AIAA Atmospheric Flight Mechanics Conference and Exhibit
21 - 24 August 2006, Keystone, Colorado

AIAA 2006-6499

A Tiered Approach to Flight Safety Analysis

Daniel P. Murray*
Federal Aviation Administration, Washington, DC, 20549

A flight safety analysis quantitatively demonstrates that a launch or reentry vehicle is capable of flying a proposed mission below accepted limits for risk to the uninvolved public. Over time, sophisticated methodologies have been developed to estimate the risks posed by a particular mission by probabilistically modeling the outcomes of multiple potential vehicle failure scenarios and the various influences on those outcomes to a high level of engineering fidelity. However, variations in planned operations, along with limitations in the availability or quality of data, suggest a need for the identification of a broader, more generalized approach. Accordingly, a "tiered" approach to flight safety analysis is explored that advocates the use of simplifying, conservative assumptions in place of complex models as an initial iteration step. Subsequent iterations, if necessary, would employ increasingly less conservative assumptions and more complex modeling techniques until either an acceptable solution is reached or the highest available level of fidelity had been applied. The advantage of such an approach is twofold in that it encourages the design of safer operations for the sake of simplicity in the analysis and it standardizes methodologies for better comparison of results and determination of uncertainties.

Nomenclature

A_c	=	casualty area
D_p	=	population density
E_c	=	expected casualty
P_f	=	total vehicle probability of failure
P_i	=	probability of impact of a debris fragment within a populated area

I. Introduction

FLIGHT safety analyses are performed within the space launch industry to quantify the risks from proposed launch and reentry activities. As participants in the planning process for such activities, flight safety analysts are tasked with the responsibility of demonstrating that these risks are below acceptable limits for the uninvolved public and other parties. The analysis approaches employed can be quite complex in nature, requiring an extensive amount of data on the vehicle, its concept of operations, and the flight environment. The results of these and other more qualitative analyses are examined in light of their supporting assumptions to create flight rules or commit criteria for safely conducting the proposed operation.

This process has been in place for many years, providing decision makers with the information necessary to safely proceed with a proposed launch or reentry operation. The Federal launch ranges apply it, in conjunction with risk containment and mitigation strategies, to the launches of expendable launch vehicles (ELVs)[1]. NASA applies these techniques in a similar fashion to the launches and reentries of the Space Shuttle[2]. In accordance with the Commercial Space Launch Act (CSLA) and its amendments, the FAA's Office of Commercial Space Transportation (AST) has established regulations requiring commercial launch or reentry vehicle and launch or reentry site operator's license applicants to quantitatively demonstrate acceptable mission risk as well[3]. As part of the licensing process, AST typically performs its own flight safety analyses to assist in the evaluation of an applicant's analysis and to gain additional insight into the risks involved.

Unlike many other entities performing these analyses, AST has the unique challenge of applying these techniques to a variety of vehicles and operational concepts, including horizontally launched and recovered vehicles with many airplane-like qualities, including human pilots, as well as vertically launched vehicles similar in design to traditional ELVs. Even more challenging, AST must perform these analyses based on vehicles and operational

* Aerospace Engineer, Office of Commercial Space Transportation, AST-300, AIAA Member.

concepts at varying stages of development, from applicants with varying backgrounds and experience in quantitative risk analysis, and using data that is accordingly of varying quantities and quality.

AST holds all licensed launch and reentry operations to the same risk limits, and license applicants are ultimately denied a license to conduct their proposed operations if a suitable demonstration that these limits will not be exceeded cannot be provided. At the same time, the CSLA instructs AST to promote and facilitate the commercial space launch industry. As such, AST attempts to engage potential applicants as early as possible in their development process and continues to work closely with them as they navigate the regulatory process. Workshops and advisory documents are provided that familiarize first time applicants with the applicable regulations. Further, consultative support, tailored to an applicant's progress toward meeting those regulations, is provided to all applicants who request it. This process provides opportunities for the assessment of progress and receipt of feedback through technical interchange meetings and the submission of draft applications and analyses. However, even with this system in place, the flight safety analysis process has proven to be somewhat overwhelming for those prospective launch and reentry operators who are less familiar with its complexities.

For these reasons, AST is beginning to explore generalized approaches to flight safety analysis, applicable across the range of flight safety analysis problems. One approach identified thus far involves a "tiered" structure of analyses. Under this approach, flight safety methodologies of varying complexity would be matched with corresponding data requirements and then sequenced in terms of the number of trade-offs made between fidelity and conservatism. In this context, the term "conservatism" represents a flight safety analyst's attempts to produce results that overestimate the risks of a particular mission using plausible assumptions that simplify the analytical process while accounting for any additional uncertainty that these assumptions may provide. Even the highest fidelity analyses – those that produce the most accurate results when compared to actual events – contain a degree of uncertainty that results from a lack of complete knowledge of the mechanisms being modeled and the randomness that these mechanisms tend to exhibit. For this reason, flight safety analysts should strive to minimize uncertainty using the most appropriate methods for the given circumstances. As such, the tiered approach looks to gather existing methods and assumptions that have been successfully employed in the past and organize them in a manner that attempts to ensure that any steps made to simplify the analysis do not bias the results in a manner that underestimates the risks or overstates the analyst's confidence in the results. Accordingly, less experienced applicants could work progressively through each tier until acceptable results are computed while more experienced applicants could select the tier that best accommodates their mission objectives, level of flight safety analysis experience, and data availability.

