and crashed.						
Voice Communications	Failure to receive/transmit adequate verbal communication					X[a]
Hazard Condition Explanation: [a]Loss of voice communications during descent and landing could prevent a vehicle from safely reaching its landing and/or abort site. Proper and adequate pilot training and experience could significantly reduce the risk of this hazard condition.						

[20] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[21]	Prohibits Safe Landing
Flight Controls (Electrical/Electronic)						
Active Sensors and Vehicle Position Transducers	Loss of performance data or control signals		X[a]			X[b]

Notes:

- Active Sensors and Transducers (i.e. pressure gages, position transducers, Linear Variable Differential Transformers, etc.) are those whose output directly affects the guidance and control of the vehicle.
- Sensor/Transducer malfunctions could result in faulty data being passed to on-board systems including the pilot and guidance and control systems

Specific RRMs:

- Incorporate redundant sensors/transducers for critical measurements that affect the control and guidance of the vehicle
- Employ “AND Gate” with majority logic voting software for the monitored sensor output signals and events

Hazard Condition Explanation:

[a]The identified failure mode could result in a loss of, and/or corrupt, guidance and control data which could lead to a loss of control, especially in autonomous systems.

[b]Loss of, and/or corrupt, vehicle position data could prevent a vehicle from safely reaching its landing and/or abort site.

Item	Failure Mode	Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material	Prohibits Safe Landing
Displays	Faulty or no display of data on monitors		X[a]			X[b]

Specific RRMs:

- Employ redundant display screens and associated circuit networks
- Employ “distributed” processing platform for on-board computation

Hazard Condition Explanation:

[a]The identified failure mode could result in a loss of, and/or corrupt, guidance and control data which could lead to a loss of control, especially in autonomous systems.

[b]Loss of, and/or corrupt, vehicle position data could prevent a vehicle from safely reaching its landing and/or abort site.

[21] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	**Vehicle Loss of Control**	**Uncontrolled Release of Debris**	**Uncontrolled Release of Hazardous Material**[22]	**Prohibits Safe Landing**
Flight Controls (Electrical/Electronic)						
Wiring/Connectors	"Open" or "Shorted" Circuitry		X[a]		X (secondary condition)	
	Faulty installation of wiring or connectors		X[a]		X (secondary condition)	

Notes:

- Short circuit or faulty wiring could lead to fire hazard

Specific RRMs:

- Locking type connectors should be used as bent pins can cause mishaps.
- Redundant paths should not go through the same connector
- Wiring should be installed to avoid chafing and/or splicing.
- Insulation resistance should be adequate to withstand any environmental conditions
- Incorporate redundant wiring circuits for critical measurements that affect the control and guidance of the vehicle
- Avoid redundant path wiring in a single wire bundle.
- Complete "end-to-end" continuity and functional checkout tests as part of vehicle final processing operations
- Install circuit breakers and fault interrupters
- Install fiber optics or laser-guided communication systems, where appropriate

Hazard Condition Explanation:

[a]Failure of circuitry associated with any guidance and/or navigation function (i.e., flight computer, GPS) could lead to vehicle loss of control.

[22] See Hazardous Materials Table, 49 CFR 172.101

<table>
<tr><th>Item</th><th>Failure Mode</th><th colspan="5">Hazard Condition/Suggested Risk Reduction Measures (RRMs)</th></tr>
<tr><th></th><th></th><th>Vehicle Breakup</th><th>Vehicle Loss of Control</th><th>Uncontrolled Release of Debris</th><th>Uncontrolled Release of Hazardous Material[23]</th><th>Prohibits Safe Landing</th></tr>
<tr><td colspan="7"><b>Environmental Control and Life Support Systems (ECLSS)</b></td></tr>
<tr><td>Cabin Materials</td><td>Loss of Fire Resistance</td><td></td><td>X[a]</td><td></td><td></td><td>X[a]</td></tr>
<tr><td colspan="7"><u>Specific RRMs:</u>
• Design cabin materials to:
  • preclude ignition in an atmosphere of 30% or less O2
  • contain ignition in an atmosphere of 30% or less O2
  • control ignition in an atmosphere of 30% or less O2
• Test cabin materials for ability to self-extinguish in atmosphere of 30% or less Oxygen
• Conduct Aging Program to determine degradation of materials used for fire resistance
• Caution and Warning (C&W) to pilot and ground
• Install smoke detectors
• Install fire extinguishers

