FAA | AST Commercial Space Transportation

Flight Safety Analysis (FSA) Workshop - AST

Federal Aviation Administration

May 28, 2024

Introduction & Questions

The purpose of this workshop is to provide the international community insight into FAA Flight Safety Analysis requirements under Title 14 of the Code of Federal Regulations (14 CFR) § 450

Three Sections:

Day 1: May 28, 2024

- Safety Criteria under Part 450

Day 2: May 30, 2024

- Overview of FSA sections 450.108 to 450.137
- Explanation of § 450.115(c) elements

- **Q&A Session will be held after each section.**
  - Participants should use the Q&A function to ask questions.
  - We will answer as many questions as time allows.
  - Any unanswered questions will be answered after the workshop in a written Q&A document or at a future FSA Office Hours.

Section 1: Safety Criteria under Part 450

Flight Safety Review – Why FSA exists:

At approximately 1930L on May 29, 1947, a Hermes II rocket was launched from LC-33 at White Sands Proving Ground. This rocket caused an international embarrassment that resulted in the first formal, ***independent*** Range Safety program.

The Hermes II missile was intended to be a testbed for ramjet technology. It was a modified V-2 rocket with a winged ramjet upper stage, and was the world's first multi-stage rocket. For this particular test, the ramjet was not active – the test was intended to merely fly the main stage down range, to the North. The missile instead flew up range to the South.

During the flight, a Range Safety Officer (RSO), was present. However, the RSO was a member of the program team, and was even co-located with one of the project scientists. There were no formal flight rules for flight termination. Given the massive deviation from the planned course, the RSO did intend to terminate flight – however, accounts of the incident relate that the project scientist physically restrained the RSO from sending the command. To the program, the data collection from the flight was invaluable.

The result was that the rocket flew so far up range that it crossed the international border into Mexico and impacted the Tepeyac Cemetery outside of Juarez. Happily, no lives were lost. Soldiers were scrambled from Fort Bliss to react to the incident, but when they arrived, dozens of enterprising locals from the Juarez area were already selling parts of the classified program as souvenirs. Upon arriving at the scene, one witness recounts, "*In the pit of the crater, a lone boy was souvenir hunting. He was late. Most of the scrap metal, fused with molten sand and rock, had been carried away by youths who had rushed to the scene. Everybody at the scene was talking at once… one word came out above the babel… Bomba!*"

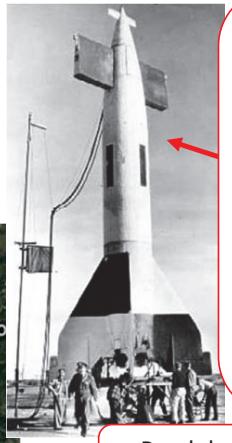
The mishap investigation revealed that the proximate cause of the flight deviation was an inertial guidance system that had been wired backwards.

One of the expatriated German scientists involved was later quoted, "*We were the first German unit to not only infiltrate the United States, but to attack Mexico from US soil!*" The Army was significantly less amused - they not only lost the mission and some sensitive hardware, but they also needed to apologize publicly to Mexico and pay for clean up and for damages. Thereafter, stricter Range Safety policies were implemented. These policies became the precursors to Range Safety across the US and are the foundation still today.

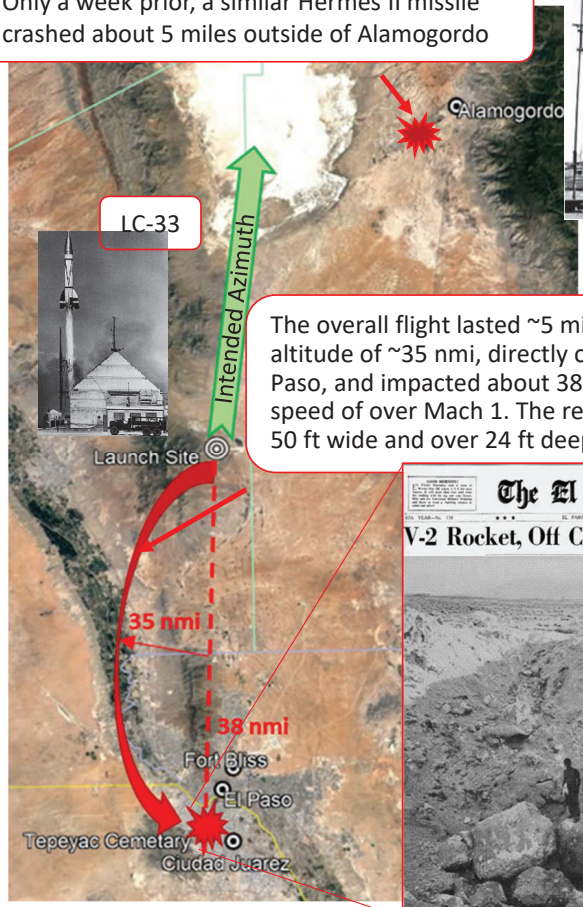
Major Lessons Learned:

Safety needs to be independent.
Flight limits need to be well defined.

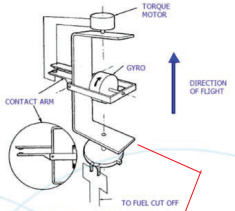
Only a week prior, a similar Hermes II missile crashed about 5 miles outside of Alamogordo



The Hermes II was 51.50 feet (15.70 meters) tall. The tail fins had a span of 17.75 feet (5.41 meters), and the second stage wing span was 15.26 feet (4.65 meters). The rocket had a gross weight of 31,750 Pounds (14,400 kilograms). The liquid oxygen/alcohol-fueled engine produced 60,000 pounds of thrust (267 kilonewtons).



Pendulous Integrating Gyro Assembly (PIGA): the INS likely utilized 3 of these



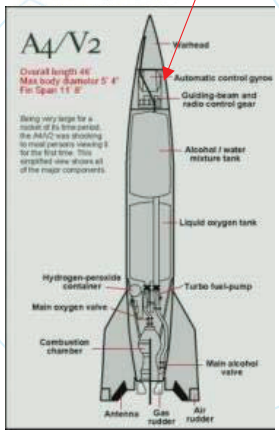
The overall flight lasted ~5 minutes, reached an altitude of ~35 nmi, directly overflew parts of El Paso, and impacted about 38 nmi up-range at a speed of over Mach 1. The result was a crater over 50 ft wide and over 24 ft deep.


The El Paso Times

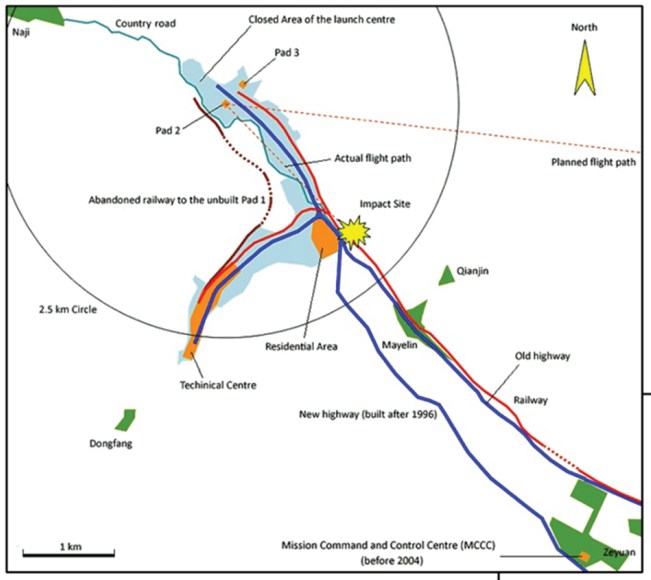
V-2 Rocket, Off Course, Falls Near Juarez

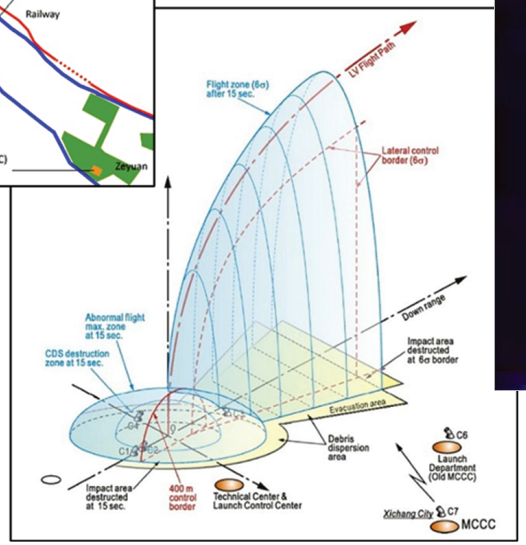
Giant Missile Lands On Rocky Knoll, Explodes

V-2 Rocket Too Close For Comfort



Flight Safety Review – Why FSA exists (Long March Intelsat):





