70th International Astronautical Congress, Washington, DC.

IAC-19-D6.1.6

FAA PROPOSED CONSEQUENCE PROTECTION CRITERIA FOR FLIGHT SAFETY SYSTEMS AND FLIGHT ABORT FOR COMMERCIAL SPACE TRANSPORTATION

Paul D. Wilde, Ph.D., P.E.
Federal Aviation Administration, USA, paul.wilde@faa.gov

The Federal Aviation Administration (FAA) regulates US commercial launch and re-entry operations to the extent necessary "to ensure compliance with international obligations of the US and to protect public health and safety, safety of property, and national security and foreign policy interests of the United States" under 51 USC §50901. The FAA recently developed a comprehensive Notice of Proposed Rulemaking (NPRM) to streamline and consolidate its regulations that govern U.S. launch and re-entry licensing. This paper will describe one of the most innovative and important elements of the NPRM: the use of consequence criteria to determine if a Flight Safety System (FSS) is necessary and when a flight abort must be implemented to protect public safety. The proposal would replace the one-size-fits-all approach in current regulations for Expendable Launch Vehicles (ELVs), which requires a highly reliable/tested FSS to prevent hazards from reaching protected areas during the flight of any guided launch vehicle. The proposal would also replace the process-based hazard control approach currently applied to Reusable Launch Vehicles (RLVs) in favor of a more quantitative and explicit criteria based on Conditional Expected Casualties (CEC). Unlike the current collective risk criterion applied to ELVs and RLVs based on Expected Casualties (EC), which factors in the probability that a dangerous event will occur, a CEC analysis reveals the expected outcome assuming a dangerous event will occur. This paper will explain the relationships between risks and consequences in general, and more specifics that distinguish the current EC and proposed CEC metrics. This paper will include an explanation of issues encountered with the current regulations, as well as the rationale for the proposed solution, including specific thresholds proposed to ensure that launch and re-entry operations pose no more threat to the public than the overflight of conventional aircraft. This paper will explain how the FAA proposes to use CEC analyses to determine the need for flight abort with a reliable FSS as a hazard control strategy, to set reliability standards for any required FSS, and inform when to initiate a flight abort, whether the vehicle is reusable or expendable. The FAA estimated that the proposed approach would save the US commercial space transportation industry millions dollars over five years, while maintaining the high level of public safety achieved under the current regulations.

I. INTRODUCTION

In May 2018, the President of the United States issued Space Policy Directive-2 that charged the Department of Transportation with revising regulations to require a single license for all types of commercial space flight operations and replace prescriptive requirements with performance-based regulations.[1] In April 2019, the FAA published a formal Notice of Proposed Rulemaking (NPRM) consistent with President Trump's Space Policy Directive-2.[2] The NPRM is intended to streamline and increase flexibility in the FAA's commercial space launch and re-entry regulations, remove obsolete requirements, and enable a vehicle operator to obtain a license for any commercial launch or re-entry that ensures the protection of the public, property, and the national security and foreign policy interests of the US. Another paper describes the extent of the proposed changes to FAA regulations, addresses the shift to a more performance-based regulatory framework, and discusses the philosophies used to strike a balance between reducing time spent by industry and government on applications and evaluations while maintaining the U.S. government's robust safety protections for public.[3]

The purpose of this paper is to explain, in the simplest terms possible, several of the most innovative aspects of the NPRM; specifically, how the proposed regulations and draft guidelines would address two critical questions:

1. When would a commercial launch/re-entry vehicle need a flight safety system (FSS)?
2. What level of reliability would be necessary for the FSS in various foreseeable circumstances?

This paper builds on the foundation laid in previous papers and provides more explanatory material than the NPRM on the following topics:

- Public risk management fundamentals applied to the governance of commercial space transportation (CST),
- Key definitions used today and proposed for future,
- Key elements of the current approach to establish when an operation must employ an FSS (referred to as the FSS "needs determination"),
- Fundamentals of conditional risk management, including the relationships between various public safety metrics,
- Key elements of the proposed use of conditional risk management (aka consequence analysis more generally), including thresholds to establish when a

FSS or other safety intervention is necessary to prevent a "high consequence" event and generate only a reasonable level of conditional public risk when implemented, and

- A summary of the rationale for the specific threshold values proposed.

II. PUBLIC RISK MANAGEMENT FUNDAMENTALS FOR CST

The fundamentals of public risk management are the same across all industries. Risk management involves a logical and systematic process to identify hazards and control the risk they pose. Hazard identification uses data on the planned performance and foreseeable malfunctions to identify scenarios that could threaten the public.

Risk controls (also known as mitigations) for any scenario must address at least one of three key elements of risk, illustrated in **Fig. 1**: (1) the probability of a dangerous event (such as a rocket crash), (2) the size of the danger area (such as the area destroyed by a rocket crash), and (3) the nature of the public exposure (such as the population density and sheltering provided in an area where a rocket could crash). Thus, public risks reflect the possibility of dangerous events that could produce serious public consequences.

Fig. 1: Key Elements of Risk

To illustrate these concepts, consider for example, that the public risk from an intact rocket impact may be controlled by reducing the probability of an intact impact, reducing the area destroyed by the impact (e.g. by ensuring the propellants are dispersed before impact), or by evacuating the public from the area that could be hit. (Note that an intact impact of a launch vehicle with substantial quantities of propellant onboard generally produces an explosion and creates a much larger danger area than purely inert debris impacts.) As a result, there are a number of ways to potentially mitigate public risk, and the level of effort required to demonstrate appropriate risk management is naturally linked to the size and complexity of the system, as well as the nature of the public exposure.

As explained in more detail elsewhere,[4] a Flight Safety System (FSS) is an important means to mitigate public risks from large orbital rocket launches by reducing the danger area (ensuring propellants are dispersed before impact) and reducing the probability of impact in populated areas. In simple terms, a FSS provides a means to terminate flight (e.g. by terminating thrust or by triggering an explosive charge to destruct[5] the vehicle) to prevent the hazardous effects of an errant vehicle from reaching protected areas. As illustrated in **Fig. 2**, a traditional FSS that complies with the FAA's current regulations would consist of an on-board flight termination system (FTS), a ground-based command and control system, and tracking and telemetry systems. Historically, the flight safety crew monitoring the trajectory and health of a vehicle would send a command to destruct the vehicle if the vehicle crossed any flight safety limit line (as defined in §417.213[6] and discussed below) and thus posed a potential threat to a protected area. While this method of flight abort through ordnance is conventional, the FAA currently does not require an FSS to be destructive, e.g. thrust termination may be acceptable.