<u>Hazard Condition Explanation:</u>
[a]A cabin fire could incapacitate a pilot and/or other control mechanisms, leading to vehicle loss of control and, possibly, inability to safely reach the landing and/or abort site.</td></tr>
<tr><td>Cabin Atmosphere Regulation Hardware</td><td>Excessive oxygen (in the Cabin)</td><td></td><td>X[a]</td><td></td><td></td><td>X[a]</td></tr>
<tr><td colspan="7"><u>Notes:</u>
• Malfunction could lead to excessive oxygen concentration which could increase fire risk

<u>Specific RRMs:</u>
• Safety factor of 4.0 for O2 lines
• Safety Factor of >2.0 for O2/N2 tanks
• C&W connected to pilot/crew suits and visible to pilot and ground crews

<u>Hazard Condition Explanation:</u>
[a]A change in cabin atmosphere could incapacitate an onboard pilot. OMCO if the pilot is the only means of vehicle control.</td></tr>
</table>

[23] See Hazardous Materials Table, 49 CFR 172.101

<table>
<tr><th>Item</th><th>Failure Mode</th><th colspan="5">Hazard Condition/Suggested Risk Reduction Measures (RRMs)</th></tr>
<tr><th></th><th></th><th>Vehicle Breakup</th><th>Vehicle Loss of Control</th><th>Uncontrolled Release of Debris</th><th>Uncontrolled Release of Hazardous Material[24]</th><th>Prohibits Safe Landing</th></tr>
<tr><td colspan="7"><b>Environmental Control and Life Support Systems (ECLSS)</b></td></tr>
<tr><td>Pressurized Cabin</td><td>Loss of pressure (in the Cabin)</td><td></td><td>X[a]</td><td></td><td></td><td>X[a]</td></tr>
<tr><td colspan="7"><u>Notes:</u>
• Pressure loss could be caused by O2 system malfunction, cabin leak, debris impact, etc.

<u>Specific RRMs:</u>
• Safety factor of 4.0 for O2 lines
• Safety Factor of >2.0 for O2/N2 tanks
• 1.5 safety factor of cabin pressure vessel
• C&W available to pilot and ground crews
• Redundant sources of cabin pressure
• >2.0 safety factor of windows and windshield
• Planned bird dispersal and/or avoidance techniques
• Alternate sources of O2 for the pilot suit pressure (redundancy)

<u>Hazard Condition Explanation:</u>
[a]A rapid change in cabin pressure could incapacitate an onboard pilot if not wearing a pressure suit. OMCO if the pilot is the only means of vehicle control.</td></tr>
<tr><td>Cabin Pressurization System</td><td>Overpressure condition (in the cabin)</td><td></td><td>X[a]</td><td>X[b]</td><td></td><td>X[a]</td></tr>
<tr><td colspan="7"><u>Specific RRMs:</u>
• 1.5 safety factor of cabin pressure vessel
• C&W available to pilot and ground crews
• >2.0 safety factor of windows and windshield
• Alternate sources of O2 for the pilot suit pressure (redundancy)

<u>Hazard Condition Explanation:</u>
[a]A rapid change in cabin pressure could incapacitate an onboard pilot. OMCO if the pilot is the only means of vehicle control.
[b]Overpressurization of the cabin could cause the pressure vessel to burst, causing debris .</td></tr>
</table>

[24] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[25]	Prohibits Safe Landing
Environmental Control and Life Support Systems (ECLSS)						
Cabin Atmosphere Controls	Contaminated air in the cabin		X[a]			X[a]

Notes:

- Mechanical malfunction could lead to contamination or loss of breathable atmosphere (due to O2 system malfunction, cabin leak, toxic fumes, excessive CO2 concentrations, and/or improper control of pressure system, etc.)
- Atmosphere contamination could lead to incapacitation of pilot and/or controller

Specific RRMs:

- Safety factor of 4.0 for O2 lines
- Safety Factor of >2.0 for O2/N2 tanks
- 1.5 safety factor of cabin pressure vessel
- C&W available to pilot and ground crews
- Operator training in regulator systems
- Air quality monitoring by ground crew
- CO2 monitoring
- LiOH/Charcoal canisters to filter cabin

Hazard Condition Explanation:

[a] A change in cabin atmosphere could incapacitate an onboard pilot. OMCO if the pilot is the only means of vehicle control.