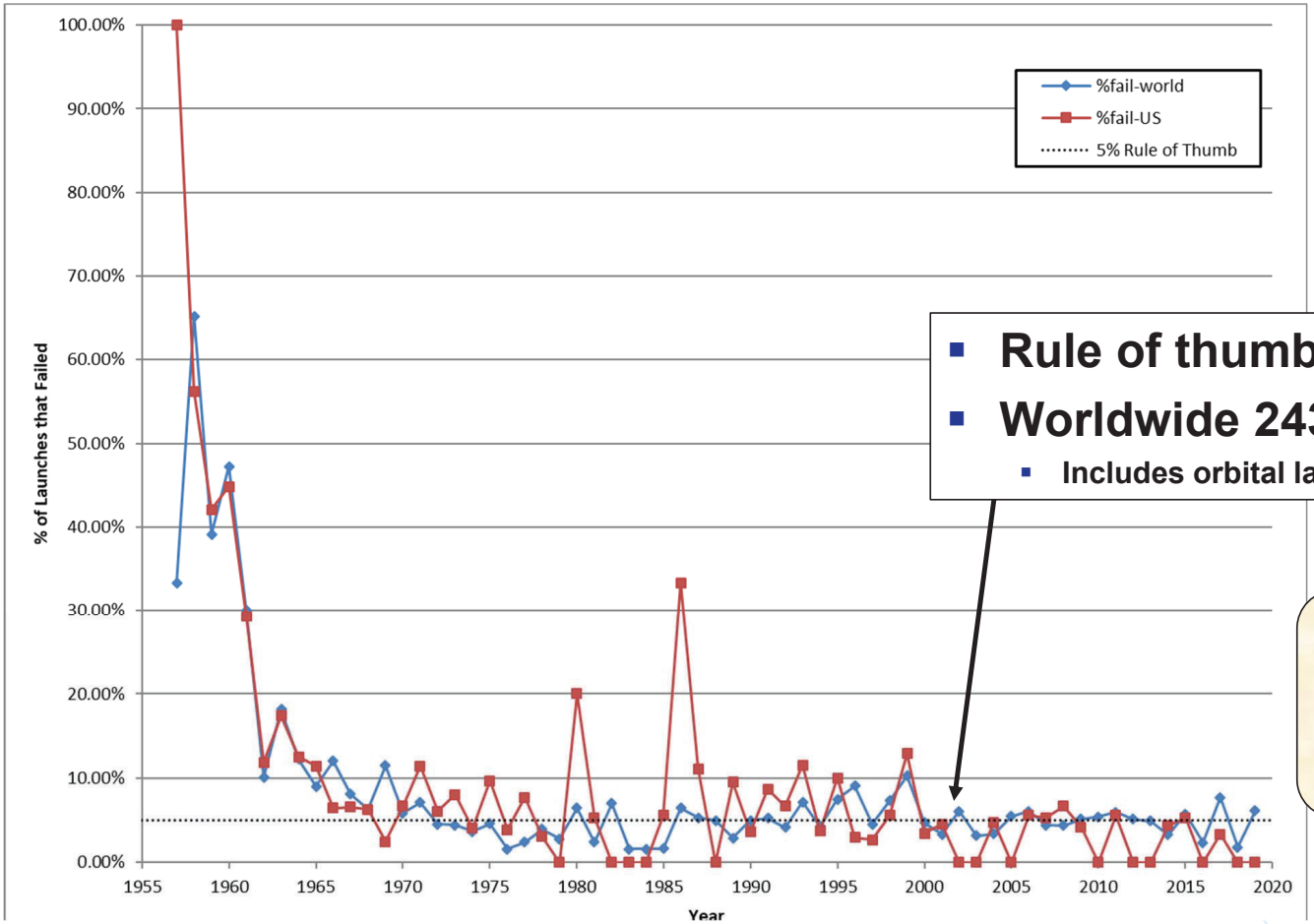
Additional Public references:

- https://www.thespacereview.com/article/2323/1 (source of pictures shown here)
- https://www.airspacemag.com/history-of-flight/disaster-at-xichang-2873673/
- https://www.youtube.com/watch?v=8_EnrVf9u8s&feature=youtu.be

Flight Safety Review – Why FSA exists (Titan Video):

Why FSA exists:

The Brutal Statistics



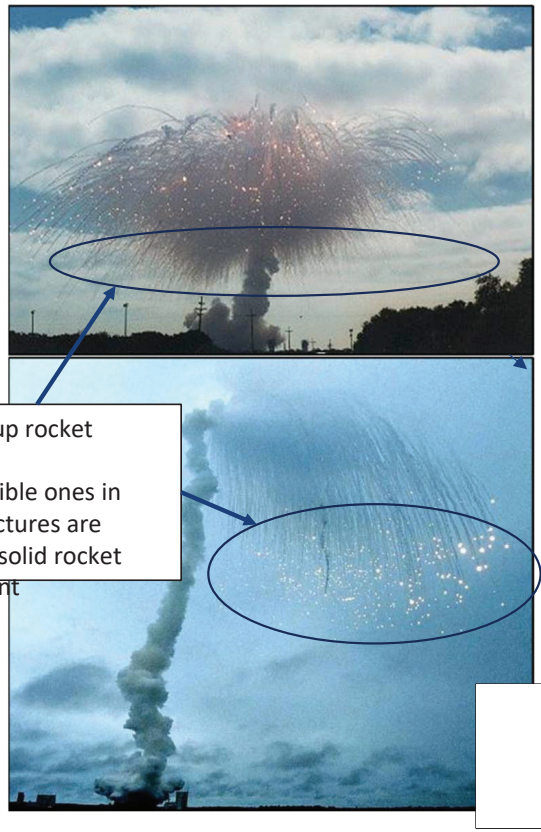
- **Rule of thumb: ~1 out of 20 fail (5%)**
- **Worldwide 243 failures/5269 launches (4.6%)**
  - **Includes orbital launch only from 1 Jan 75 – 31 Dec 19**

Note: These are for orbital space launch. Statistics differ based on the range application (missile, sounding rocket, balloon, UAV, etc).

Flight Safety Review – Rocket Hazards

• what kind of hazards can exist?

Debris Impact



Broken up rocket pieces
Most visible ones in these pictures are burning solid rocket propellant

Toxic Dispersion

Blast Overpressure

Adequate Safety

Range Safety is the application of safety policies, principles, and techniques to determine or enforce adequate protection from hazards associated with an operations at a Range.

Safety is focus on:

1. ***Public Safety***
2. ***Worker Safety***
3. ***Property Safety***

All analysis techniques, safety system design requirements, and overarching policies are focused on achieving acceptable safety

What is safe "enough"?

Ideal: Containment

The hazard is contained and cannot affect people or property

Imperfect: Risk Acceptance

Containment is not always possible; when this is the case there has to be some level of probability accepted that a hazard can occur - First application of modern risk acceptance was actually in the application of probabilistic risk assessments for nuclear power in the late '50s, but the munitions and aerospace communities quickly followed suit in the '60s

Risk Concept – Key Elements

Risk is a concept that accounts for three key elements:

1. **Probability** of a dangerous event (e.g. a rocket crash)
2. Size of the "**danger area**" (e.g. the area destroyed by a rocket crash)
3. Nature of the **public exposure** (e.g. the population density and sheltering where a rocket could crash).

- **Risk is** computed as **the product of probability and consequence.**
- **Risk controls** (or mitigations) must **address at least one of three key elements** of risk illustrated in Figure.

Probability is a number from 0 to 1 that expresses the chance of an event outcome.

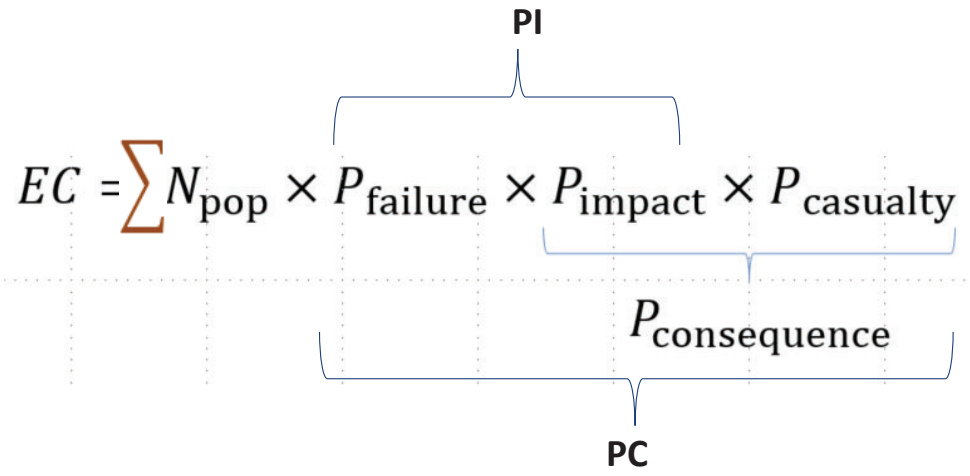
- **E.g. the probability of a 6 resulting from a single roll of an evenly weighted die is 1/6**

Three Fundamental Types of Risks

- AST regulates the risk of casualties, on individual and collective basis
  - A **casualty is** defined as a **serious injury or worse** for a human, including death. For the purposes of a FSA, serious injury is defined as Abbreviated Injury Scale (AIS) Level 3 or more.
  - **Individual risk** is the chance of a specified individual getting hurt or killed (measures as a Probability of Casualty, PC)
  - **Collective risk is not a probability**, but accounts for the chance that some member of a group of people becomes a casualty (measured as a sum of all Expected Casualties, Ec)
  - **High Consequence Event** include incidents that could involve multiple casualties, massive toxic exposures, extensive property or environmental damage, or events that jeopardize the national security or foreign policy interests of the United States

AIS SCORE	SEVERITY OF INJURY	INJURY TYPE
0	NONE	NONE
1	MINOR	SUPERFICIAL
2	MODERATE	REVERSIBLE, MEDICAL ATTENTION REQUIRED
3	SERIOUS	REVERSIBLE; HOSPITALIZATION REQUIRED
4	SEVERE	LIFE THREATENING; NOT FULLY RECOVERABLE W/O CARE
5	CRITICAL	NON-REVERSIBLE; NOT FULLY RECOVERABLE EVEN WITH CARE
6	VIRTUALLY UNSURVIVABLE	PROMPT FATALITY

Safety Criteria Metrics



$$CEc = N_{pop} X\ P_{consequence}$$

$p_{Consequence}$ is the *probability of consequence* and depends on the probability that hazardous debris impacts at or near the population center, and the probability that the impact results in a casualty

$$P_I = \sum (P_{failure} * P_{impact})$$

where:
P_I = Probability of Impact for the Cell,
Pf=Probability of failure for the event
P_i = Probability of impact accounting for number fragments impacting area and dispersion pattern

$$P_C = \sum \left(P_I * \frac{A_{cas}}{A_{cell}} \right); \qquad P_{casualty} = \frac{A_{cas}}{A_{cell}}$$

where:
P_C = Probability of casualty
P_I = Probability of Impact for the Cell,
A_{cas} = Fragment Casualty Area including shelter effects, and
A_{cell} = Cell Area

$$E_C = \sum (P_C * N)$$

where:
N is the number of people in one grid cell
P_C is the probability of casualty
And, when N=1, $E_C = P_{C\ (per\ pop\ center)}$

Safety Risk Criteria (450.101)

Collective Risk (Expected Casualty		
Public (Excludes NOPS & People on Aircraft)	450.101(a/b)(1)	1.E-04
Neighboring Ops (NOPS)		2.E-04
Launch Essential	N/A	N/A
Individual Risk (Probability of Casualty)		
Public (Excludes NOPS, People on Aircraf)	450.101(a/b)(2)	1.E-06
Neighboring Ops (NOPS)		1.E-05
Launch Essential	N/A	N/A
Aircraft protection (Probability of impact by casualty causing debris)		
People on Aricraft	450.101(a/b)(3)	1.E-06
High Consequence Protection (Conditional Expected Casualty)		
People in uncontrolled areas (land only)	450.101(c)	1) Flight abort in accordance with § 450.108 2) CEC is no greater than 1e-3, or 3) demonstrated reliability
Asset Protection (probability of loss of functionality)		
Critical Asset	450.101(a/b)(4)	1.E-03
Critical Payload		1.E-04