Under the current regulations, an FSS must include an ability to track the vehicle trajectory and terminate the flight if the vehicle experiences a malfunction that violates pre-defined mission rules. The FAA currently requires that any vehicle that employs an FSS must use tracking data sources that are "independent of one another, and at least one source must be independent of any vehicle guidance system." In the past, the decision to terminate flight was exclusively made by a human being, referred to here as the Mission Flight Control Officer (MFCO). Whether the decision to terminate flight is made by a MFCO or by an automated (i.e. computer) system, the terminate decision is always based on mission rules (i.e. flight abort criteria), which include "flight safety limits" (also known as destruct lines).

In simple terms, the flight safety limits are lines on a map that designate when the flight safety system should be triggered if the vehicle "tracking icon"[7] crosses them as illustrated in **Fig. 2**. (There are other types of flight safety limits than just those on a map.)

The FAA currently requires (in §417.213) that "a flight safety analysis must identify the location of populated or other protected areas, and *establish flight safety limits that define when a flight safety system must terminate a launch vehicle's flight to prevent the hazardous effects of the resulting debris impacts from*

reaching any populated or other protected area and ensure that the launch satisfies the public risk criteria."

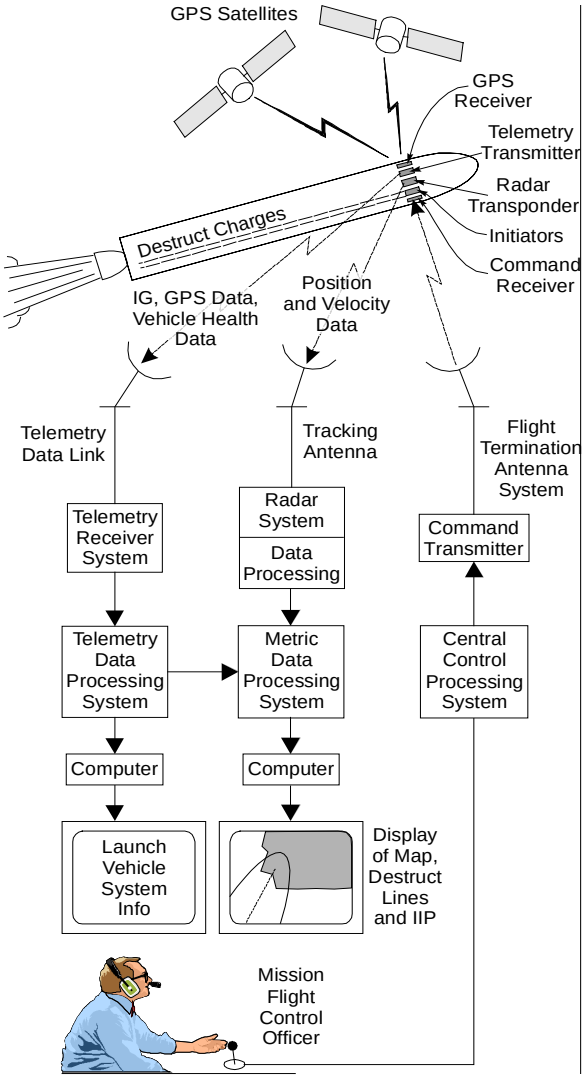

Fig. 2: Traditional Flight Safety System Elements.

One fundamental tenet of risk management is that acceptable risk levels are set with an understanding of the consequences of a hazard and the likelihood of its occurrence. Of course, no serious public consequences from launch or re-entry are truly acceptable, in that no responsible authority would regard such an event as routine or permissible. The FAA seeks to maintain a level of public safety where adverse public consequences remain rare events by enforcing well-defined regulatory risk tolerability criteria supported by multiple lines of logic.[8,9] While the unmitigated consequences of CST hazards can be substantial (e.g. multiple casualties and millions of dollars in damages would be the expected outcome if a large launch or re-entry vehicle crashed on a major city as explained in more detail below[10, 11]), the acceptable risk levels contained in FAA/AST regulations are only a small fraction of the "normal background risk…accepted in the course of normal day-to-day activities."[12] For example, AST's risk limits equate to less than 1% of the annual risk accepted by US pedestrians on an individual and collective basis. The risk criteria set by AST in the commercial space regulations for licensed operations are the same for each mission. These limits were set as a means to manage the risk for current and expected future operations, consistent with the goal that adverse public events remain rare. AST will periodically re-evaluate the risk criteria to account for the frequency of CST activities; the demonstrated safety record and benefits provided; technological capabilities and maturity of the industry; risks tolerated in other industries, and common perceptions of CST risks.[13]

No US space launch has created a public casualty. FAA/AST seeks to maintain a level of public safety where adverse public consequences remain rare events. AST enforces public safety requirements that were initially developed and implemented by the US Air Force and NASA. Building upon this experience and approach, the FAA has promulgated and implemented the current set of public safety regulations that include specific operating requirements, specific safety requirements for critical systems, and the application of a public risk management process that uses quantitative analyses. A primary purpose of the public risk management process applied to launch and re-entry is to facilitate informed decisions regarding the operating parameters and vehicle design features that are necessary to limit the predicted public risks to pre-defined criteria. AST uses a *risk informed* process to systematically identify, reduce, monitor, and ensure acceptable public risks. Compliance with the applicable regulations constitutes what is "necessary" to protect the public during CST in general.

III. IMPORTANT DEFINITIONS AND CONTEXT

Current

Several formal definitions help facilitate an understanding of the FAA's public safety criteria, including those central to traditional risks and conditional risk criteria.

Risk is a metric that accounts for both consequence and probability of a hazard over a specified interval of exposure. The total risk accounts for all possible outcomes and can be computed as the product of the probability of each event and its consequence.

Individual risk expresses the risk to a single person. A common individual risk is the annual risk of a person being killed by lightning worldwide, which can be estimated as the average number of people killed by lightning per year divided by the total population of the world. United States Air Force Space Command Manual (AFSPCMAN) 91-710[14] provides a formal definition of individual risk): "Individual risk is the risk that any single

person will suffer a consequence. Unless otherwise noted, individual risk is expressed as the probability that any individual will become a casualty from a given hazard (P_C) at a specific location and event."

A casualty is someone that suffers a serious injury or worse, including death. A launch or re-entry risk analysis computes the maximum individual risk as the highest probability of casualty for any individual as a result of the launch or re-entry.

Collective risk is the risk of an adverse outcome among a group of individuals, often expressed in terms of expected values: the average (i.e., mean) consequences predicted to occur as a result of a launch or re-entry if the launch or re-entry were to be repeated many times. For example, the collective risk of fatality posed by lightning on an annual basis is the average number of people killed by lightning each year (i.e. Expected Fatalities, E_F). Note that a collective risk, such as the expected number of casualties, is *not* a probability (since it could exceed one) as described and defined below.