[25] See Hazardous Materials Table, 49 CFR 172.101

Item	Failure Mode	Hazard Condition/Suggested Risk Reduction Measures (RRMs)				
		Vehicle Breakup	Vehicle Loss of Control	Uncontrolled Release of Debris	Uncontrolled Release of Hazardous Material[26]	Prohibits Safe Landing
Environmental Control and Life Support Systems (ECLSS)						
Cabin Temperature Control System	Loss of Cabin Cooling/Heating Control		X[a]			X[a]

Notes:

- Mechanical malfunction could lead to excessive cabin temperatures due to a system failure (coolant line contamination or clogging, coolant line leak, coolant tank leak and/or rupture, pump and/or regulator malfunctions, etc.)
- Excessive cabin temperatures could incapacitate the pilot and/or controller

Specific RRMs:

- Inspection and checkout of coolant system (regulator, reservoir, and lines) prior to launch
- Multiple fault tolerances on thermal control components
- C&W available to pilot and ground
- Alternate sources of coolant for the pilot suit pressure (redundancy)
- Safety factor of 2.0 for coolant lines
- Operator training in regulator systems operations

Hazard Condition Explanation:

[a]A change in cabin atmosphere could incapacitate an onboard pilot. OMCO if the pilot is the only means of vehicle control.

Recovery Hardware						
Parachutes	Failure to deploy or open properly	X[a]				X[b]

Specific RRMs:

- Increase design margin on parachutes
- Designate and control a safety zone outside the intended landing zone.

Hazard Condition Explanation:

[a]Vehicle breakup could be caused by high aerodynamic an/or g loads on a vehicle resulting from the failure of a drag device to deploy.

[b] During the Soyuz 1 reentry, the main parachute failed to deploy. The reserve parachute tangled with the drogue chute and the capsule crashed. A similar failure of a parawing could lead to an impact outside the landing zone.

[26] See Hazardous Materials Table, 49 CFR 172.101

<table>
<tr><th rowspan="2">Item</th><th rowspan="2">Failure Mode</th><th colspan="5">Hazard Condition/Suggested Risk Reduction Measures (RRMs)</th></tr>
<tr><th>Vehicle Breakup</th><th>Vehicle Loss of Control</th><th>Uncontrolled Release of Debris</th><th>Uncontrolled Release of Hazardous Material[27]</th><th>Prohibits Safe Landing</th></tr>
<tr><td colspan="7"><b>Recovery Hardware</b></td></tr>
<tr><td rowspan="2">Airbags</td><td>Premature deployment</td><td></td><td>X[a]</td><td></td><td></td><td></td></tr>
<tr><td>Failure to deploy</td><td></td><td></td><td></td><td></td><td>X[b]</td></tr>
<tr><td colspan="7"><u>Specific RRMs:</u>
• Design Safe and Arm system with multiple “AND” logic arming paths

<u>Hazard Condition Explanation:</u>
[a]The unintentional deployment of an airbag at high altitude and/or velocity could cause non-nominal aerodynamic and/or g loads on a vehicle which could result in loss of control of the vehicle.
[b] Failure of the airbag to properly deploy on descent could result in a hard landing, possibly outside of the target zone.</td></tr>
<tr><td rowspan="2">Landing Gear</td><td>Failure to deploy or extend properly</td><td></td><td></td><td></td><td></td><td>X[a]</td></tr>
<tr><td>Unintentional Deployment</td><td>X
(secondary condition)</td><td>X[b]</td><td>X
(secondary condition)</td><td></td><td></td></tr>
<tr><td colspan="7"><u>Specific RRMs:</u>
• Design gear deployment interlock to prevent high-speed deployment, include manual override
• Incorporate multiple “non-identical” landing gear extension schemes
– For example, the Space Shuttle uses a) gravity; b) hydraulics; and c) Ordnance, if needed

<u>Hazard Condition Explanation:</u>
[a]OMCO
[b]On X-15 flight 2-36-63, the main landing gear extended during flight at Mach 4+. Resultant asymmetric drag made control difficult.</td></tr>
</table>

[27] See Hazardous Materials Table, 49 CFR 172.101

Annex A X-33 Preliminary Casualty Expectation Analysis

Below is a list of parameters used in modeling the X-33 Expected Casualty. This list may be compared with the parameters used in the examples in section 5.2.1 and 5.2.2.