§ 450.101 Safety Criteria

(a) Launch risk criteria
- (1) *Collective risk*
- (2) *Individual risk*
- (3) *Aircraft risk*
- (4) *Risk to critical assets*

(b) Reentry risk criteria
- (1) *Collective risk*
- (2) *Individual risk*
- (3) *Aircraft risk*
- (4) *Risk to critical assets*

(c) High consequence event protection

(d) Disposal safety criteria

(e) *Protection of people and property on-orbit*

(f) *Notification of planned impacts*

(g) *Validity of the analysis*

Overview of (Underlying) Rationale Risk Criteria

Wilde, P. Public Risk Tolerability Criteria for Space Launch and Reentry, Presented at the 51st Scientific and Technical Subcommittee of the United Nations Committee on the Peaceful Uses of Outer Space, Vienna Austria, 8 Feb. 2014

Acceptable Risk

- Collective (1e-4)
- AST's collective risk criterion is lower than the 3rd party risks from conventional aviation, on an annual basis adjusted for the number of people exposed.
  - **Risk from an average commercial transport flight is ~1E-6 EC**
- Individual Risk (1e-6)
- Equals maximum individual risk of death allowed by any US public safety regulation (No regulatory precedent to allow higher.)
- Reasonably small relative to other background risks
  - **0.5% of the annual risk accepted by each US pedestrian**
  - About half the US annual individual fatality risk from falling objects or the chance of becoming a casualty from lightning
  - If you were at 1E-6 PC for a launch that occurred once a day, everyday since the year 720 BC, then you would be statistically expected to have been seriously injured or killed about now, but there's nearly 50% chance you would not have sustained any injuries.
- 1E-6 P_C internationally viewed as broadly acceptable on an annual basis for involuntarily imposed risks to the public
  - AST's per operation criterion thus assumes that it's unlikely the same individual is exposed repeatedly during a year to the maximum level

High Consequence

- FAA has accepted Conditional Expected Casualty (CEc) as the metric for the consequence as an appropriate means to assess the need for prudent mitigations (such as flight abort) of risks to public safety and the safety of property.
  - Both traditional and conditional risk metrics to evaluate the level of rigor required for safety analyses and hazard control strategies, including flight abort and flight hazard analyses.
    - **Ec** factors in the probability of occurrence for each reasonably foreseeable dangerous event
    - **CEc** determines the expected casualties assuming the dangerous event will occur
      - Free from the large uncertainties typically associated with the failure probabilities for launch or reentry operations
      - Better quantifies the consequences of an event and is embedded in quantitative risk analysis
- CEc threshold of 1e-02:
  - DOD/NASA/FAA use quantity-distance limits originally designed to limit conditional individual risk of fatality to 0.01 from inert debris fragment impacts (propelled by accidental explosions)
  - USAF/NASA explosive safety standards do not permit public buildings at closer distances than where hazardous debris impacts corresponding to a consequence limit of no more than 0.01 conditional risk of fatality
  - The average ground consequence from a general aviation crash is 0.01 conditional expected fatality
- CEC as used in 450 is the metric to determine:
  1. The need for flight abort with a reliable FSS as a hazard control strategy
  2. The reliability standards for any required FSS
  3. When to initiate a flight abort

Flight Safety Analysis Purposes

- A Flight Safety Analysis (FSA) must demonstrate compliance with the safety criteria in § 450.101 (defines how safe is safe enough).
  - Criteria include individual and collective public risks limits *separately applied* from lift-off through orbital insertion AND for reentry
  - A valid FSA is part of a risk management process that will also:
    (1) Provide a basis for well informed safety decisions by identifying the dominant sources of public risks and uncertainties, as well as potential mitigations.
    (2) Help inform the FAA's Maximum Probable Loss (MPL) determination and the USG critical asset risk assessment.

Inert Debris

- Total injury is due to the sum over specific body parts:
  - Head, thorax, abdomen, legs
- Injury is due to horizontal component of impact speed, except head which considers both horizontal and vertical impact speeds separately

$$p_{casualty} = \sum_{j=0}^{N_{cells}} CA_{cell_j} / A_{cell_j}$$

$$CA_{cell} = HA_{cell} \times p_{injury}$$

$$p_{casualty} = CA / A_{roof}$$

From AC 450.115-1A

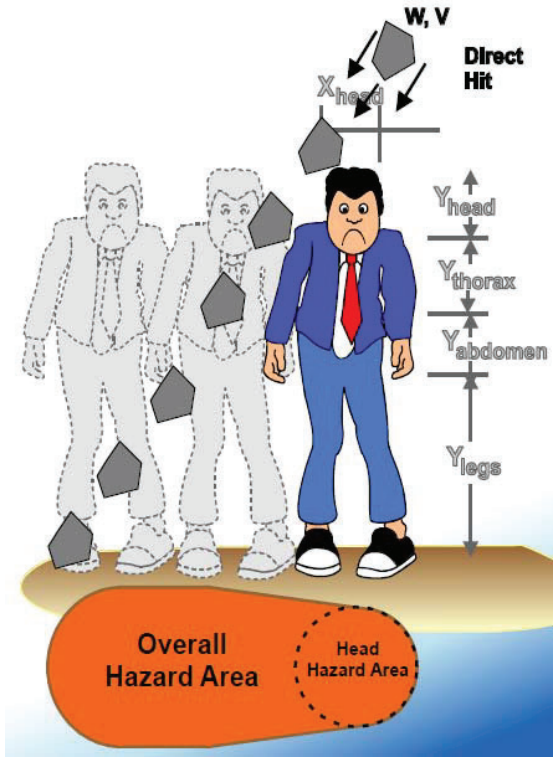
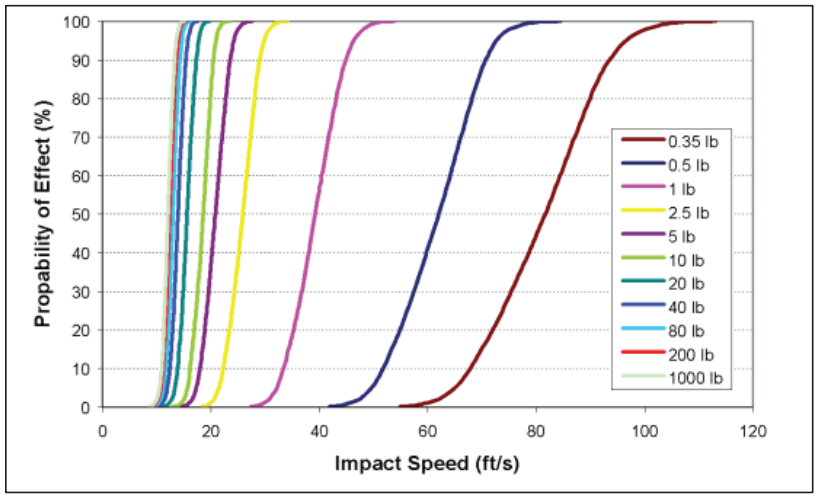


Figure 2 – Probability of Casualty Curves for Non-Mission Essential, Vertical Impact to Head, Blunt Injury



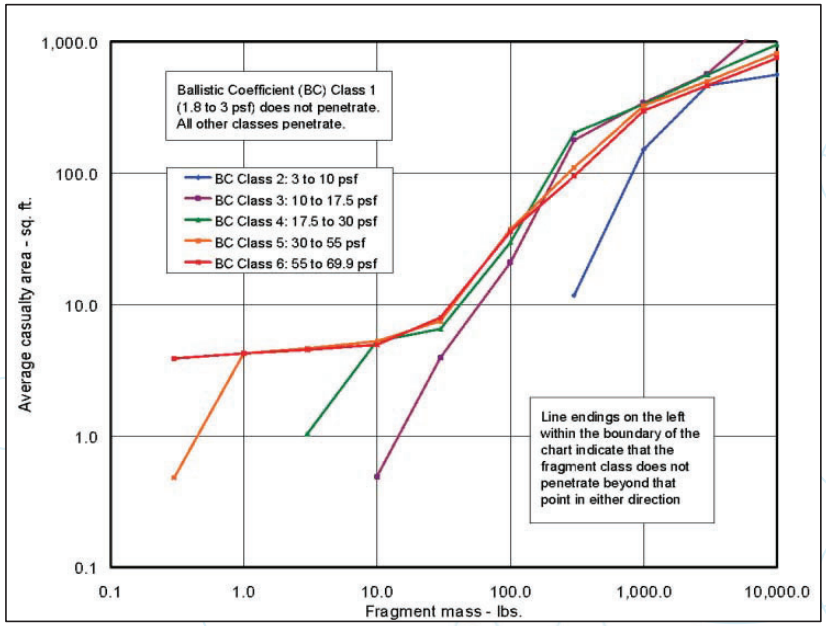


Figure 7 – Effective Casualty Areas of Hazardous Debris Hitting a Light Metal Roof (Class A)

Injury From Blast Waves

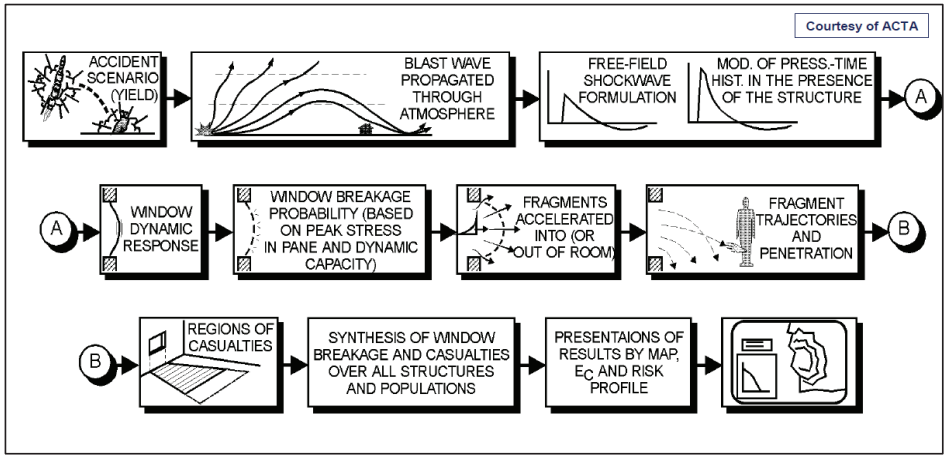
- Exploding propellant are evaluated for ground and ship impacts
- The weight and speed of the exploding propellant (and maybe surface type) determines yield, which is converted to pressure (P) and impulse (I)
- Injury to people is dominated by the effect on four body parts: the lungs, gastrointestinal (GI) tract, larynx, and eardrum.