Proposed

In the FAA's proposed parlance, a "flight abort" means the process to limit or restrict the hazards to public health and safety and the safety of property presented by a launch vehicle or re-entry vehicle, including any payload, while in flight by initiating and accomplishing a controlled ending to vehicle flight. Under the NPRM, a flight abort would be required as a hazard control strategy for a phase of flight that is shown by a consequence analysis to potentially have significant public safety impacts (as explained in some detail below) without flight abort or another safeguard. Otherwise, the NPRM would allow an operator to bypass the traditional FSS-centric hazard control strategy and instead use alternative strategies: e.g. where a launch vehicle that does not have sufficient energy for any hazards associated with its flight to reach the public or critical assets (physical containment); given wind-weighting for an unguided suborbital launch vehicle[15]; or using a flight hazard analysis.[16] Irrespective of the hazard control strategy used, the proposal would require an operator to conduct flight safety analyses as necessary to demonstrate that a launch or re-entry meets the quantitative public safety criteria for debris, far-field overpressure, and toxic hazards. (Other hazards such as those from nuclear power sources would be addressed on a case-by-case basis.) The NPRM would continue the public risk tolerability criteria already in place under 14 CFR 417.107(b), with a couple of exceptions as described in the NPRM. The NPRM would add a quantitative criterion to protect against the loss of functionality of an asset essential to the national interests of the United States. Critical assets would be defined and identified as discussed below.

The proposal includes new or updated formal definitions for the following terms.

"Critical asset" would mean an asset that is essential to the national interests of the United States. Critical assets include property, facilities, or infrastructure necessary to maintain national defense, or assured access to space for national priority missions. Critical assets would also include certain military, intelligence, and civil payloads, including essential infrastructure when directly supporting the payload at the launch site. Under this proposal, the FAA anticipates that it would work with relevant authorities, including licensed launch or re-entry site operators or Federal property owner, to identify each "critical asset" and its potential vulnerability to launch and re-entry hazards.

"Expected Casualty" would be defined as the mean number of casualties predicted to occur per flight operation if the operation were repeated many times. The proposal clarifies in § 450.101 that the operator may initiate the flight of a launch vehicle only if all risks to the public satisfy the criteria. This means a debris risk analysis must demonstrate compliance with public safety criteria either (1) prior to the day of the operation, accounting for all foreseeable conditions within the flight commit criteria; or (2) during the countdown using the best available input data.

In the past, the FAA defined "public safety," but the NPRM included a proposed definition of public for the first time. "Public" would mean, for a particular licensed or permitted launch or re-entry, people and property that are not involved in supporting the launch or re-entry and includes those people and property that may be located within the launch or re-entry site, such as visitors, individuals providing goods or services not related to launch or re-entry processing or flight, and any other operator and its personnel.

IV. CURRENT FLIGHT SAFETY SYSTEM NEED

As alluded to in the previous section, and explained further in this section, the main purposes of a FSS are to (1) prevent high consequence events as a result of launch/re-entry vehicle failures, and (2) ensure that each CST operation satisfies the public risk criteria. However, the current regulations for ELVs and RLVs use starkly different approaches to establish the need for a FSS.

Current Regulations for ELVs

For Expendable Launch Vehicles (ELVs), the current FAA regulation in §417.107(a) requires a launch operator to employ a FSS if either (1) any hazard from a launch vehicle, vehicle component, or payload can reach any protected area at any time during flight; or (2) a failure "would have a high consequence to the public" in the vicinity of the launch site, and (3) "if the absence of a flight safety system would significantly increase the

accumulated risk from debris impacts" in the downrange area.

As with any hazardous operation, full hazard containment is the preferred approach during a launch or re-entry. However, physical containment for a commercial space transportation vehicle is rarely possible. Setting aside potential toxic and explosive hazards for a moment, just the amount of kinetic energy required to reach Earth orbit generally means that some hazard from an orbital launch vehicle (e.g. the potential for a debris impact) can reach a populated area at some time during flight. Thus, a FSS is practically always necessary for an orbital ELV to comply with §417.107(a), at least in the launch area, because without a FSS some hazardous debris impact *could* reach the public in the launch area. Hence, the high energy and complex nature of launch and re-entry, particularly for orbital operations, means that the protection of public safety generally involves "risk management."

Furthermore, a FSS is typically necessary to ensure that an orbital launch satisfies the public risk criteria given (1) the relatively high probability of failure for ELVs, particularly for new ELVs compared to certified aircraft,[17,18] and (2) the potential for a high consequence event given a failure, especially during the first stage of flight when large quantities of propellant are onboard. The demonstrated flight experience of even the most reliable ELVs to date, such as the Delta II, reveal failure probabilities on the order of 1%, and the demonstrated flight history shows that new vehicles developed by experienced manufacturers have a POF near 0.3 for initial launches. New ELVs from inexperienced developers have demonstrated failure probabilities about twice high. In contrast, certified commercial transport aircraft have demonstrated accident rates on the order to one in ten-million per flight, roughly five orders of magnitude lower than the most reliable ELVs.

Thus, public safety for large orbital launch vehicles has traditionally been protected with the use of a highly reliable FSS and quantitative risk analysis (QRA) to ensure any "residual risks" are acceptable. The term residual risk refers here to public risk from a launch or re-entry that is not mitigated by a FSS.

Another example of a residual public risk from ELV launches involves downrange overflight of populated areas. For example, launches to the International Space Station (ISS) from Cape Canaveral Air Force Station, or from the Guiana Space Center (near Kourou, French Guiana) typically overfly portions of Europe while the upper-stage is thrusting prior to orbital insertion.[19] A failure during downrange overflight, such as a thrust termination or an on-trajectory explosion, would result in debris impacts over a large area and could produce debris impacts in populated areas. During downrange overflight or large landmasses, the activation of a FSS cannot completely prevent the possibility of debris impacts in populated areas. Thus, downrange overflight usually involves a significant residual risk to the public, and in some cases, activation of a FSS could increase the risks.