Parameters used in the modeling the X-33 Expected Casualty include:

- Trajectory Modeling
  - Potential trajectories from Space Port 2000 and Haystack Butte to potential landing sites
  - Vehicle position and velocity (speed) updated every 10 seconds of powered flight
  - Trajectories “moved” earth-relative in order to evaluate debris risks from other candidate launch sites on Edwards
- Atmospheric Modeling
  - Mean (average) annual winds at Edwards
  - Edwards Air Force Base winds aloft
  - Range Commanders Council Range Reference Atmosphere
  - Population Modeling:
  - Population numbers,
  - Facility shelter types and coverage areas throughout the base and local communities
  - database for downrange cities, towns, and rural population to cover all areas potentially at risk
- Vehicle Reliability Modeling
  - Assumed failure probability 1/250, derived from 220 seconds of powered flight from comparable expendable launch vehicles (Atlas, Delta, and Titan II) and Space Shuttle LH2 and LOX main engines used for launch through Main Engine Cut Off
  - Assumed engineering reliability factors based on component data, degree of redundancy, and comparable components used to establish a failure probability of 1/6823 for MECO to landing
- Failure Characteristics Modeling
  - Failure scenario includes both uncontained engine failure and loss of thrust/control failure modes
  - Both failure modes assumed to result in vehicle breakup and explosion

The parameters used for Vehicle Reliability Modeling are worth noting in particular. Note that the assumed vehicle failure probabilities are assumed based upon analogous historical launch activities. The preliminary nature of this analysis made those assumptions acceptable.

However, before the AF were to grant flight approval, vehicle-specific failure probabilities would need to be developed, approved, and applied in the analysis. It is the development of those values that would largely drive deeper systems analysis to identify safety-critical systems as outlined in this document.

In order to perform hazard modeling and risk projections, and “X-33 debris library” was estimated. The evaluation identified X-33 intact debris pieces likely to result from worst-case vehicle breakup (1 ton trinitrotoluene (TNT) equivalent) in-flight explosion.

To create the debris library, engineers consulted with subcontractors and vendors for estimation of subsystem breakup mechanisms for propellant tanks, main propulsion system;, avionics, landing gear, thermal protection system, ruddervators, rudders, thrust and intertank structure, turboalternators, main engines and engine ramps, etc. From the breakup analysis, 1269 components or intact debris pieces were identified. These pieces accounted for 18,900 kg (41,700 lb.) of 26,600 kg (58,700 lb.) of X-33 dry mass. Basic vehicle composition was expected to be: 30% composites (graphite/epoxy); 21% inconel/MA-754/ 19% aluminum; 16% steel; 10% titanium; and 4% ORCC.

For each identified piece of debris the following parameters were determined:

- unit weight
- quantity
- dimensions
- approximate shape for ballistic coefficients
- material composition

Figure 7 is a sample of the X-33 debris library created for this preliminary analysis.

With a debris library in place, the next task was to determine the impact point for each piece of debris. This impact point must take into account atmospheric perturbations, winds, the impulse delivered to each piece of debris by a vehicle explosion, the aerodynamic characteristics of each piece of debris and other parameters.

Since the impact point moves with time as the flight progresses, debris impact points must be computed at several time stations along each trajectory under the assumption that a failure may occur at any time in the flight.

Figure 8 is a map of debris impact ellipses for an X-33 flight from Edwards AFB (Haystack Butte) to Malmstrom AFB in Montana. It should be noted that Malmstrom was only one of several candidate landing sites for the X-33 and that this analysis was undertaken for each site.