$$PC(d) = 1 - \left(1 - p_{eardrum}(d)\right)\left(1 - p_{larynx}(d)\right)\left(1 - p_{GI\,Tract}(d)\right)\left(1 - p_{lungs}(d)\right)$$

- Both the breakup of the walls and windows should be evaluated. The reaction of the building should consider both the peak overpressure and impulse of the blast wave.

$$PC(d) = P_{wall}(d) + P_{window}(d) - P_{wall}(d)P_{window}(d)$$

From AC 450.115-1A



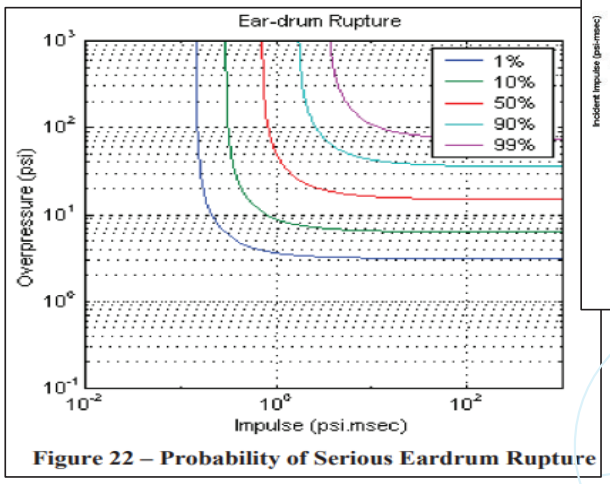
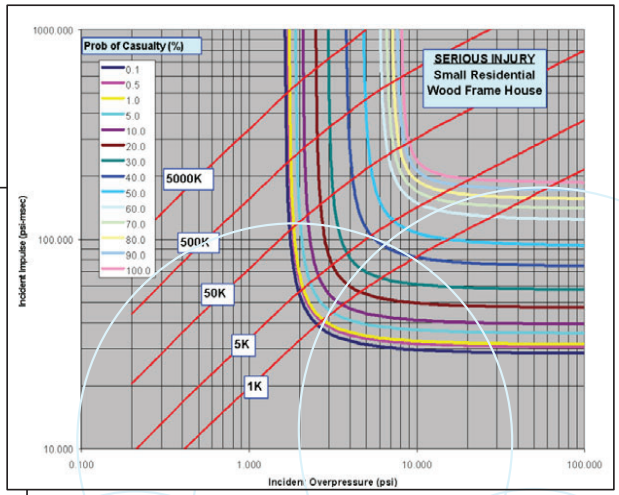


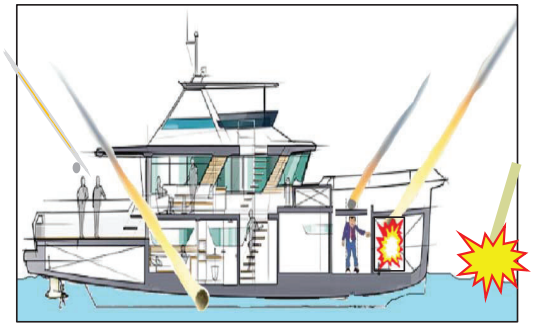
Figure 22 – Probability of Serious Eardrum Rupture



Federal Aviation Administration

Ship Vulnerability

- Local Effects
  - People on deck treated same as people in the open on land
  - Inert debris: For people inside the ship, the deck must be penetrated, in which case $CA = 3 \times A_{fragment}$
- Loss of Ship
  - Hull is penetrated
  - Deck is penetrated and fuel below is reached and subsequently ignites
- Nearby Explosion
  - Casualty due to near explosive impact effects on water (based on a threshold water distance)



$$A_{CasUnshelt}(\text{Frag}, Y) =$$
$$Min\{A_{ship}, Max[A_{Cas,inert\ Unshelt}(\text{Frag}), A_{Cas,deck\_expl\ Unshelt}(Y)] \text{ --- local effects}$$
$$+ A_{ship}[(1 - F_{fuel})P_{LossHull}(\text{Frag}) + F_{fuel}P_{deckpen}(\text{Frag})] \} \text{ --- loss of ship}$$
$$+ 2(L_{ship} + W_{ship})r_{Cas,near}(Y) + \pi\,(r_{Cas,near}(Y))\text{^}2 \text{ --- nearby explosion}$$

Table 6-10. Threshold Values For Significant Hull Damage

Ship Category		Penetration Criteria	
Generic Class of Ship	Deck/hull Material	Minimum Mass Fragment (lb)	Minimum Kinetic Energy (ft lbf)
< 25 ft	One plywood layer: 0.75 inch	0.6	25
25-50 ft	Two plywood layers: 0.5 inch and 0.75 inch	0.7	115
50-100 ft	Two plywood layers: 0.75 inch each	1.0	205
100-200 ft	Two steel layers: 0.1 inch and 0.2 inch	35	40,000
200-295 ft	Two steel layers: 0.2 inch and 0.3 inch	115	71,000
> 295 ft	Two steel layers: 0.2 inch and 0.4 inch	6300	1,250,000

From RCC 321-23 Supplement

Table 6-11. Threshold Loss of Ship Distances for Explosions in Water

Ship Category	Hazard Criteria	
Generic Class of Ship	Minimum Yield (lb-TNT)	Loss-of-Ship Distance (ft), $r_{Loss,near}$
< 25 ft	0.01	$37.5\ Y^{0.333}$ ($\approx$ 1.3 psi)
25-50 ft		
50-100 ft		
100-200 ft	10.0	$7\ Y^{0.36}$
200-295 ft		
> 295 ft	50.0	$12\ Y^{0.27}$

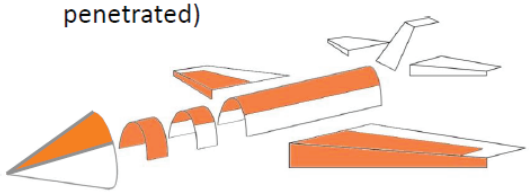
Table 6-12. Threshold Casualty Distances for Explosions in Water

Ship Category	Hazard Criteria	
Generic Class of Ship	Minimum Yield (lb-TNT)	Casualty distance (ft), $r_{Cas,near}$
< 25 ft	Same as loss-of-vessel	
25-50 ft		
50-100 ft		
100-200 ft	3.0	$20\ Y^{0.375}$
200-295 ft		
> 295 ft	10.0	$7\ Y^{0.44}$

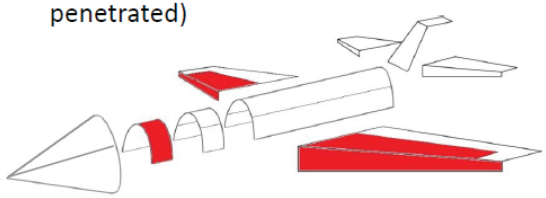
Aircraft Vulnerability

- Hit probability 1 x 10^-6
- Below 1 gm there is no damage, and above 300 gm is a catastrophic event
- Otherwise, aircraft risk computed from a “vulnerability area”, or “casualty area”, is due to all sections of the aircraft sections that are penetrated

Casualty Assessment
(Orange regions indicate casualty if penetrated)



Catastrophe Assessment
(Red regions indicate catastrophe if penetrated)



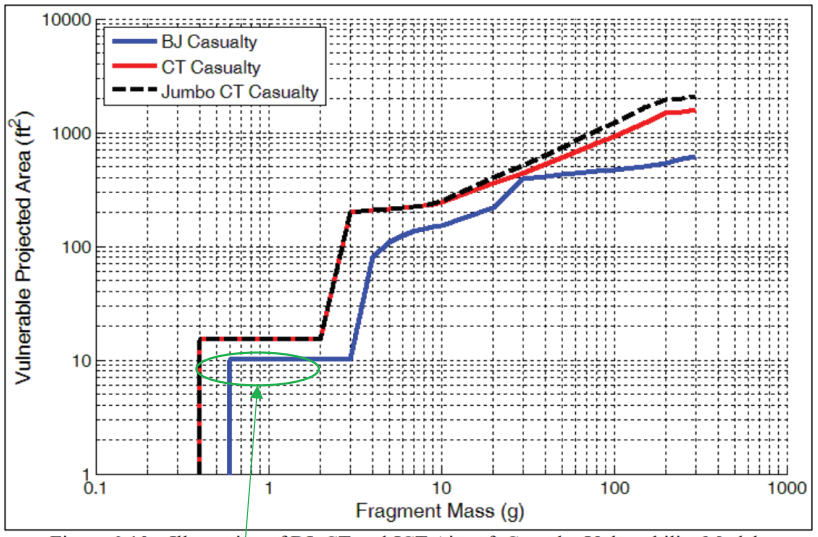


Figure 6-10. Illustration of BJ, CT and JCT Aircraft Casualty Vulnerability Models

15.3 square feet pf aircraft is vulnerable to 0.4 to 2 gram. A casualty would be expected if probability of impact of fragment with mas 0.4 grams of more is equal to or greater then 1E-06 within a aircraft projected area of 15.3 square feet.