There are several reasons that the public risks from downrange overflight are often below the acceptable risk criteria, which AST applies equally to foreign and domestic populations. First, the probability of a failure that could produce debris impacts in populated areas is often very low because downrange overflight usually involves a short dwell time of the Instantaneous Impact Point (IIP) over populated areas; usually there is only a period of a few seconds where a failure could produce debris impacts in a populated area during downrange flight because the IIP moves very rapidly as the vehicle approaches orbital insertion. Second, the lower stages of the vehicle are usually jettisoned into the ocean long before the IIP reaches any populated area during downrange overflight. A failure of an upper-stage as the vehicle approaches orbital insertion generally produces much smaller danger areas (more often called casualty areas) compared to failures earlier in lower-stage flight because (1) the inert mass associated with an upper-stage is generally much lower than a lower-stage, (2) propellants often disperse naturally following such high speed and high altitude break-ups, and (3) the inert debris may be reduced by ablation following a failure where the vehicle speed exceeds Mach 10.

The foregoing paragraph explains why activation of a FSS during downrange overflight may be unnecessary to protect public safety, and why the FAA only requires and ELV to be equipped with a FSS during downrange overflight "if the absence of a flight safety system would significantly increase the accumulated risk from debris impacts." For example, this key regulation (in §417.107) generally means that a FSS, or an alternative mitigation, is necessary to prevent a vehicle or payload (e.g. a capsule) with full propellant tanks from surviving to impact, and thus producing a relatively large danger area due to the ensuing explosion. A specific example is that SpaceX designed the thermal protection system of the Dragon capsule so that a launch failure during downrange overflight would result in break-up and demise, and thus mitigate the risk from the potential for the capsule to survive intact to impact.[20]

Current Regulations for RLVs

The FAA's current regulation, in § 431.43(a)(5), explicitly links the need for initiation of a FSS to the quantitative pubic risk criteria (i.e. limits on collective and individual risks): an applicant must submit procedures "*for initiation of a flight safety system that safely aborts the launch of an RLV if the vehicle is not operating within approved mission parameters and the vehicle poses risk to public health and safety and the safety of property in excess of acceptable flight risk as*

defined in § 431.35." The current RLV regulation also contains a limit on the conditional risk posed by an "unproven RLV;" 431.43(d) states that "*any unproven RLV may only be operated so that during any portion of flight…the expected average number of casualties to members of the public does not exceed 1E-4* ***given a probability of vehicle failure equal to 1***." The preamble for Part 431[21] explained the intent of this section: "when failure consequences may be too great to be tolerated then population overflight would be barred," and "because unproven vehicles have an unknown or uncertain failure rate, *the FAA considers it reasonable to ensure that risk is most effectively mitigated by controlling the consequences of a failure*."

Summary of Current Regulatory Approaches

Although both the current ELV and RLV regulations relevant to FSS needs determination include limits on the risks and consequences of reasonably foreseeable failures, there are stark differences in the substance and style of these current regulations. In the case of ELVs, the consequence limit is qualitative and effectively moot due to the overriding requirement for a highly reliable/tested FSS (at least in the launch area) to prevent hazards from reaching protected areas during the flight of any guided vehicle. To date, public safety for all orbital CST vehicles has been protected with the use of a highly reliable/tested FSS and quantitative risk analyses (QRAs) to ensure that any "residual risks" are acceptable based on compliance with numerous specific requirements in Part 417 on the nature of the FSS and the QRA. In contrast to the much more explicit and relatively prescriptive regulations for ELV launch safety, the FAA's current RLV regulations are process based and devoid of any specific requirements on the nature of the FSS and the QRA. However, the current RLV regulations includes an explicit quantitative limit on conditional risks, but only for an "unproven" RLV, which was not formally defined. Although the process-based approach in Part 431 has protected public safety for several suborbital RLVs and RV reentries, no CST launch has reached orbit to date under the current RLV regulations.

V. CONDITIONAL RISK MANAGEMENT

As explained below, the NPRM proposed to treat ELVs and RLVs equally with respect to the need for a FSS, by removing the one-size fits all approach applied to ELVs by the current regulations and replacing the process-based hazard control approach currently applied to RLVs in favour of a more quantitative and explicit criteria based on Conditional Expected Casualties (CEC).

Fundamentals of Conditional Risk Management

Before delving into the specifics of the proposed approach to establish the need for a FSS, it is helpful to review the fundamentals of conditional risk management, aka consequence analysis, and understand the essential difference between risk and consequence (aka conditional risk).

As explained above, public risks reflect the probability of dangerous events that could produce negative public consequences, such as casualties or loss of critical asset functionality. Whereas the risk from a launch or re-entry accident is quantified as the product of probability of the accident and the average (i.e. mean) consequence of the accident, a conditional risk analysis examines the outcome of an event independent of the probability of that event. Thus, consequence analysis is central to and embedded in risk analysis. Mathematically, the only difference between risk and consequence analyses is that a consequence analysis assumes that a reasonably foreseeable event occurs: the probability of the event, e.g. a vehicle failure of some kind, is assumed to be one. An example of a conditional risk limit is given in § 431.43(d) as described in the previous section. The NPRM proposed a more precisely defined conditional risk limit, explained in precise mathematical terms elsewhere.[22]

An examination of empirical data on the outcome of commercial transport aircraft departures helps illustrate the conceptual difference between risk and consequence. Empirical data for the 30-year period between 1984 and 2013, showed that the probability of an airline accident was about three in ten-million (2.9E-7) per departure: in other words, there were an average of about three airline accidents for every ten million departures in that period. The same empirical data set showed, as listed in **Table 1**, that an average airline accident between 1984 and 2013 produced about one (actually 0.9) ground fatality; in other words, an US airline accident had a mean consequence of one fatality for people on the ground in that 30-year period.

Table 1. Ground Fatalities per Fatal Accident Based on 30 Years of NTSB Data (1984 through 2013)

AVIATION CATEGORY	GROUND FATALITIES PER ACCIDENT	95 PERCENTILE UPPER BOUND
All US Civil (Part 91, 121, 135)	0.02	0.06
Airlines (Part 121)	0.91	3.85
Scheduled (Part 135)	0.02	0.14
General Aviation (Part 91)	0.01	0.03

Therefore, the collective risk to the public from an airline departure was empirically demonstrated to be about 2.6E-7 expected fatalities between 1984 and 2013 (i.e. 2.9E-7 probability of an accident per departure multiplied by 0.9 fatality per accident). In simple terms,

empirical data showed that about three ground fatalities resulted on average from every ten million airline departures in the 30-year period from 1984 to 2013. The data in **Table 1** also shows that the average consequence of a General Aviation (GA) fatal accident (i.e. where someone on-board dies) is 0.03 casualties on the ground; in other words after 100 GA accidents, on average three people on the ground are seriously injured or killed. Thus, the conditional risk for ground dwellers from a fatal GA accident is 0.03 CEC.