Three basic tiers are outlined in the following sections. The two bounding tiers, a high and a low, are described first, with the high tier corresponding to a complex, physics-based analysis, and the low composed of risk containment strategies and highly conservative, simplifying assumptions. A medium tier is then defined to lie between these two ends, characterized by a mix of complexity and conservatism. A broad gap exists between the high and low, presenting opportunities for the medium tier to be tailored to the flight safety analysis experience level of the user, the availability and quality of their data, and the specifics of the problem at hand. AST is particularly interested in approaches that fall into this tier, as it is currently identifying and validating requirements for a future medium fidelity flight safety analysis computational tool to be provided to applicants and industry partners. As is the case with many other complex problems, there are advantages and disadvantages to a tiered approach, and these will be also be addressed.

At the heart of the majority of flight safety analyses is the computation of a risk quantity known as expected casualty. FAA regulations call for collective risk to be quantified in terms of expected casualty, and AST provides additional guidance on its computation in its Advisory Circular 431.35-1[3, 4]. Since many of the supporting analyses and simplifying assumptions discussed in the following sections relate to the composite elements of this quantity, a brief discussion of its meaning and purpose is provided as an introduction to the tiered approach.

II. Risk Management and Expected Casualty

Within the safety community, risk is often expressed as the product of the probability of occurrence of an event and the potential consequences of that event. If there is more than one possible outcome for an event, total risk is expressed as the sum, over all possible outcomes, of the products of the relative probability of each outcome and its associated consequence. The probability of occurrence of an outcome is expressed mathematically as a value between zero and one. However, the consequences of that outcome can theoretically take any value – the larger the value, the greater the risk. Risk can be relatively high if the probability of occurrence of an undesirable outcome is high or, if the consequence is great even while the probability is low. Mitigation measures that reduce the probability that a particular outcome will occur or ameliorating measures that reduce the consequences of that

outcome can be used to lower risk. For example, designing for high reliability in a vehicle system or subsystem can reduce the probability of its failure. If this system or subsystem performs a function that is essential to the safe operation of the vehicle, then this increase in reliability can mitigate the risks. Moreover, planning a mission that avoids the overflight of populated areas can decrease or eliminate consequences of human casualties even if the vehicle should fail, thereby ameliorating the consequences. Hence, the strength of a quantitative risk analysis lies not only in the resulting risk values, but also in the risk management decisions reached during the design of the operation and the performance of the analysis. In that regard, a quantitative risk criterion can serve as an indicator of when sufficient risk mitigation and ameliorization measures have been applied.

From a risk management perspective, the ideal scenario would place the operations in an area where the vehicle's performance would prevent it from reaching a populated area. This situation is known as "hazard isolation" or "complete containment". In this situation, the requirements of the flight safety analysis are reduced to a thorough analysis of the vehicle's trajectory that verifies the maximum range of the vehicle during nominal and off-nominal situations and its outputs include any operating restrictions that may be required to ensure containment, such as wind restrictions or limits on the amount of propellant loaded. Unfortunately, it is becoming exceedingly more difficult to find geographical locations that would allow for such operations without severe limits on vehicle and mission capabilities. More often than not, a "partial containment" approach is followed. In this situation, a sparsely or unpopulated operating area is sized to contain the normal flight of the vehicle and a flight safety system, composed of a limited number of highly reliable components, is activated during off-nominal flight to cease the vehicle's progress toward more densely populated areas or an operating area boundary. This approach is typically accomplished through thrust termination, followed by abort maneuvers or in some cases, vehicle destruction. As in the complete containment case, operations are ideally situated so as to minimize the likelihood of population overflight. However, since a potential for population overflight exists, a flight safety analysis is typically conducted to quantify the residual risk – the risk remaining after known risks have been reduced to acceptable levels.

This analysis would focus first on the construction of abort or destruct lines that would work in conjunction with abort criteria or flight rules to determine the circumstances under which the flight safety system should be activated. For instance, a flight rule might be proposed that required the termination of the flight prior to the point where the vehicle's instantaneous impact point crossed a boundary, such as a coastline or border. The terms of this rule would account for the subsequent ballistic or gliding flight of the vehicle and such factors as an operator's response times, hardware and software delays, winds, and map errors, in such a manner that would prevent an impact within a populated area. Risks to any populations within the abort/destruct boundaries or from a failure of the flight safety system would then be computed.

Within the flight safety analysis community, residual risks are often expressed in terms of expected casualty (E_c). Expected casualty computations combine a number of elements to produce the expected average number of human casualties per mission[4]. These elements include an estimate of the total probability of vehicle failure (P_f), one or more debris models or catalogs based upon the vehicle's failure modes from which to compute casualty areas (A_c), and the population density (D_p) of the region that the vehicle could potentially hazard.