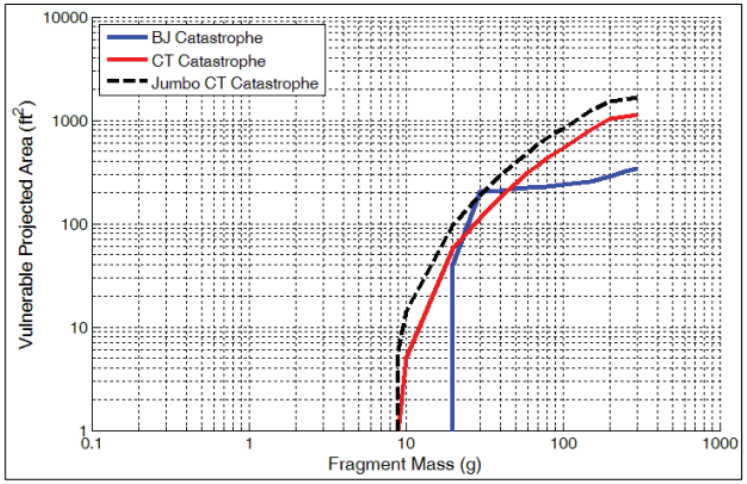


Figure 6-11. Illustration of BJ, CT, and JCT Aircraft Catastrophe Vulnerability Models

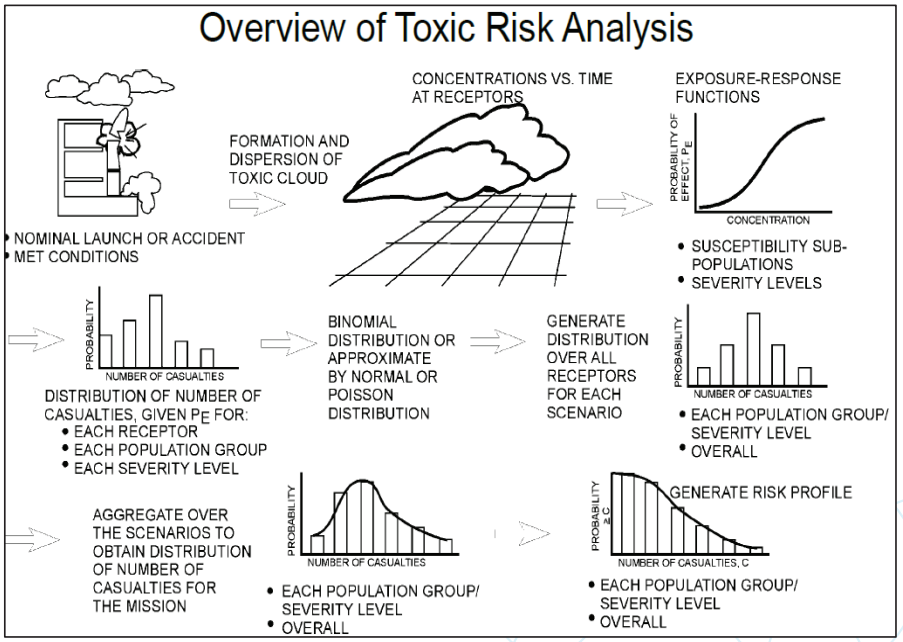
From RCC 321-23 Supplement

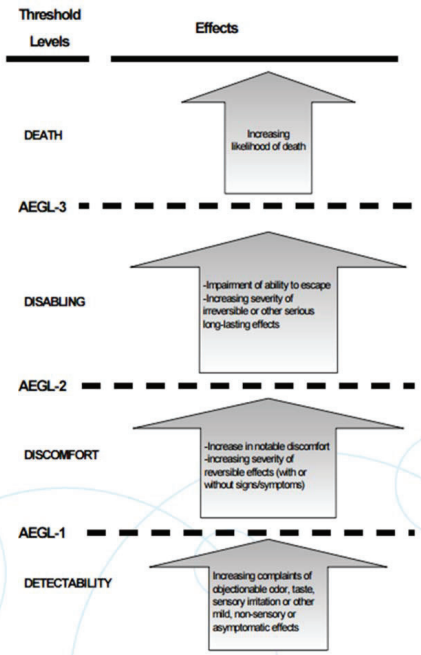
Toxic Spills

- Liquid propellants, such as hypergolic propellants, are toxic to people.
  - Batteries have chemicals that affect long-term health of environment.
  - Payloads may carry hazardous material, such as nuclear material, and any hazardous materials as defined in 49 CFR § 172.101
- Cold spill Hot spill
- Acute Exposure Guidance Levels (**AEGL**)
- People exposed to the toxic cloud within a threshold distance from the spill and cloud's lateral span is considered a casualty

$$p_{consequence} = \sum_{n=0}^{N_{cells}} p_n^{impact}(PC = 1)$$

- *Safety Design for Space Operations* references at the end of that chapter can assist in determining the length and width of the plume

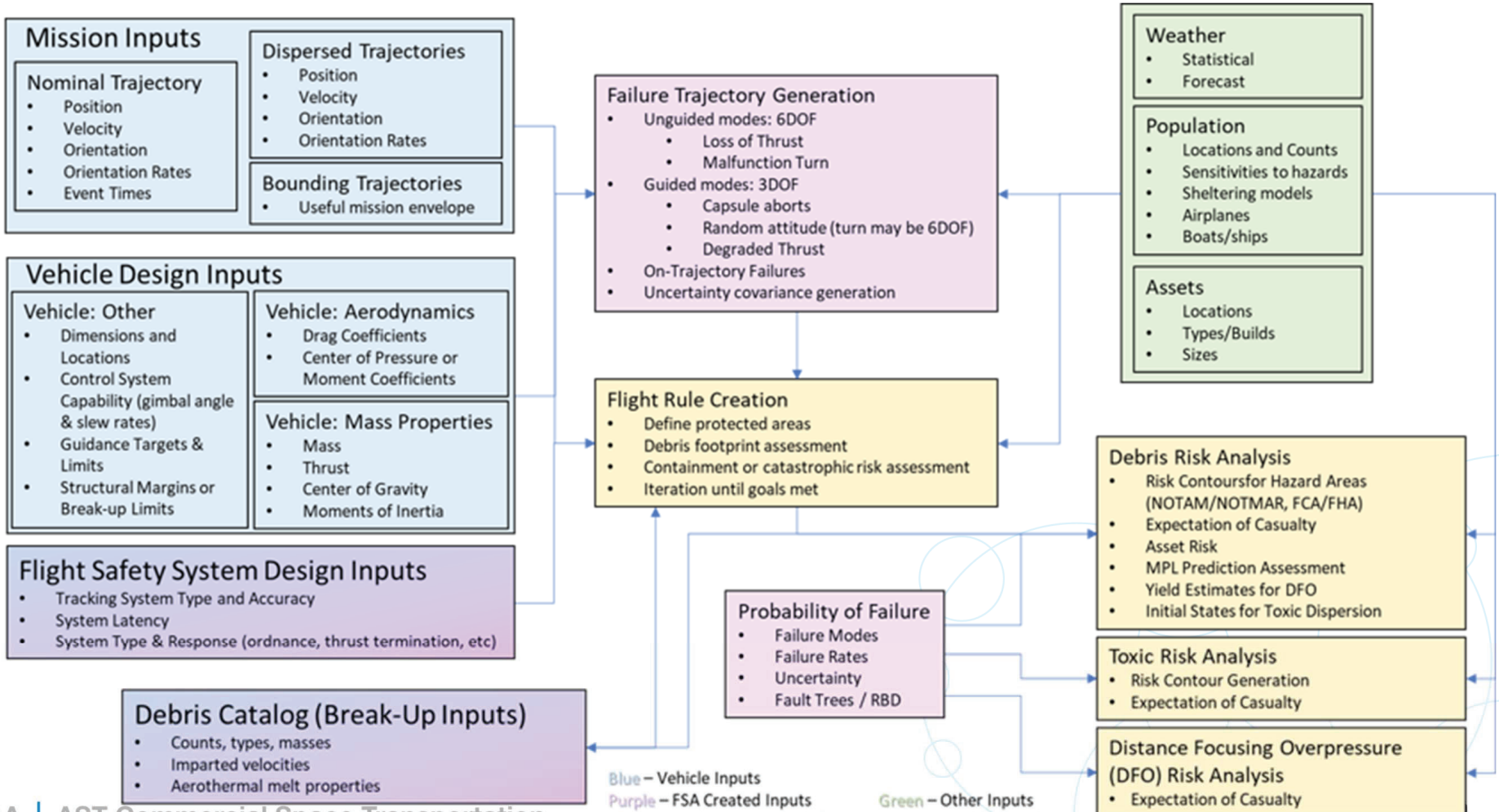




From AC 450.115-1A

Federal Aviation Administration

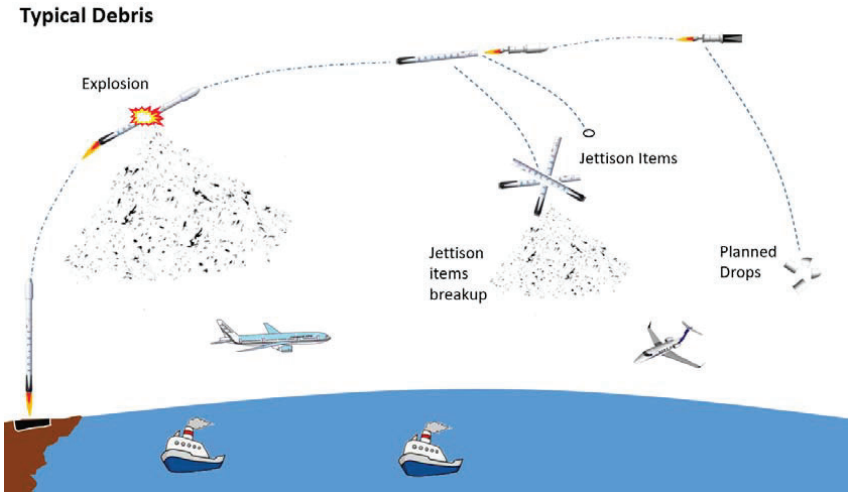
FSA Assessment Process

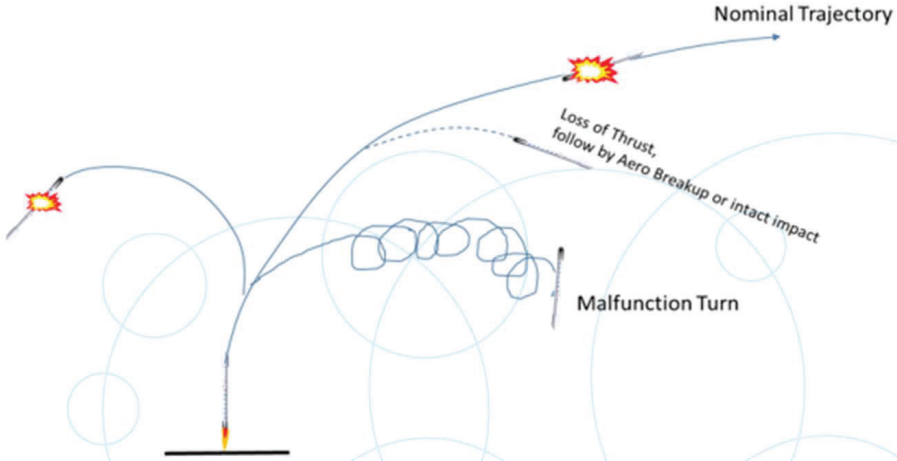


Planned Debris Failures

1. Planned debris
   - Include any solid object planned to fall uncontrolled through the navigable airspace as the result of a Launch activity, such as jettisoned stages, nozzle covers, fairings, and inter-stage hardware.