Previous work done by the Range Commanders Council (RCC) Risk Committee outlined the steps for a conditional risk management approach to ensure that any "safety intervention," such as activation of a traditional FSS or a contingency abort to an alternative landing site for an RLV, will (1) be implemented to prevent "high consequence" events, and (2) produce reasonable conditional risks given implementation. In addition to the RCC 321 Supplement, a publicly available paper[23] described a systematic and detailed QRA approach to manage conditional risks associated with safety interventions and supplement the traditional risk management standards in RCC 321.[24]

Example - Risks Posed by the *Columbia* Accident

The public risks posed by the *Columbia* accident provide a good example to explain the relationship between various conditional risk metrics (e.g. CEC, the probability of one or more casualties, and a "risk profile" *given an accident*).

Shortly after the breakup of *Columbia* over Texas, dramatic images of the Orbiter debris surfaced: an intact spherical tank in a parking lot, an obliterated office rooftop, mangled metal along roadsides, charred chunks of debris in fields. These images, combined with the large number of debris fragments recovered (~90,000 pieces with an average weight near one pound), compelled some to proclaim it was a "miracle" that no one on the ground was hurt.[25] The *Columbia* Accident Investigation Board (CAIB) commissioned a study to determine if the lack of reported injuries on the ground was a predictable outcome or simply exceptionally good fortune.

The formal risk analysis sponsored by the CAIB found that the lack of general-public casualties from the *Columbia* break-up was in fact the statistically expected outcome. The CAIB chose to quantify and explain the conditional collective risk to the public (given the accident) occurred using the probability of one or more casualties, a metric that was thought to be more readily understood compared to the FAA's current regulatory metrics (i.e. expected casualties, conditional or otherwise). The CAIB reported that the probability of one or more casualties was near 0.2 (one in five) *given the accident occurred when and where it occurred.* The CAIB analysis also showed that the probability of two or more casualties was about ten times lower than the probability of one or more casualties, as shown in **Fig. 3**.

The small relative likelihood of multiple ground casualties is typical for a re-entry that leads to debris impacts on areas with low population densities; *Columbia's* debris fell on an area with an average of about 85 inhabitants per square mile. An Aerospace Corp. study found that multiple ground casualties due to a re-entry is "very unlikely" unless the debris generated include objects with a dimension of at least 25 feet.[26] The Aerospace study predicted that a re-entry would likely result in multiple ground casualties if the debris impacted in an area with a population density in the highest one percentile of the world population.

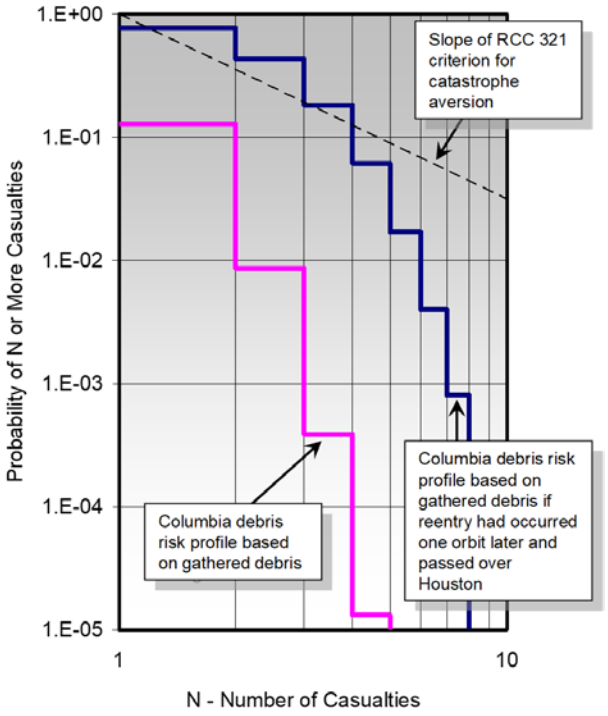

Fig. 3: Sample Risk Profiles for Columbia Accident

The probability of one or more casualties given an event is a less complicated metric for conditional collective risk than CEC. However, these two conditional risk metrics are closely related, and nearly equal for typical re-entry operations. The CAIB study found that the CEC was generally equal to the conditional probability of one or more casualties to one significant figure as shown in **Table 2**. In all cases, the CEC value is equal to the conditional probability of at least one casualty given the event multiplied by one casualty, plus the conditional probability of at least two casualties given the event multiplied by two casualties, plus the conditional probability of three casualties given the event times three casualties, etc.

Fig. 3 illustrates the graphical relationships between CEC and the probability of one or more casualties given an event that can be seen in a conditional casualty "risk profile." A casualty risk profile (conditional or not) is an even more comprehensive expression of collective risk than expected casualties, or the probability of one or more casualties, because it reveals the relative probability of various numbers of casualties that could occur (among other things). Specifically, the abscissa of a casualty risk profile is the number of casualties (K) and the ordinate is the probability of K *or more casualties*. Thus, a risk profile provides more information about the nature of the risks posed by an event than mean risk values, such as the EC. The risk profile is particularly useful for making an MPL estimate because it reveals the largest predicted consequence (i.e. monetary loss) above a specific probability level.[27] As previously mentioned, the EC is defined as the mean number of casualties predicted to result from a given hazard (e.g. debris) from a launch or re-entry operation. The expected number of casualties (EC) due to the impact from a single piece of debris or from a collection of fragments can be computed from the area under the risk profile from 1 to X_{MAX}. The proof of this follows: the risk profile is discrete and is defined for each value of k as the sum of all of the probabilities of exactly p(k) for $k < X_{MAX}$ (the maximum number of casualties predicted for any outcome) as shown below.

$$P(\geq 1) = p(1) + p(2) + p(3) + \ldots$$
$$P(\geq 2) = p(2) + p(3) + \ldots$$
$$P(\geq 3) = p(3) + \ldots$$

$$\sum_{k=1}^{n_{max}} P(\geq k) = p(1) + 2p(2) + 3p(3) + \ldots + n_{max}\,p(n_{max}) = \sum_{k=1}^{n_{max}} k \times p(k)$$

which is the classical definition of E_C, *i.e.* $E_C = \sum_{k=1}^{n_{max}} k \times p(k)$

As a mean value, the last equation for the EC (aka E_C) is readily recognized. The equivalent derivation for equating expected values (casualties or fatalities) with the area under the continuous distribution form of a frequency (say per year) versus consequence (F-N) curve can be found elsewhere.[28]

Debris Case	% of Total Orbiter Weight	E_C	P[≥1 casualty]
Recovered Debris	38%	0.14	0.13
60% of total wt. survived	60%	0.21	0.19
80% of total wt. survived	80%	0.29	0.25
100% of total wt. survived	100%	0.36	0.30