Probability of failure encompasses the subset of all mission scenarios that could present risk to the public (i.e. failure modes) and the relative probability of their occurrence. System safety analyses and data from historical outcomes involving similar vehicles and operations are typically used as the basis for identifying potential modes and associated probabilities[5]. Casualty area represents the projected impact area of a piece of space vehicle debris on the Earth's surface within which any member of the public, if present, would be considered a casualty. The casualty producing area of potential debris fragments resulting from identified failure modes are computed, accounting for their projected area, the projected area of a typical person, and the extent of any subsequent hazards that their impacts can produce. Population density is extracted from existing models, typically based on census data.

In its most basic form, expected casualty represents the projection of a casualty area onto a population, as shown in Fig. 1, producing a number of people potentially at risk, and then scales that number by the probability that the risk to that population will exist.

The probability that the risk will exist represents both the probability that the vehicle will fail in a way that produces casualty-causing debris (P_f) and the probability that this debris will impact within the populated area (P_i). The product of each of these terms produces the

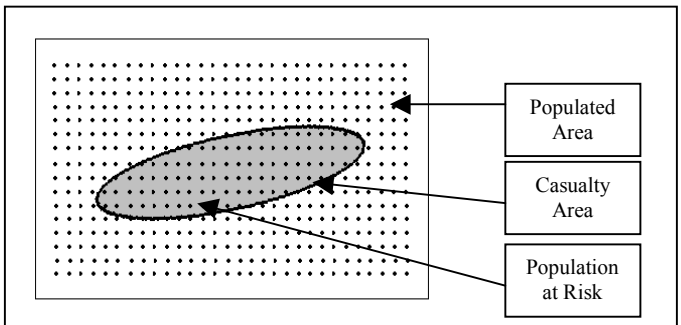

Figure 1. Basic Expected Casualty

number of casualties within that population that would be expected to result from that failure.

$$E_{c_i} = \left[\left(P_f \cdot P_i\right) \cdot A_c \cdot D_p\right]_i \tag{1}$$

This calculation is performed for all populations potentially at risk and then the resulting number of casualties associated with each population is summed to produce a total expected casualty value.

$$E_c = \sum_{i=0}^{n} E_{c_i} \tag{2}$$

The FAA chooses to address the risk from licensed commercial space launches and reentries in terms of casualties, where a casualty is defined as either a fatality or a serious injury, and currently limits total expected casualty to 30 casualties in one million missions. Acceptable analyses not only produce results below this threshold, but they also a valid representation of the potential risks. As such, the analyses must be thorough, methodical, and based on sound engineering principals. In that regard, a suitable demonstration of acceptable risk should encompass the probabilities and consequences of all reasonably expected scenarios, both nominal and off-nominal. In addition, any assumptions employed should be clearly identified, applied consistently, and supported by a combination of data, analysis, and valid engineering judgment. When assumptions are supported solely by engineering judgment or when the data or analyses applied contain a substantial amount of uncertainty, the analysis should include the sensitivity of the resulting expected casualty values to thosee uncertain inputs.

III. Tier 3: A High Fidelity Approach

High fidelity analyses produce expected casualty results to a high degree of engineering rigor through the use of tools that accurately model the physics of the problem. These tools typically account for such factors as the ability of a person to withstand the impact of a debris fragment, the ability of shelters to protect people from particular categories of debris, and the overlapping or interdependent effects of such phenomena as the aerodynamic lift and drag forces acting on falling debris, the effects of winds, and explosive imparted velocities.

High fidelity risk analyses are based on accurate models of the vehicle's trajectory across a wide variation of anticipated operating conditions. This includes the definition of a nominal trajectory, which defines the vehicle's path when all of the potentially variable parameters, including vehicle performance and atmospheric conditions, assume expected or optimal values, and dispersed trajectories, which model the effects of dispersions on this trajectory from foreseeable variations in those parameters. Malfunction trajectories that may result from vehicle component or system failures, such as a nozzle burn-through, gimbal lockup, flight control failure, or guidance and navigation errors, are also modeled. The resulting deviations from the nominal trajectory can result in tumble turns or trimmed turns, depending upon the stability characteristics of the vehicle across a range of angles of attack. For vehicles with abort capabilities, analysts also model the trajectories anticipated as a result of an abort decision. This collection of nominal, dispersed, failure, and abort trajectories, overlaid on a map, defines the region at risk from the proposed operation.

Vehicle failure scenarios are further analyzed as part of failure probability and debris analyses. A failure probability analysis examines the likelihood of the vehicle and its systems, subsystems, and components to fail in a manner that results in a hazard to the public. These analyses typically employ both top-down and bottoms-up analysis techniques. Preliminary hazard analyses, event trees, fault trees, and failure modes and effects analyses are examples of some these techniques, as described in detail in Ref. 5. The results of these analyses are supplemented by the results of a comprehensive validation and verification program[6] and historical data from previous operations of the vehicle in question or the operations of similar vehicles operated in similar circumstances, where available[7].