2. Malfunction debris
   - Include debris from vehicle malfunctions (FTS action)
     - Malfunction Turn (usually results in aero breakup)
     - Random Attitude (diabolic turns – could result in FTS action or aero breakup)
     - On trajectory explosion
     - Lost of thrust (aero breakup)



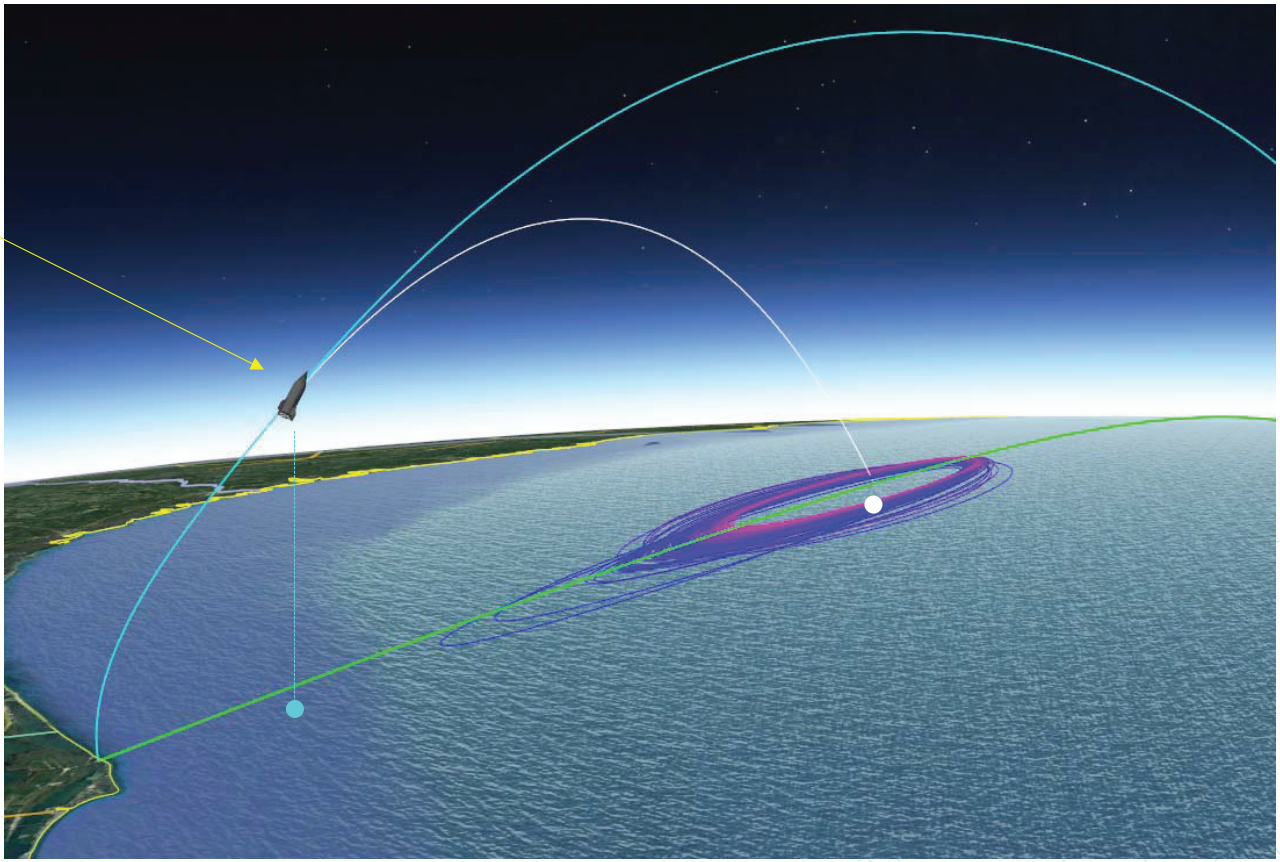


Note: Planned debris has probability of 1 (absolute) of occurring. In general 'On Trajectory Explosion' has a significant higher probability of occurring than another malfunction turns; this becomes evident in the resulting AHAs.

Side Note: IIP and Other Terms

Vehicle In-Flight

The only thing discussed here that an observer of the launch would actually see.

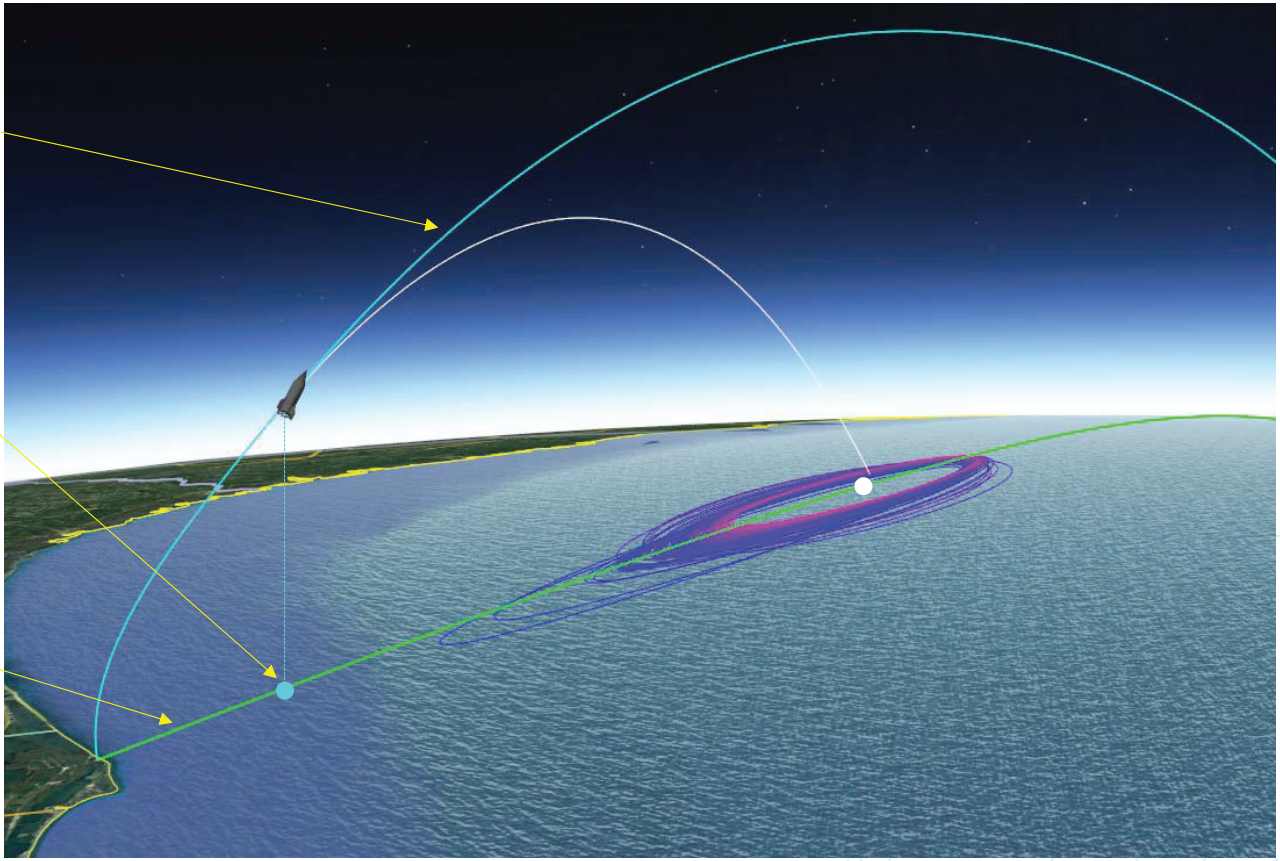


Side Note: IIP and Other Terms

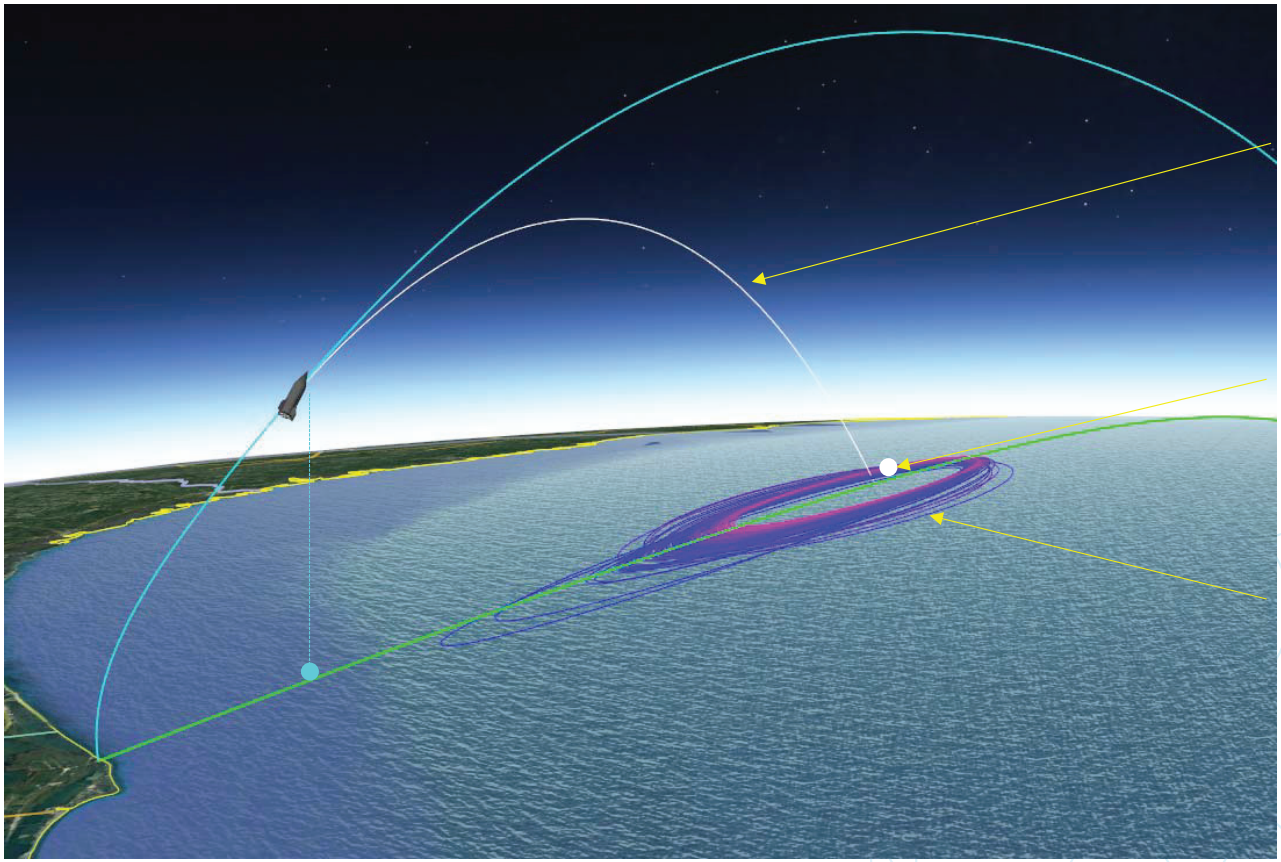
Nominal Flight Path
The trace of where the vehicle would nominally fly through its planned trajectory.