Table 2. Ground Conditional Risk Results for *Columbia*

Fig. 3 shows two sample *conditional* risk profiles based on the *Columbia* accident: plots of the probability of exceeding various numbers of casualties predicted to result *given the break-up of the Orbiter*. The two conditional risk profiles correspond to two different events: the lower one (in pink) was computed given where and when the accident actually occurred (using the best available evidence of the debris recovered, etc.), and the other (in dark blue) corresponds to a hypothetical event that could have occurred if the *Columbia* re-entry was delayed by one orbit and the Orbiter broke up at the same altitude such that the debris field fell on Houston. In the case of the dark blue risk profile, the CAIB study computed that the probability of one or more casualties was in the range of 0.89 to 0.98, depending on the amount of debris that survived, with one or two ground casualties predicted as the most likely outcome given a break-up that produced debris impacts on Houston. Notice that the dark blue risk profile is not nearly as steep as the actual Columbia accident scenario (in pink): given a large number of re-entry debris impacts on a major city, the probability of three or more casualties is within an order of magnitude of the probability of one or more casualties.

VI. KEY PROPOSED CEC REGULATIONS

This section describes the FAA's proposed approach to use conditional risks to evaluate the need to implement mitigation measures, such as flight abort, based on quantitative assessments and thresholds that are consistent with past precedents, current U.S. Government consensus standards, and formal comments provided by a recent Advisory Rulemaking Committee (ARC).

Need for Mitigation Measures

The FAA proposed to use the CEC metric for the consequence from reasonably foreseeable failures as an appropriate means to assess the need for prudent mitigations (such as flight abort) of risks to public safety. The FAA proposed to use traditional risk analysis as an important tool to ensure public safety also. Both traditional and conditional risk metrics can be useful to inform the level of rigor necessary in various safety analyses and to establish appropriate hazard control strategies, including flight abort and flight hazard analyses.

Separating the two (conditional and traditional risks) can facilitate a better understanding of precisely where the various types of safety analyses and hazard mitigation strategies are important. Specifically, the use of both conditional and traditional risk analyses can help identify where the uncertainties in an analysis make a difference to the decisions regarding hazard controls and verifications. For example, if an analysis shows that compliance with the traditional risk requirements is strongly dependent on the allocation of failure probability to failure modes or as a function of time, then

the level of rigor of the system safety process and/or the basis to establish a statistically valid allocation of the failure probability are important. On the other hand, if a launch or re-entry operation would clearly meet the risk criteria regardless of the type of foreseeable vehicle response modes or failure times, then a lower fidelity system safety program or statistical analysis could be acceptable. As another example, if compliance with the risk requirements depends on the consequence of a given vehicle response mode being low, then the methods to establish the low consequence of that VRM must be well verified and a high fidelity analysis may be necessary.

Unlike EC that factors in the probability of occurrence for each reasonably foreseeable dangerous event, CEC determines the expected casualties assuming the dangerous event will occur. Thus, a CEC analysis can be relatively free from the large uncertainties typically associated with the failure probabilities for launch or re-entry operations. (The uncertainties in the failure probability are typically are the largest contributor to uncertainty in public risk estimates; the epistemic nature failure probability uncertainties renders especially difficult to assess.[29]) However, a challenge has been to identify the best conditional risk metric: to specify precisely what type of event should be assumed to have a probability of one and if the outcome of that event should be an average, or at a 95% confidence level, etc. A previous paper described the CEC metric that the FAA proposes to help ensure public safety during launch and re-entry operations precise mathematical terms,[30] which is not the focus of this paper.

In the simplest terms, the NPRM proposed to require a consequence analysis with threshold values explained below to replace key aspects of the "one-size-fits-all approach" embedded in current FAA regulations, as discussed above. The proposed regulations would use consequence criteria to protect the public from unlikely, but catastrophic events. For example, proposed §450.101(c) would require that operators quantify the consequence of a catastrophic event by calculating CEC for each one-second period of flight prior to orbital insertion. More specifically, the FAA proposed to use that CEC metric to determine:

1. The need for flight abort as a hazard control strategy or other safeguards agreed to by the Administrator, and
2. The reliability standards for any required FSS.

In essence, the NPRM proposed to replace the one-size fits all approaches in the current regulations by setting FSS design reliability and verification requirements based on quantitative conditional risk thresholds. Specifically, the NPRM proposed to require in § 450.145(a) that the operator must use a flight safety system, or other safeguards agreed to by the Administrator, on the vehicle, vehicle component, or payload with the following reliability:

(a) 0.999 at 95% confidence and commensurate design, analysis, and testing (i.e. consistent with the current FSS requirements in §§ 417.303 and 417.309) only if the CEC without a FSS is 0.01 (1E-2) or greater, and
(b) 0.975 at 95 percent confidence with commensurate design, analysis, and testing requirements necessary to verify this reliability if the CEC is between 0.01 and 0.001 (1E-3).

If the CEC for a given CST operation is less than 0.001, and the individual and collective risk criteria are met, then the NPRM would not require a FSS. Thus, under the NPRM a Part 417 compliant FSS would only be required for any phase of flight in which the CEC exceeds 0.01 (1E-2). This threshold is consistent with past precedent, FAA waivers, and U.S. Government consensus standards as explained below.

Proposed § 450.101(c) would apply to all phases of flight during launch and re-entry, unless otherwise agreed to by the FAA based on the demonstrated reliability of the launch or re-entry vehicle during that phase of flight. For example, the flight of a certificated aircraft that is carrying a rocket to a drop point would likely not need an FSS, even though the CEC could be above the threshold, because the aircraft would have a high demonstrated reliability (such as the L-1011 that carries Pegasus).

Rationale for the Proposed CEC Thresholds

As explained in this section, a conditional risk threshold of 0.01 is consistent with a key explosive safety threshold used by many parts of the USG, industry and USG consensus standards, and FAA waivers for relatively recent CST operations.