Once a total probability of failure estimate has been determined, relative probabilities are typically assigned to specific events or failure modes and allocated across mission phases. Historical data has suggested that powered (propulsive) flight phases result in more failures than unpowered phases[8, 9]. Within these phases, transient events such as engine ignitions and stage separations or other component jettisons have produced more failures than steady state operations. This sort of historical failure data can be culled using sophisticated filtering algorithms and weighting factors to produce a failure allocation model for vehicles of similar types and configurations[10].

A debris analysis estimates the number and characteristics of debris fragments generated by a vehicle failure. Several alternate catalogs of debris can be constructed, based on the anticipated outcomes of each of the potential

failure scenarios. For example, a breakup resulting from the high aerodynamic loads that could be encountered during a malfunction turn could produce debris with different characteristics than the debris generated upon the activation of a destructive flight termination system. Knowledge of the vehicle's material properties, anticipated operating envelope, design limitations, and structural weak points can provide insight into the contents of a debris catalog. Analysts typically begin to assemble a debris catalog using a list of the vehicle's components, focusing on attachment points and points of transition between component geometries to identify potential fracture locations. Analytical techniques such as finite element analyses, test results including the static and dynamic failure strengths of load-bearing components, and historical data from previous failures can be examined relative to the anticipated flight envelope to produce the contents of a catalog.

Supporting analyses identify characteristics of the debris that are used to estimate their points of impact and the extent of the hazards that these impacts can create. For example, explosions at altitude have the tendency to impart velocity on the resulting debris fragments, dispersing them from the point of failure as they begin to fall toward impact. The aerodynamic characteristics of falling debris and their tendency to become entrained in prevailing winds can further disperse their points of impact. Some fragments are capable of exploding on impact with the surface or an object on the surface. The yields and overpressures of these fragments are calculated based on estimates of the amounts of explosive material remaining at the time of failure and the amounts that mix or burn at the time of impact. Some fragments are capable of bouncing, sliding, or splattering upon impact. The resulting hazards of such impacts, including the characteristics and trajectories of these fragments and any ejected or propelled surface materials are assessed using a secondary effects analysis[11].

Some analyses are used to filter debris with particular characteristics out of a debris catalog. For instance, failures at the instances of peak aerodynamic heating can vaporize or incinerate debris fragments. Therefore, debris survivability analyses compare the material properties of the fragments in a debris catalog against the failure environment to determine if sufficient energy exists to reduce the size of debris fragments or eliminate them altogether from consideration in the risk analysis. In addition, the results of studies of human vulnerability are often used to determine if the impacting energy of surviving fragments of debris will be sufficient to cause a casualty to an unprotected person[12]. The characteristics of the potential fragments, including their orientation and relative angle of impact, and the area on the body of the impacted person can be examined against data from other trauma producing injuries to determine a threshold value for kinetic energy of impact sufficient to cause a casualty.

Population data is also adjusted to account for the effects of sheltering. Depending upon the type and construction of a structure, its roof and walls may be capable of protecting a person from some debris impacts. Pieces impacting with low kinetic energy may be simply deflected by a structurally reinforced roof. However, larger, more energetic debris can penetrate or even collapse a structure, potentially producing more extensive casualties. Sheltering analyses account for materials, construction type, and number of floors of structures at risk from impact and allocate percentages of the total population to these structures based on census counts, growth rates, and demographic information[13]. The number, sizes, types, and age of windows in a building are also examined to determine casualties from flying glass fragments generated from explosive shock waves.

Vehicles carrying large amounts of toxic materials or propellants require additional analyses to determine the risks from failures that release these materials into the atmosphere. In addition, vehicles capable of creating large explosions at or near the surface of the earth are examined to determine the effects of radiating shock waves reflected back toward the surface as a result of certain atmospheric conditions, an analysis known as far field overpressure blast effects.

While other analyses may be required depending upon the specifics of particular missions, the combination of supporting analyses described above constitutes the high tier which can be applied universally across the spectrum of vehicles and operational concepts currently being designed and operated. They are summarized in Table 1, along with some examples of the types of data required to conduct them. Specific requirements regarding these and other analyses, including required output quantities, can be found in FAA regulations[3].

Table 1: Summary of Example High Fidelity Tier Analysis Data Requirements

Supporting Analysis	Examples of Required Input Data
Trajectory	• Vehicle characteristics and performance data, such as mass properties, propulsive capabilities, aerodynamic and stability data, and performance variations • Mission-specific data such as the launch point location and flight azimuth, flight phases, mission objectives such as the target orbit or final position, the corresponding profile of guidance commands, wind data, and timing of mission events • Potential vehicle malfunction scenarios and vehicle turning capability as a result of a malfunction • Locations of abort/destruct boundaries
Probability of failure	• Potential hazards and failure modes and their effects and the effects of mitigation and ameliorization measures • Historical data from previous missions or similar vehicles or systems • Verification data from tests, demonstrations, or analyses of vehicle systems or subsystems
Debris risk	• Potential causes of vehicle breakup, including results of flight safety system actions • Vehicle aerodynamic and inertial load limits • Characteristics of resulting debris fragments, including number and size, ballistic coefficients, imparted velocities, explosive yields, and impacting kinetic energies • Wind data • Locations and populations of areas at risk, including automobiles, ships and aircraft • Locations and types of sheltering structures • Population demographic data • Impacting energy and surface characteristics for computing secondary effects • Material properties and failure conditions for computing debris survivability
Toxic release hazard	• Types and amounts of toxic materials • Meteorological data • Locations and populations of areas at risk • Locations and types of sheltering structures • Population demographic data • Human vulnerability data
Far field overpressure blast effects	• Meteorological data • Locations and populations of areas at risk • Locations and types of sheltering structures, including numbers, sizes, types, and ages of windows • Population demographic data • Human vulnerability data