Present Position Ground Track
The projection of the vehicle's current location onto the surface of the Earth.

Ground Track
The projection of the nominal flight path onto the surface of the Earth.



Side Note: IIP and Other Terms



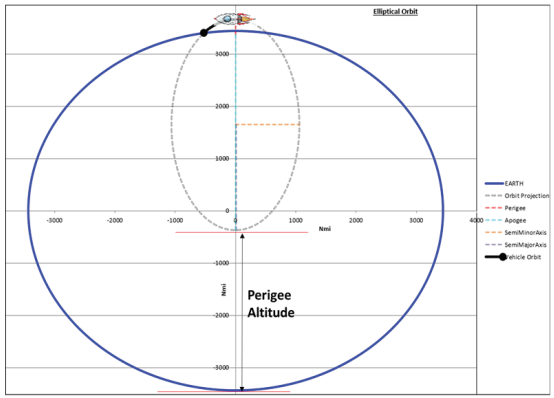
Ballistic Trajectory
The predicted trace of the vehicle's trajectory if all thrust were to cease. This can be propagated with atmosphere (aero force) or without (vacuum).

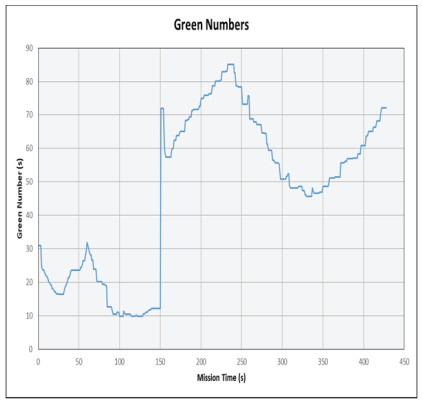
Instantaneous Impact Point (IIP)
(Can be drag corrected or vacuum)
The location where the ballistic trajectory intersects the surface of the Earth.

Debris Footprint
Ellipses representing a probability bound of where individual fragment groups would fall. Each group could represent single fragments or hundreds of fragments.

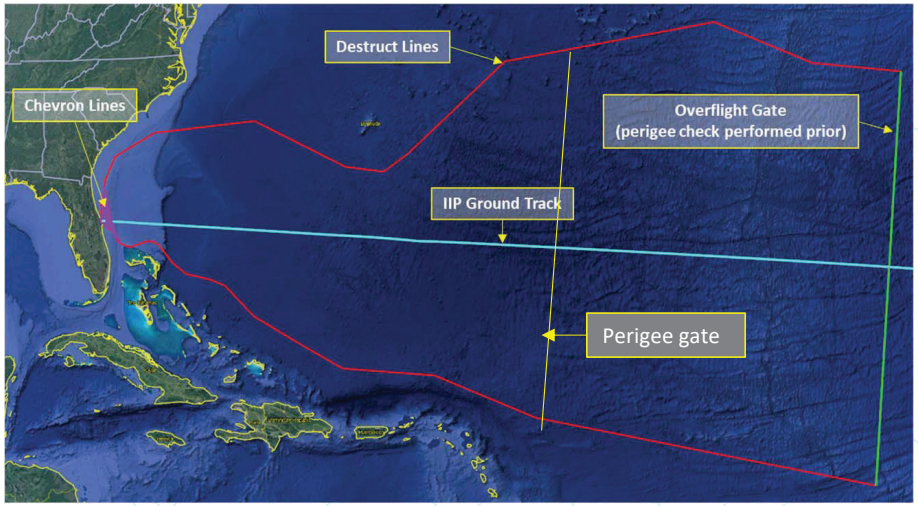
Flight Rules

- Flight Rules: Basic Types & Definitions
  - Impact Limit Line:
    - Boundary line across which no hazardous debris is allowed to fall
  - IIP Based Rules:
    - **Destruct Lines:**
      - Line Segments placed such that if a vehicle IIP track were to cross it, debris could fall beyond the ILL
    - **Chevron Lines:**
      - Moving destruct lines, typically utilized predominantly in the launch area to account for debris footprint growth as the vehicle (ideally) moves downrange
  - Present Position Based Rules:
    - **Azimuth/Elevation Limit:**
      - Limits defined for different times (or positions) of flight that limit the azimuth angle (or yaw or heading) and the elevation angle (or pitch or flight path angle) that the vehicle is allowed to fly
    - **Vertical Planes:**
      - Similar to azimuth/elevation limits, but projected onto a plane that is perpendicular to the ILL; the result is a set of "critical angles" that represent elevation angles at the relative azimuth
      - No longer used (duplicative in capability to chevron lines)



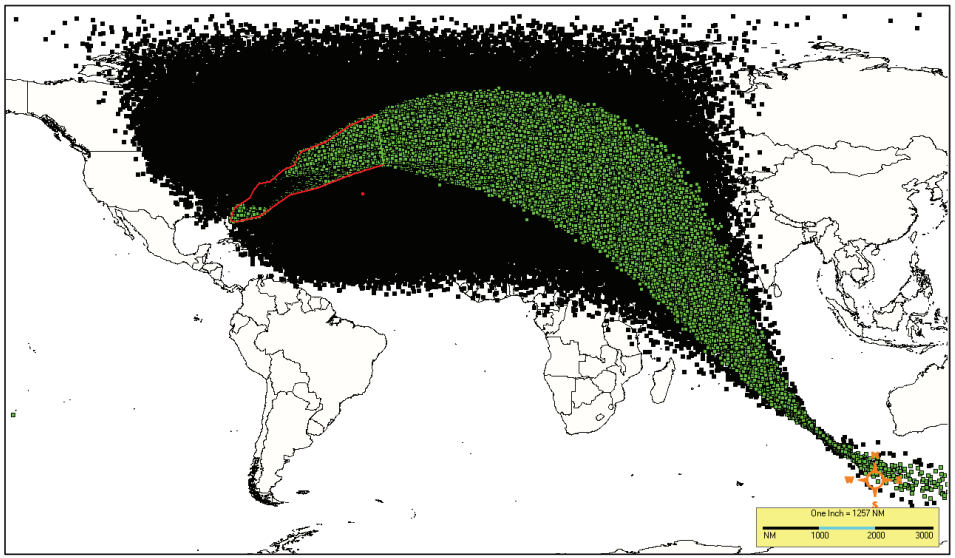


- Other Types of Common Rules:
  - **Straight-Up Time:**
    - Time limit based on when the debris footprint would exceed the ILL if the vehicle flew straight-up without pitching over
  - **Energy Check:**
    - Can be implemented in several forms (time, perigee, delta-v, etc), but should be checked to ensure good health prior to allowing overflight
  - **Minimum Altitude:**
    - Lowest altitude allowable (after a time/velocity) before commanding destruct to minimize overpressure from impact
  - **No Data Times:**
    - Minimum time that a vehicle could fly for in order to present a hazard – time counts down if all sources of data or tracking are lost
- Gates:
  - Places where a vehicle is allowed to fly through flight rules if it meets any given conditions (e.g. normal flight)