Finally, with the debris impact points mapped, the population models in place, and the vehicle reliabilities determined to first order, it was possible to derive a preliminary Expected Casualty value for an X-33 flight via a probabilistic combining of these probabilistic models. The X-33 program estimated in this preliminary analysis that their Expected Casualty for this flight was 4.5 x 10^{-6}.

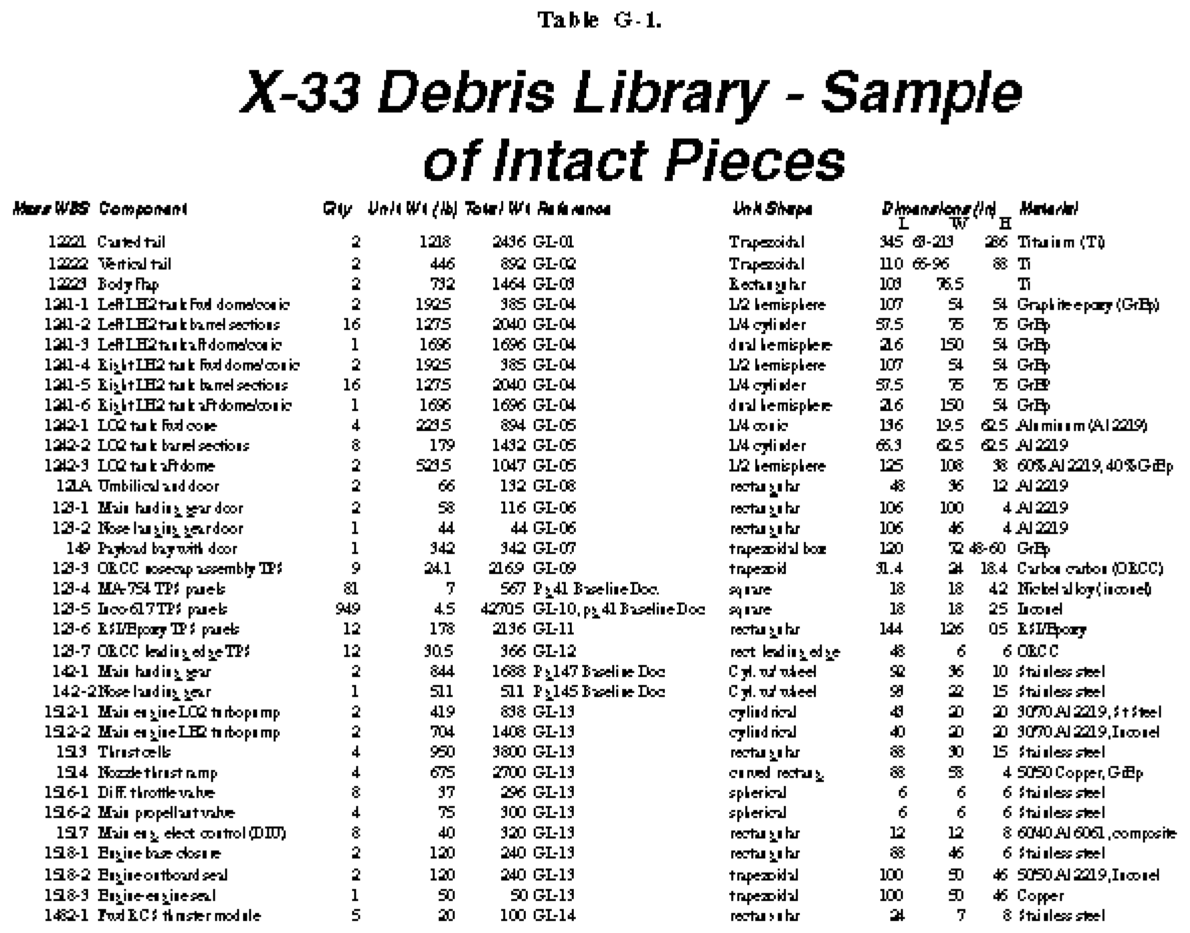

Table G-1.