Each of the supporting analyses listed in this table requires the analyst to obtain a working knowledge of relatively complex physical and scientific principles, an in-depth knowledge of the subject vehicle and its concept of operations, and an extensive amount of supporting data. Much of this information is typically unavailable early in the risk analysis process if the vehicle and operational concept are being concurrently designed and tested, as is often the case with many of the applicants that apply to AST for a launch or reentry license. A low tier that produces preliminary estimates requiring less data and simpler models would be useful in these situations to provide early identification of potential safety issues and risk reduction strategies, scope the resource requirements of future efforts, and perhaps bound the risks associated with the proposed operation. Further, it would present an option that

would tend to be less susceptible to errors when used by less experienced flight safety analysts. The following section proposes such a tier.

IV. Tier 1: A Low Fidelity Approach

Over time, a number of simplifying assumptions have been identified that can be used in place of some of the more complex supporting analyses described above under the high tier, such as population estimates, flight safety system failure rates, and the lethality of impacting debris. A subset of these simplifying assumptions provides maximum conservatism to the aspects of the analysis to which they are applied. Maximum conservatism implies worst-case conditions that, although they may be extremely unlikely to ever occur in reality, do not underestimate the likelihood or severity of the particular aspect of the analysis to which they are applied. As such, they relieve the analyst of the burden of gauging the sufficiency of the conservatism that they provide. The collection of these assumptions and the details of their application provide the basis for the low tier.

The most basic of theses assumes that the total vehicle probability of failure estimate is equal to one. This assumption is useful in situations where historical reliability data for either the vehicle or its safety-critical systems is either lacking or inapplicable. Such is the case for many research and development vehicles that utilize a number of new technologies or vehicles designed, manufactured, or operated by inexperienced parties. This assumption can be used in place of a total vehicle probability of failure estimate obtained through a probability of failure analysis. In addition, the analyst could assume that an impact of the vehicle or all of its debris will occur within the highest population density population area. This assumption completely removes probability from the expected casualty computation and focuses solely on the severity of the consequences. If the resulting risk values are sufficiently low even under these worst-case failure conditions, due either to a vehicle design that minimizes casualty area or a concept of operations that minimizes population overflight or both, the analyst may not have to proceed any further with the flight safety analysis.

In addition to probability, assumptions can also be applied to the casualty area element of the expected casualty computation to simplify the computations and relieve the analyst of the burden of collecting a large amount of data. For example, the analyst could assume that any physical contact between any debris fragment and a person causes a casualty. This assumption could be employed in place of human vulnerability analyses that assess the casualty-causing ability of particular debris fragments or the ability of a person to absorb the energy a particular impact without sustaining a serious injury. Since vehicle failures are capable of generating debris fragments of various sizes and weights, some smaller, lighter fragments that impact with lower kinetic energy might not be capable of causing a casualty if they struck a person. When determining the number of fragments that could potentially cause a casualty, the analyst could also assume that all debris survives to impact with the surface or an object on the surface. This assumption could be used in place of debris survivability analyses.

Assumptions can also be applied to conservatively model the characteristics of debris fragments and the circumstances of their impacts. For example, an analyst could assume that all inert debris impacts in the orientation that maximizes the casualty area. Since debris fragments, especially those with an irregular shape, may tumble as they fall, they can project a variable area onto the surface below and impact in any orientation. Alternatively, the aerodynamic forces acting on some debris fragments, such as those in the shape of a plate or a cylinder, may cause them to stabilize as they fall and impact end-on. Such impacts would produce smaller casualty areas than if they had impacted lengthwise. Assuming an impact of the fragment in an orientation that maximizes the amount of its surface area that it exposes to the surface conservatively overestimates the resulting casualty area corresponding to an impact in any other orientation.

If a debris fragment could be either inert or explosive, an analyst could assume the larger casualty area to remove the burden of determining the fragment's state at impact and add conservatism to the analysis. Solid rocket motor casings and liquid propellant tanks will not explode if they are empty, and even when some amount of propellant remains at impact, it still may not lead to an explosion. Further, depending upon the circumstances of the failure, a burning solid rocket motor may continue to burn as it falls to the surface, reducing the amount of explosive material on hand at impact and thus its casualty area. For vehicles using liquid propellants, the tanks containing these propellants could rupture or separate during a failure, dispersing the propellants to some extent and reducing or even eliminating the potential for them to mix and detonate on impact. By assuming an explosion and calculating the extent of that explosion assuming that no additional propellant burns or disperses between the time of failure and the time of impact and all remaining material contributes to the explosion, the analyst can be confident that he or she is bounding the severity of the impact without having to perform any additional analyses. Finally, secondary effects of debris, such as skip, bounce, and splatter could be conservatively overestimated by applying a multiplicative factor of seven to the debris casualty area, in place of a secondary effects analysis[11].