Other government entities use a consequence threshold of 0.01 to protect against explosive hazards. The Department of Defense, NASA, and the FAA use quantity-distance limits originally designed to limit conditional individual risk of fatality to 0.01 from inert debris fragment impacts. Specifically, the ubiquitous "quantity-distance" standard define minimum separation distances between potential sources of high speed fragments (propelled by accidental explosions) and areas where the public is exposed to ensure no more than one hazardous fragment impact per 600 sqft, with the assumption that any exposed person has a vulnerable area of 6 sqft. The most recent NASA explosive safety standards do not permit public buildings at closer distances than where hazardous debris impacts (with kinetic energy of 58 ft-lb or greater) exceed 1/600 sqft, corresponding to a consequence limit of no more than 0.01 conditional risk of fatality.[31] The most recent USAF explosive safety also defines a hazardous fragment density in the same way.[32]

This threshold is also rooted in the longstanding and often cited principle that launch and re-entry "to provide

for the public safety, the Ranges, using a Range Safety Program, shall ensure that the launch and flight of launch vehicles and payloads present no greater risk to the general public than that imposed by the over-flight of conventional aircraft."[33] In addition to the USAF, the RCC, an American National Standard[34] and the FAA have identified the public risks posed by conventional aircraft as an important benchmark for the acceptable risks posed by launch vehicles. Like commercial space operations, civil aviation poses an involuntary hazard to the public on the ground. Therefore, the FAA looked to this risk to the public on the ground to derive consequence limits for commercial space activities. The results shown in **Table 1** show that the average consequences on the ground from all fatal civil aviation accidents are 0.06 casualties and 0.02 fatalities. The average ground consequence from a general aviation crash is 0.01 conditional expected fatality (and 0.03 conditional expected casualty) as described above. Given this range of aviation related accident consequences, as well as the significant differences in aviation and space transportation safety paradigms, the uncertainty inherent in casualty consequence predictions for space launch and re-entry missions compared to the empirical data shown in Table 1, and the unique prevailing conditions in commercial space transportation, the proposed threshold appears reasonable. Note that the current collective risk limit used for CST (1E-4 EC) is a half order of magnitude lower than the maximum that could be justified as "*no more dangerous than conventional airplanes flying overhead."*[35]

An acceptable conditional collective risk criterion of 0.01 expected casualties is consistent with recent decisions made to protect public safety during commercial space operations. For example, in assessing the potential public safety impacts associated with debris with ballistic coefficients outside of the impact limit lines for the SpaceX Falcon-9 stage 1 return to launch site as part of the Orbcomm2 mission, the FAA leveraged state-of-the-art techniques to examine the CEC of a failure that could generate debris outside of the impact limit lines. [1] The analysis conducted by the FAA and 45SW/SELR demonstrated that the consequence of events that could produce debris (with ballistic coefficient above 3 psf) outside of the impact limit lines for a small portion of the stage 1 fly back operations (where the concern exists) was below this threshold (0.01 CEC), even with input data corresponding to the worst case weather conditions. Thus, the FAA determined that a waiver to the requirements of § 417.213 (a) and § 417.213 (d) would not jeopardize public health and safety or the safety of property. This waiver implies that a CEC below 0.01 does not constitute a "high consequence" event in the context of §417.107(a), which requires that FSS be employed if a failure "would have a high consequence to the public" in the vicinity of the launch site.[36] Another example, which involved downrange overflight of the Dragon, was described briefly above. Specifically, a safety mitigation was implemented (an intentional weak spot in the thermal protection system), such that a launch failure would not result in CEC above 0.01 due to an intact impact of the capsule.

The use of a consequence metric is consistent with the comments made by the Advisory Rulemaking Committee (CST industry) during the development of the NPRM. The ARC suggested that an FSS with a reliability of 0.999 at 95 percent confidence is appropriate for high consequence, low probability events. The ARC did not identify any threshold values to define "high consequence"; however, the proposal does identify quantitative consequence thresholds in terms of CEC.

VII. SUMMARY AND CONCLUSIONS

In summary, a FSS provides a means to terminate flight (e.g. by terminating thrust or by triggering an explosive charge to destruct the vehicle) to prevent the hazardous effects of an errant vehicle from reaching protected areas by ensuring propellants are dispersed before impact and reducing the probability of impact in populated areas. A FSS of some form has been used to mitigate public risks from all US orbital rocket launches to date. Although the current ELV and RLV regulations relevant to FSS needs determination include limits the risks *and consequences* of reasonably foreseeable failures, there are stark differences in the substance and style of these current regulations. In the case of ELVs, the consequence limit is qualitative, and effectively moot due to the overriding requirement for a highly reliable/tested FSS (at least in the launch area) to prevent hazards from reaching protected areas during the flight of any guided vehicle. In contrast to the much more explicit and relatively prescriptive regulations for ELV launch safety, the FAA's current RLV regulations are process based and devoid of any specific requirements on the nature of the FSS and the QRA necessary to demonstrate compliance with the public risk criteria. However, the current RLV regulations includes an explicit quantitative limit on conditional risks, but only for an "unproven" RLV, which was not formally defined. The process-based approach in Part 431 has successfully protected public safety for several suborbital RLVs and RV reentries, but no CST launch to date has reached orbit under the current RLV regulations.

The NPRM proposed to replace the one-size fits all approaches in the current regulations and treat RLVs and ELVs equally with respect to FSS needs, by setting FSS

design reliability and verification requirements based on quantitative conditional risk thresholds. Specifically, the NPRM proposed to require that a CST operator must use a flight safety system, or other safeguards agreed to by the Administrator, on the vehicle, vehicle component, or payload with the following reliability:

(a) 0.999 at 95% confidence and commensurate design, analysis, and testing (i.e. consistent with the current FSS requirements for ELVs) only if the CEC without a FSS or other approved safeguard, is 0.01 (1E-2) or greater, and
(b) 0.975 at 95 percent confidence with commensurate design, analysis, and testing requirements necessary to verify this reliability if the CEC is between 0.01 and 0.001 (1E-3).

If the CEC for a given CST operation is less than 0.001, and the individual and collective risk criteria are met, then the NPRM would not require a FSS. Thus, under the NPRM a Part 417 compliant FSS would only be required for any phase of flight in which the CEC exceeds 0.01 (1E-2). The FAA estimated that the proposed approach would save the CST industry millions dollars over five years, while maintaining the high level of public safety achieved under the current regulations.

The proposed CEC requirements regarding FSSs would apply to all phases of flight during launch and re-entry, unless otherwise agreed to by the FAA based on the demonstrated reliability of the launch or re-entry vehicle during that phase of flight. For example, the flight of a certificated aircraft that is carrying a rocket to a drop point would likely not need an FSS (such as the case currently with the L-1011 that carries Pegasus).

A conditional risk threshold of 0.01 is consistent with a key explosive safety threshold used by many parts of the USG, industry and USG consensus standards, and FAA waivers for relatively recent CST operations. The key elements of the rationale for specific threshold values proposed:

(a) Third-party casualty consequences of aviation accidents are a reasonable basis for criteria to determine the circumstances that warrant activation of an FSS or other safety intervention.
(b) Equivalent to the USG safety requirements used to protect the public from stored explosives.