X-33 Debris Library - Sample of Intact Pieces

Mass WBS	Component	Qty	Unit Wt (lb)	Total Wt	Reference	Unit Shape	Dimensions (in) L	W	H	Material
12221	Canted tail	2	1218	2436	GL-01	Trapezoidal	345	68-213	286	Titanium (Ti)
12222	Vertical tail	2	446	892	GL-02	Trapezoidal	110	66-96	88	Ti
12223	Body Flap	2	732	1464	GL-03	Rectangular	103	76.5		Ti
1241-1	Left LH2 tank Fwd dome/conic	2	192.5	385	GL-04	1/2 hemisphere	107	54	54	Graphite epoxy (GrEp)
1241-2	Left LH2 tank barrel sections	16	127.5	2040	GL-04	1/4 cylinder	57.5	75	75	GrEp
1241-3	Left LH2 tank aft dome/conic	1	1696	1696	GL-04	dual hemisphere	216	150	54	GrEp
1241-4	Right LH2 tank Fwd dome/conic	2	192.5	385	GL-04	1/2 hemisphere	107	54	54	GrEp
1241-5	Right LH2 tank barrel sections	16	127.5	2040	GL-04	1/4 cylinder	57.5	75	75	GrEP
1241-6	Right LH2 tank aft dome/conic	1	1696	1696	GL-04	dual hemisphere	216	150	54	GrEp
1242-1	LO2 tank Fwd cone	4	223.5	894	GL-05	1/4 conic	136	19.5	62.5	Aluminum (Al 2219)
1242-2	LO2 tank barrel sections	8	179	1432	GL-05	1/4 cylinder	66.3	62.5	62.5	Al 2219
1242-3	LO2 tank aft dome	2	523.5	1047	GL-05	1/2 hemisphere	125	108	38	60% Al 2219, 40% GrEp
121A	Umbilical and door	2	66	132	GL-08	rectangular	48	36	12	Al 2219
123-1	Main landing gear door	2	58	116	GL-06	rectangular	106	100	4	Al 2219
123-2	Nose landing gear door	1	44	44	GL-06	rectangular	106	46	4	Al 2219
149	Payload bay with door	1	342	342	GL-07	trapezoidal box	120	72	48-60	GrEp
123-3	C/CC nosecap assembly TPS	9	24.1	2169	GL-09	trapezoid	31.4	24	18.4	Carbon carbon (C/CC)
123-4	MA-754 TPS panels	81	7	567	Pg 41 Baseline Doc.	square	18	18	4.2	Nickel alloy (inconel)
123-5	Inco-617 TPS panels	949	4.5	42705	GL-10, pg 41 Baseline Doc	square	18	18	2.5	Inconel
123-6	RSI/Epoxy TPS panels	12	178	2136	GL-11	rectangular	144	126	0.5	RSI/Epoxy
123-7	C/CC leading edge TPS	12	30.5	366	GL-12	rect. leading edge	48	6	6	C/CC
142-1	Main landing gear	2	844	1688	Pg 147 Baseline Doc	Cyl. w/ wheel	92	36	10	Stainless steel
142-2	Nose landing gear	1	511	511	Pg 145 Baseline Doc	Cyl. w/ wheel	98	22	15	Stainless steel
1512-1	Main engine LO2 turbopump	2	419	838	GL-13	cylindrical	48	20	20	30/70 Al 2219, St Steel
1512-2	Main engine LH2 turbopump	2	704	1408	GL-13	cylindrical	40	20	20	30/70 Al 2219, Inconel
1513	Thrust cells	4	950	3800	GL-13	rectangular	88	30	15	Stainless steel
1514	Nozzle thrust ramp	4	675	2700	GL-13	curved rectang.	88	58	4	50/50 Copper, GrEp
1516-1	Diff. throttle valve	8	37	296	GL-13	spherical	6	6	6	Stainless steel
1516-2	Main propellant valve	4	75	300	GL-13	spherical	6	6	6	Stainless steel
1517	Main eng. elect control (DIU)	8	40	320	GL-13	rectangular	12	12	8	60/40 Al 6061, composite
1518-1	Engine base closure	2	120	240	GL-13	rectangular	88	46	6	Stainless steel
1518-2	Engine outboard seal	2	120	240	GL-13	trapezoidal	100	50	46	50/50 Al 2219, Inconel
1518-3	Engine-engine seal	1	50	50	GL-13	trapezoidal	100	50	46	Copper
1482-1	Fwd RCS thruster module	5	20	100	GL-14	rectangular	24	7	8	Stainless steel