Worst-case assumptions can also be applied in a manner to reduce computational burden. For example, for a region with varying population density, an analyst could apply the highest density of any populated area within that region to every populated area within the region. By equating the population density variable in the expected casualty equation for all areas within the region to a constant value, this assumption would relieve the analyst of the burden of managing a potentially large amount of population data and expedite the computation. Alternatively, the analyst could apply the highest population density of any area in a region to the entire region as a whole. This assumption would reduce the required number of individual expected casualty computations for that region to just one, since a separate expected casualty computation is typically performed for each populated area.

As another example, aggregate casualty areas are often used to represent the total casualty area of a number of debris fragments. Rather than compute risks based on each casualty area associated with each debris fragment, the casualty areas are summed to compute an aggregate casualty area that is then used to produce one risk value per populated area. Although in reality the casualty areas of individual fragments would most likely overlap and reduce the total casualty area, aggregating provides additional conservatism and reduces the number of necessary computations.

Table 2 summarizes the assumptions described above. Note that this is not an exhaustive list; and a number of other assumptions of this nature may exist.

Table 2: Summary of Example Low Fidelity Tier Analysis Assumptions

Supporting Analysis	Simplifying Assumption
Probability of failure	• Assume a vehicle failure capable of causing a casualty will occur
Debris risk	• Assume an impact of the vehicle or all of its debris into the highest density populated area • Assume all debris impacts with sufficient energy to cause a casualty • Assume all debris survives to impact • Assume all debris impacts in an orientation that maximizes casualty area • Assume the larger casualty area of debris that could be either inert or explosive • Assume no solid propellant burns between the time of failure and time of impact • Assume no liquid propellant disperses between time of failure and impact • Assume complete mixing of all remaining propellants at impact • Assume a secondary effects factor of seven[11] • Apply the largest population density of any population center in a region at risk to all population centers • Apply the largest population density of any population center in a region to the entire region as a whole • Use aggregate casualty areas

Since these examples assume worse case conditions or maximum conservatism, their application is relatively straightforward. Accordingly, they provide a great deal of utility for preliminary analyses, providing the analyst with an opportunity to scope the extent of the problem and identify opportunities to mitigate or ameliorate risks early on, when programs generally have a higher tolerance for changes. For example, a preliminary risk computation may show that a particular populated area constitutes the majority of the total risk. A small change in the flight azimuth may reduce this risk by moving the proposed trajectory farther from this area. In that regard, choices made during the design of the vehicle and its concept of operations have the potential to lower risks. Note that, using a low fidelity approach, the exact risk value is not computed. Rather, the use of conservative assumptions serves to demonstrate that the risks are below the resultant value. When this value meets acceptable limits using valid conservative assumptions, no further analyses may be necessary. In that regard, choices made during the design of the vehicle and its concept of operations also have the potential to reduce the burden of a flight safety analysis.

However, situations exist in which overflight of populations is unavoidable. In these situations, the use of a number of simplifying, conservative assumptions, such as those listed above, would most likely produce risk

estimates that exceed the acceptable limits. The majority of operations conducted from inland launch sites will likely fall into this category. For that reason, a medium tier is necessary, in which a mixture of higher fidelity supporting analyses and conservative assumptions are applied to meet risk limits.

V. Tier 2: A Medium Fidelity Approach

Since there is a such broad gap between the high and low tiers, as presented above, there is ample opportunity for an analyst to pick and choose a combination of supporting analyses and conservative assumptions that best suit his or her experience level, the availability of data describing the vehicle and its concept of operations, and the needs of the problem at hand. Any number of permutations of analyses and assumptions could describe a medium tier flight safety analysis. In that regard, the medium categorization applies less to the specific assumptions employed and more to the general characteristics of those assumptions. Unlike those described under the low tier, medium tier assumptions tend not to maximize conservatism. In fact, depending upon the circumstances of its application, a particular assumption may apply conservatism to one analysis and not to another. For reasons such as these, the medium tier is characterized by the additional analyses that are typically required to determine if a sufficient amount of conservatism has been applied.