[1] *Space Policy Directive-2, Streamlining Regulations on Commercial Use of Space*; May 24, 2018

[2] *Streamlined Launch and Re-entry Licensing Requirements.* 84 FR 72, 15296-15444, 15 April 2019

[3] Monteith W., J. Easterson, and J. Sloan, *Streamlining FAA Commercial Space Transportation Regulations*, 70th IAC, Washington, DC, 21-25 October 2019

[4] Range Commanders Council (RCC) 319-19 Standard, *Flight Termination System Commonality Standard*, 2019.

[5] The FAA formally defined "destruct" in §417.3 as the act of terminating the flight of a launch vehicle flown with a flight safety system in a way that destroys the launch vehicle and *disperses or expends all remaining propellant* and renders remaining energy sources non-propulsive before the launch vehicle or any launch vehicle component or payload impacts the Earth's surface.

[6] *Licensing and Safety Requirements for Launch*; 71 FR 165, August 25, 2006 (see p. 50537)

[7] The FAA formally defined "tracking icon" in §417.3 as the representation of a launch vehicle's instantaneous impact point (IIP), debris footprint, or other vehicle performance metric that is displayed to a flight safety crew during real-time tracking of the launch vehicle's flight.

[8] Wilde P., *Public Risk Criteria and Rationale for Commercial Launch and Re-entry*, 5th IAASS Conference, Versailles, France, October 2011.

[9] The FAA's NPRM does not propose to change the current public risk criteria, which was promulgated five years ago. See 42241 of Federal Register, Vol. 79, No. 139, July 21, 2014

[10] Lin, M. Y. Y., Larson E. W. F., and Collins J. D., *Determination of Debris Risk to the Public Due to the Columbia Breakup During Re-entry*, Appendix D.16 to the Columbia Accident Investigation Board Final Report, Vol. II, pp. 475-506

[11] Wilde P., C. Brinkman, and S. Millard, *FAA Public Risks and Insurance Requirements for Orion's First Entry Flight Test*, 65th IAC, Toronto, 2014 (IAC-14-D6.1.6)

[12] See page 19605 of Federal Register, Vol. 64, No. 76, April 21, 1999.

[13] *Changing the Collective Risk Limits for Launches and Re-entries and Clarifying the Risk Limit Used to Establish Hazard Areas for Ships and Aircraft*; 81 Federal Register 139, p. 47017 20 July 2016

[14] Air Force Space Command, Air Force Space Command Manual 91-710 (AFSPCMAN 91-710), *Range Safety User Requirements*, July 2004 (see paragraph A4.2.2.2.1)

[15] Wilde P.D., *Range Safety Requirements and Methods for Sounding Rocket Launches*, Journal of Space Safety Engineering, Vol 5, Issue 1, 2018, pp. 14-21.

[16] Hazard analysis here refers to a proven engineering discipline that, when applied during system development and throughout the system's operational lifecycle, identifies and mitigates hazards and, in so doing, eliminates or reduces the risks to the public.

[17] Fragola J.R., *Aerospace Failure Data Handbook: A Reference Guide to Understanding and Assessing Risk and Reliability of Aerospace Systems and Spacecraft Design*, Valador, Inc., 2010.

[18] Wilde P, Morse E, Rosati P., Cather C, *Probability of Failure Analysis Standards and Guidelines for Expendable Launch Vehicles*, 6th International Association for the Advancement of Space Safety Conference in Montreal, Canada – May 21-23, 2013

[19] In the NPRM, orbital insertion means the point at which a vehicle achieves a minimum 70-nautical mile (130 km) perigee based on a computation that accounts for drag.

[20] See page 78619 of Federal Register, Vol. 75, No. 233, December 6, 2010.

[21] Federal Register, Vol. 65, No. 182, September 19, 2000, p 56626

[22] Ricketson T., Wilde P., and Larson E.F., *Proposed Flight Abort Criteria to Ensure Public Safety during Commercial Launch and Re-entry Operations*, 10th IAASS Conference, Los Angeles, CA, May 2019.

[23] Wilde P., *Potential Uses of Consequence Analyses for Range Safety*, 8th IAASS Conference, Melbourne, FL, May 2016

[24] Range Commanders Council Risk Committee of the Range Safety Group, *Common Risk Criteria for National Test Ranges*, RCC 321-07, White Sands Missile Range, New Mexico, 2007

[25] "And stunningly, in as much as this was tragic and horrific through a loss of seven very important lives, it is amazing that there were no other collateral damage happened as a result of it. No one else was injured. All of the claims have been very, very minor in dealing with these issues." NASA Administrator Sean O'Keefe, testimony before the United States Senate Committee on Commerce, Science, and Transportation, May 14, 2003.

[26] Patera R., *Managing Risk from Space Object Re-entry*, copyright 2003 by the Aerospace Corp.

[27] Collins J.D., Chrostowski J.D, and Wilde P.D., *Measures and Techniques for Inserting Catastrophe Aversion into the Explosive Safety Risk Management Process*, 32nd US Dept. of Defense Explosives Safety Seminar, Philadelphia, PA, August 2006 (see also ref 8)

[28] Vrijling, J.K. and van Gelder, P.H.A.J.M., *Societal Risk and the Concept of Risk Aversion*, Dept. of Civil Engineering, Delft University of Technology

[29] Wilde P, Duffy J, *How Many Significant Figures Are Useful for Public Risk Estimates?*, 6th IAASS Conference in Montreal, Canada – May 21-23, 2013

[30] See reference 16

[31] NASA-STD-8719.12A, *Safety Standard for Explosives, Propellants, and Pyrotechnics*, – Approved 2018-05-23, p. 63.

[32] Air Force Space Command, Air Force Space Command Manual 91-201, *Explosive Safety Standards - Supplement*, 13 Sept. 2017 (see paragraph 12.22)

[33] Eastern and Western Range 127-1, *Range Safety Requirements*, Oct. 31, 1997

[34] According to ANSI/AIAA S-061-1998, "during the launch and flight phase of commercial space vehicle operations, the safety risk for the general public should be no more hazardous than that caused by other hazardous human activities (e.g., general aviation over flight)."

[35] In 1949, Congress enacted Public Law (PL 81-60), which authorized the Secretary of the Air Force to establish a joint proving ground, which became the present-day Eastern Range. A letter from the Secretary of Defense to the Speaker of the House stated that the location was chosen such that "from a safety standpoint (test flights of missiles) will be no more dangerous than conventional airplanes flying overhead." Although this language is not binding in any way to current decisions made by any federal agency, it does indicate a logical and historical connection between appropriate risk levels for launch/re-entry activities and conventional aircraft. See reference 5 for addition explanation.

[36] *Waiver of Debris Containment Requirements for Launch*. 81 FR 1470 (January 12, 2016), at 1470-1472.