Figure 7 – Sample of the X-33 Debris Library

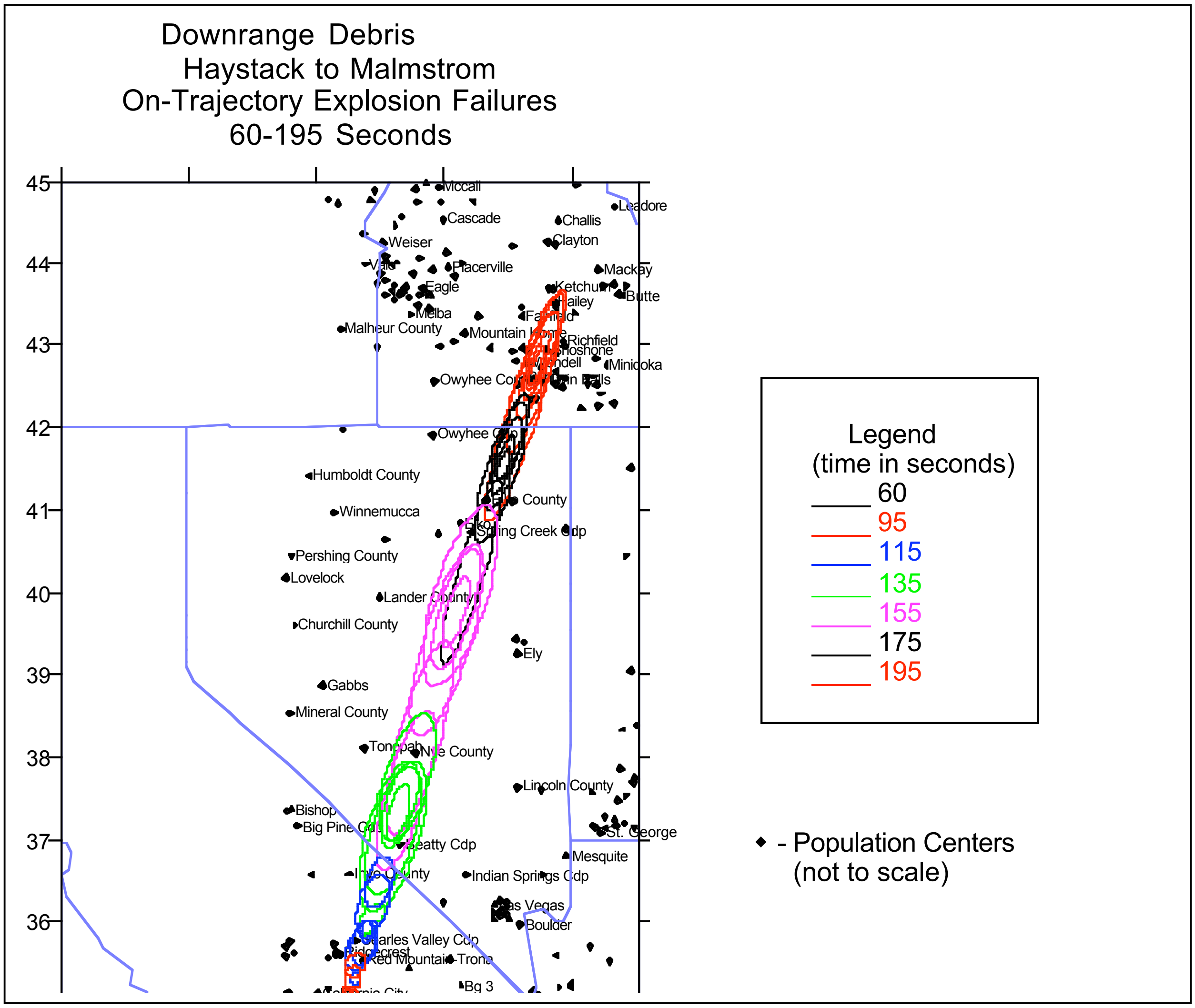

Figure 8 – X-33 Debris Impact Ellipses Haystack Butte to Malmstrom AFB