To cite a particular example, several mutually exclusive failure modes can be identified for a particular vehicle, such as an on-trajectory explosion, an on-trajectory intact inert impact, or a malfunction turn that results in an explosive or inert impact. Modeling each one of these modes separately provides additional insight into the severity of their hazards, but data describing the probability that one of these modes will occur relative to the others is typically difficult to obtain. Analysts often allocate conditional probabilities to each mode based on test data, historical data from similar vehicles, and engineering judgment. However, depending upon the severity of the outcomes of these failure modes, this allocation can greatly influence the resulting risk values. To characterize this influence, the analyst would gauge the sensitivity of the resulting risk values over a range of relative probabilities of occurrence of each failure mode. If historical data suggests a ratio of 85:15 may describe the relative probability of occurrence of on-trajectory failures to malfunction turns for similar vehicles, the analyst could compute the resulting risk using that allocation. If this produces acceptable results, the analyst could then apply some additional conservatism by assuming that the vehicle would fail more often in the worse case of the two failure modes than the historical data suggests. If the data suggests that a malfunction turn results in a more severe outcome, which is often the case, the analysts could recompute the resulting risk using a 75:25 or even a 50:50 ratio. If those ratios produce steadily increasing yet still acceptable risk results, then the analyst can gain more confidence that they have selected an appropriate ratio of failure modes and bounded the risk of the problem, even if in reality those ratios are less likely to occur.

Further complicating this situation is the fact that many of the simplifying assumptions employed in flight safety analyses offer a conditional conservatism that depends upon the circumstances under which they are applied. Returning to the example above, the assumption was made that malfunction turn failures are more severe than on-trajectory failures, and they were therefore weighted more heavily to produce more conservative results. As stated above, this assumption is typically conservative; however, it relies heavily on the distribution of the population at risk. If more of the population at risk is situated some crossrange distance away from the nominal trajectory, then decreasing the ratio of on-trajectory failures to malfunction turn failures has the effect of stretching out the probability of impact distribution, which is typically modeled as a normal distribution, exposing these populations to more risk. If, however, more population is situated closer to the nominal trajectory, the stretching of the distribution associated with this same ratio has the tendency to decrease the risks to these close-in populations. This circumstance is not easily verified by inspection and often requires the types of sensitivity analyses described in the example above.

Another example involves the assumption that the entire population at risk is standing in the open. This assumption is often employed in place of a sheltering analysis. In many circumstances, this assumption is more conservative, in that certain structures have the potential to protect the populations allocated within them from smaller, less energetic debris that would otherwise cause a casualty if it impacted any of these people directly. However, if there is a potential for a vehicle or its larger components to impact intact, the structure itself may contribute to the resulting casualty area. For instance, a larger casualty area tends to be produced when chunks of a penetrated roof fall upon the occupants of a structure than would have been produced if the same piece of debris had impacted in the open. Depending upon the type of construction of the structure, the material it is constructed from, and the energy of the impacting debris, whole roofs, floors, or even structures may collapse, further increasing the casualty area.

Two other assumptions that tend to fall into this conditionally conservative category include analyzing risk using historical worst-case winds in place of less severe seasonal, measured, or mission specific winds, and modeling malfunction turns as instantaneous high-angle turns rather than trajectories based on vehicle performance characteristics and structural limits. Both of these assumptions have the tendency to overestimate the area at risk. Generally, such overestimations produce more conservative risk estimates, since increases in the area at risk generally involve increases in the population at risk. However, if the rate of increase in area at risk overwhelms the rate of increase in population at risk, it can have the opposite effect, producing lower risk estimates.

The broad scope of the medium tier offers the analyst the flexibility to apply these and other assumptions successively in place of low tier assumptions or high tier supporting analyses. This provides the analyst with an opportunity to proceed iteratively from the low tier through the medium and toward the high, applying additional conditionally conservative assumptions or supporting analyses one at a time to gauge their effects on risk results. Experience gained through this process could assist the analyst in identifying additional assumptions, as well as establish more specific guidance and best practices for future analyses.

Table 3 lists a few of the assumptions that could be categorized as medium tier assumptions.

Table 3: Summary of Example Medium Fidelity Tier Analysis Assumptions

Supporting Analysis	Simplifying Assumption
Trajectory	• Assume instantaneous high-angle malfunction turns
Probability of failure	• Apply variable failure rates across flight phases • Apply conditional probabilities of occurrence to failure modes
Debris risk	• Assume all populations at risk are in the open (no sheltering) • Apply worst case winds

As was the case with the low tier described above, the medium tier also provides opportunities for the analyst to identify opportunities to lower risk through the addition of mitigation and ameliorization measures. For example, the consideration of a propellant dump system or additional abort opportunities could provide a basis from which the analyst could justify assumptions regarding the frequency of occurrence of explosive impacts with regard to inert impacts in a similar manner as the frequency of on-trajectory failures to malfunction turn failures was described above. Such assumptions could be explored in the context of high tier elements, such as component and subsystem reliability analyses and associated test results.

VI. Advantages and Disadvantages of a Tiered Approach

Like nearly all other aspects of space flight, flight safety analysis is not easy, even when employing a low fidelity approach or a user-friendly high fidelity tool. For that reason, the tiered approach is being explored as a candidate methodology for organizing the various techniques, supporting analyses, and simplifying assumptions in such a way as to promote a standardized approach to flight safety analysis, applicable across the range of problems that analysts currently face and foresee. Any standardized approach to flight safety analysis would allow for better comparison of results, provide for a more accurate assessment of uncertainties, and lay the foundations for a standardized set of tools. The tiered approach in particular, has the potential to do all these things and at the same time promote the design of operations that increase the applicability of conservative assumptions for the sake of simplicity in the analysis. Analysts with little or no flight safety experience would find such an approach advantageous, since performing many of the high tier analyses described above in an incorrect manner, either due to a lack of understanding of their complexities or the use of low quality or insufficient data, could create a false sense of safety.

At the same time, the tiered approach has its disadvantages. Heavy reliance on conservative assumptions has the tendency to oversimplify the problem and lead analysts away from the complexities and associated merits of higher fidelity approaches. Compounding conservatism through the use of multiple assumptions has the potential to produce outcomes that are too unrealistic to be applicable. Further, applying overly conservative assumptions to one aspect of an analysis may not make up for the uncertainty or lack of conservatism in another. For instance, to cite an example from the low tier used above, the conservatism that comes from assuming an impact of the vehicle or all of its debris into the highest density populated area may not be sufficient if the casualty area associated with such an impact has been underestimated.

Gauging sufficient conservatism in the number and types of assumptions so as to offset the potential effects of uncertainty or insufficient conservatism is difficult to determine. However, sensitivity analyses or other parametric studies can provide confidence bounds to help convey the uncertainty. Further, running multiple analyses using

various approaches can provide additional insight for decision makers. Even in circumstances where a lower-fidelity analysis is capable of clearly demonstrating acceptable flight risk, AST still advocates the use of multiple analyses of varying levels of fidelity whenever circumstances allow. No matter how conservative the simplifying assumptions employed are, some degree of uncertainty in the results always exists, and this uncertainty should be addressed and carefully considered throughout the analysis process. Multiple analyses using different methodologies and assumptions, used in concert with sensitivity and parametric studies, can provide further insight to help characterize this uncertainty.

VII. Conclusion

The tiered approach to flight safety analysis offers a basis from which an analyst can pursue a risk estimate across a hierarchy of assumptions and supporting analyses to determine the most appropriate combination. Like most any other analysis technique, it requires careful attention to the assumptions employed and a solid understanding of the aspects of the problem being modeled. Accordingly, the graduated level of complexity that spans from the low tier to the high tier offers the analyst the opportunity to gain the necessary skills and understanding in a more structured manner. Although an iterative application of this approach is not required, it provides a perspective with which the analyst can gauge the trade-offs made between fidelity and conservatism. As additional assumptions and supporting analyses are identified and the gap between the low and high tiers narrows, there is a potential for analyses to increasingly rely on successful precedent and less on engineering judgment. Sensitivity and uncertainty studies can provide additional information. Any tool designed to employ a tiered approach should be designed so as to accommodate these types of studies, and AST intends to incorporate such functionality as it continues to identify requirements for future tools.

Every problem that a flight safety analyst attempts to address is unique, as is typically the corresponding quantity and quality of the available input data. The potential for a particular approach to standardize the analysis process in such a way as to guide the analyst through it would be of great value to AST and many of the applicants it works with. For that reason, AST will continue to explore other potential methodologies that could be applicable across the broad range of flight safety analysis problems. The utility of any standardized approach will lie in its ease of understanding and its ability to accommodate the quality of the data on-hand and to compensate for a lack of additional data. In addition, it must be flexible so as to provide for opportunities to incorporate lessons learned during future analyses. In that regard, aspects of a standardized approach to flight safety analysis, as embodied in the tiered approach, can facilitate knowledge sharing and the use of best practices across programs, agencies, and perhaps industries, benefiting anyone conducting quantitative risk analyses.

References

[1] "Common Risk Criteria for National Test Ranges", Range Commanders' Council Range Safety Group Standard 321-02, June 2002

[2] Procedural Requirements 8715.5 – Range Safety Program, National Aeronautics and Space Administration, July 2005

[3] 14 CFR Parts 401, 404 et al., "Commercial Space Transportation Licensing Regulations – Final Rule", June 1999, September 2000, October 2000

[4] "Expected Casualty Calculations for Commercial Space Launch and Reentry Missions", FAA Advisory Circular 431.35-1, August 2000

[5] "Guide to Reusable Launch and Reentry Vehicle Reliability Analysis", Federal Aviation Administration, April 2005

[6] "Guide to Reusable Launch Vehicle Safety Validation and Verification Planning', Federal Aviation Administration, September 2003

[7] "Guidelines on Probability of Failure Analysis for New Expendable Launch Vehicles", Federal Aviation Administration, 2005

[8] "Launch and Performance Histories of US Space Launch Vehicles, Final Report", RTI International, January 2005

[9] "Analysis of Launch Vehicle Failure Trends", Futron Corporation, July 2006

[10] "Launch Vehicle Probability of Failure Allocation", RTI International, January 2003

[11] "Casualty Areas for Impacting Inert Debris for People in the Open", RTI International, April 1995

[12] "Human Vulnerability to Inert Debris", ACTA Inc., October 2002.

[13] *CAIB Report*, Columbia Accident Investigation Board (CAIB), August 2003