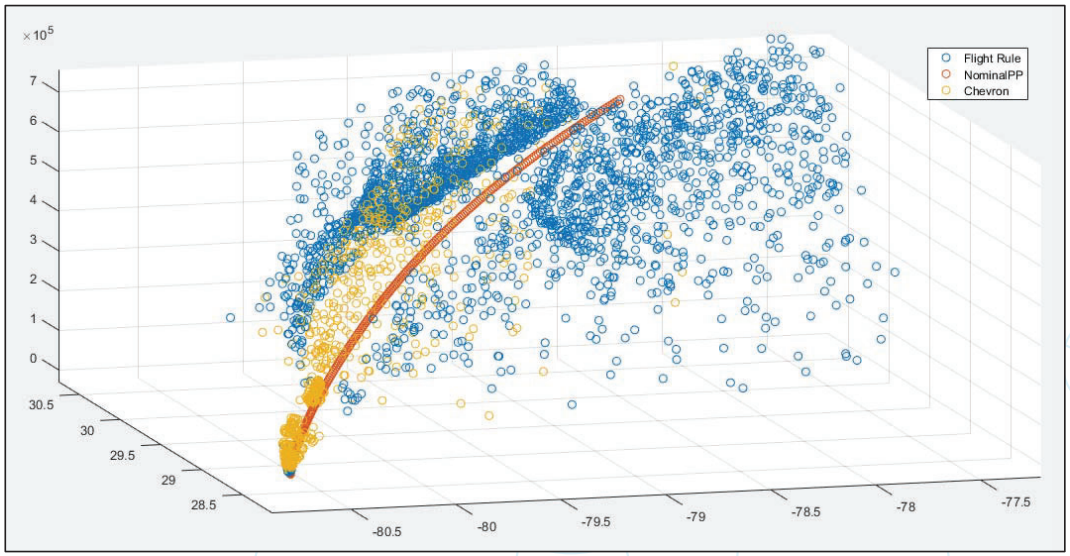


Flight rules in action

No flight Rules vs Flight Rules

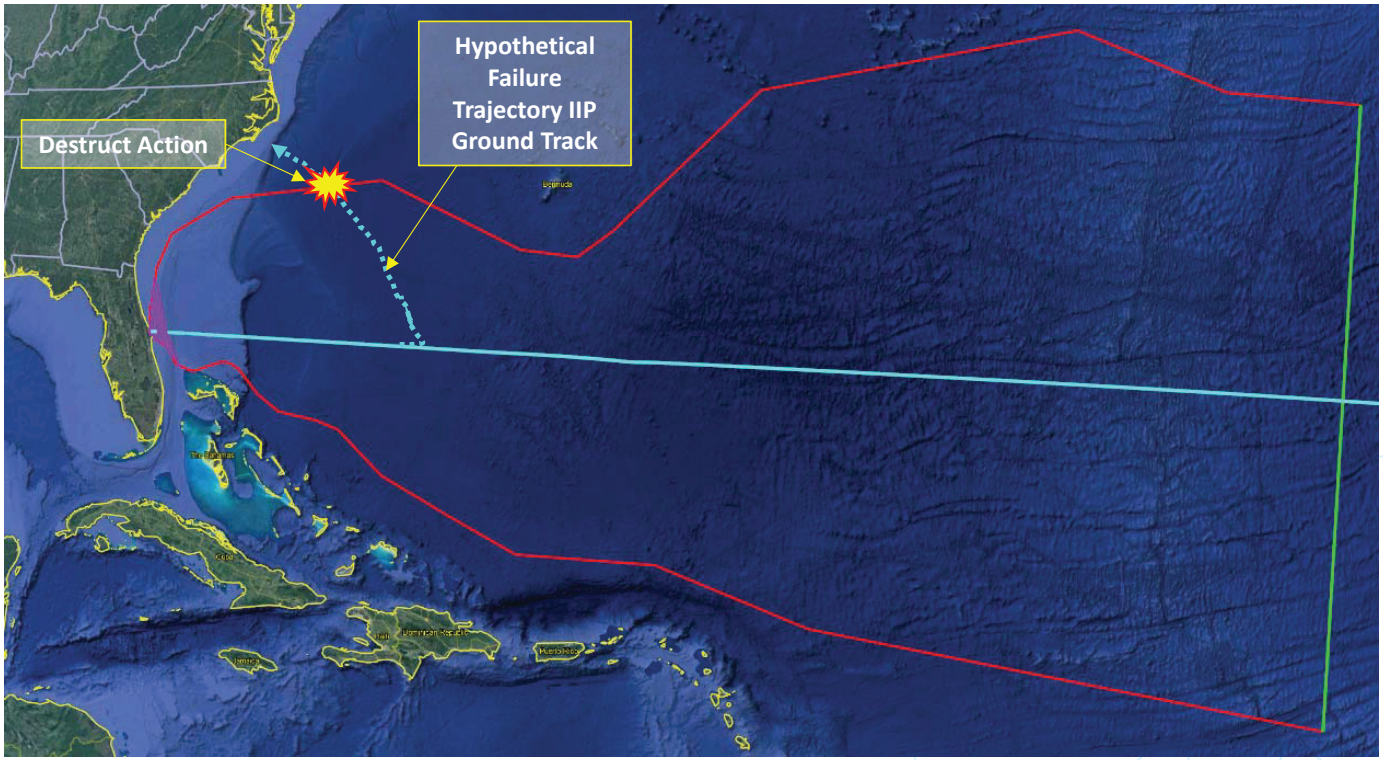


Nominal vs. Present Positions Caught by Flight Rules



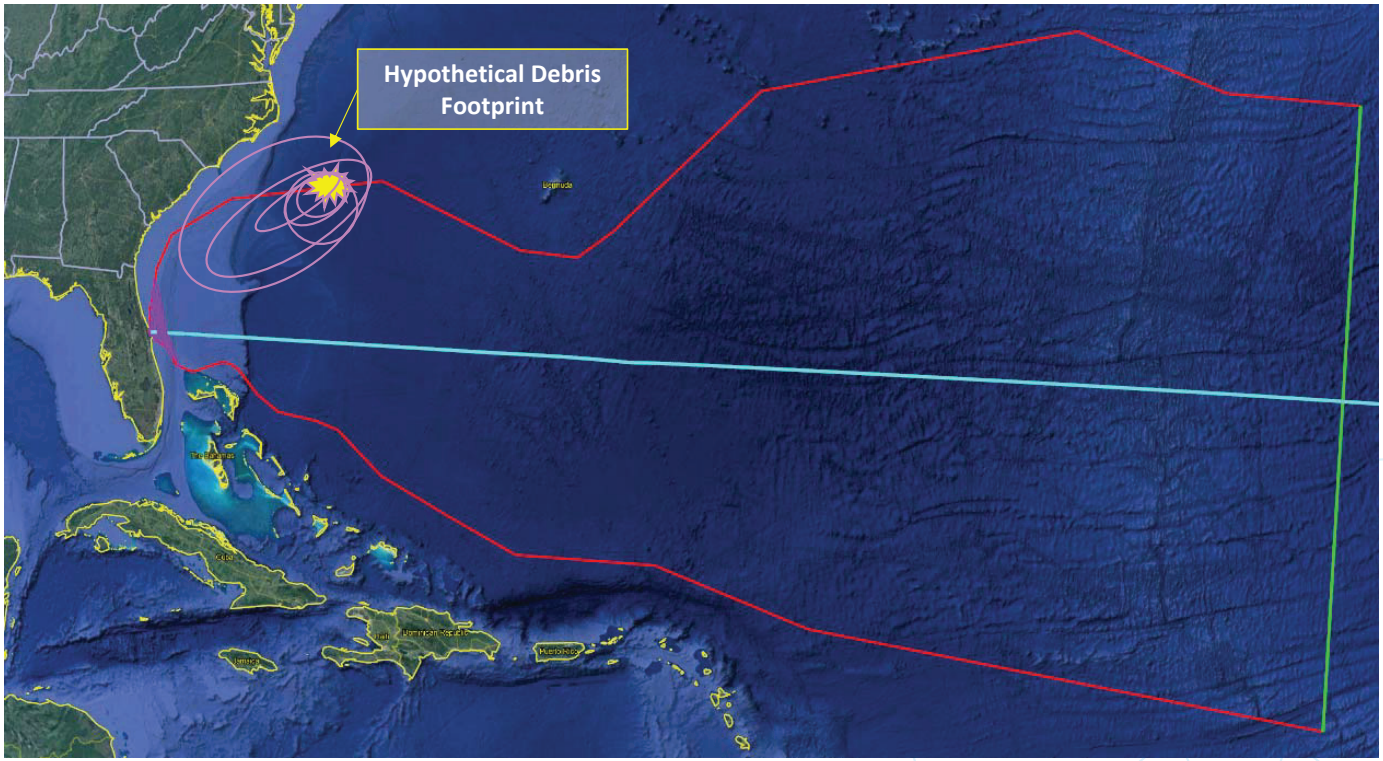
Risk Management in Action

- High Level Example of Common Flight Rules



Risk Management in Action

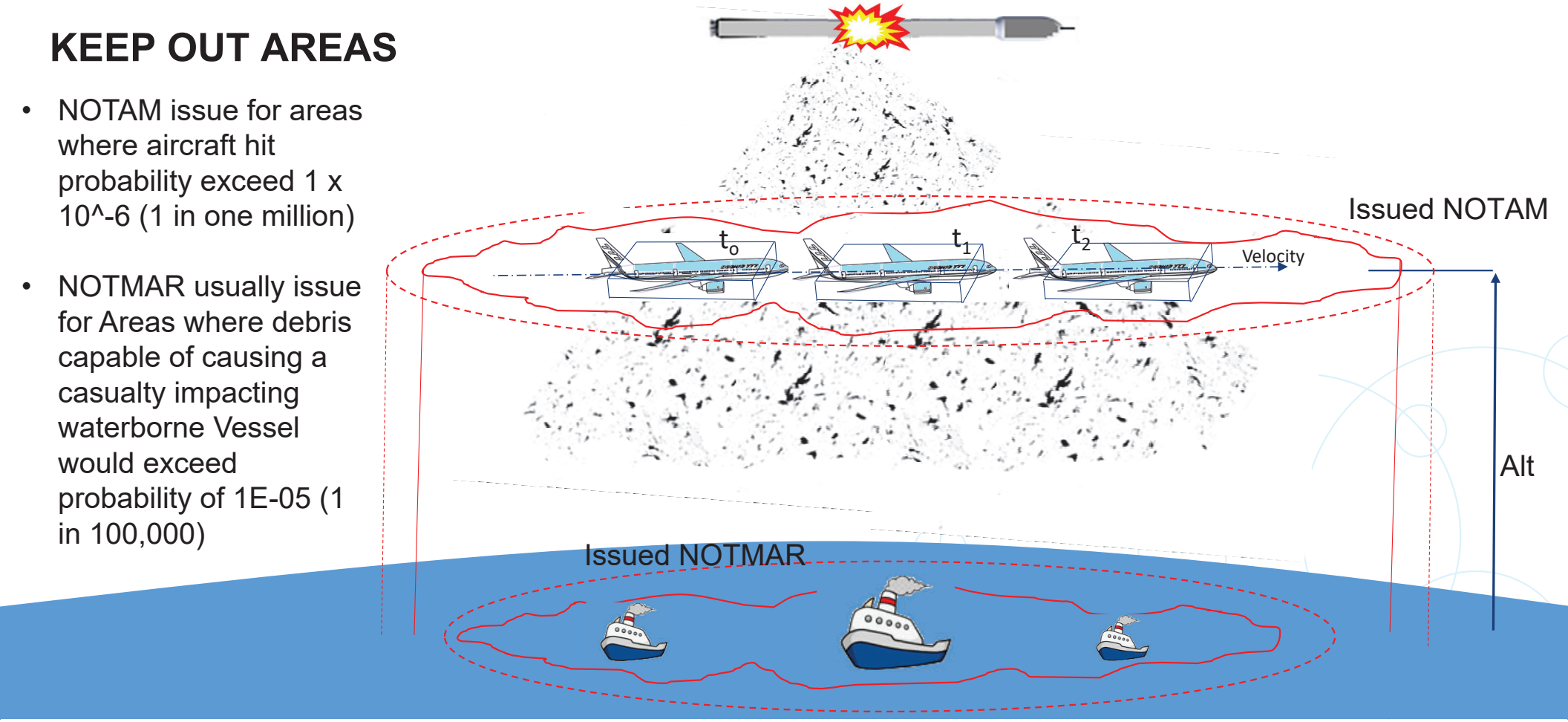
- High Level Example of Common Flight Rules



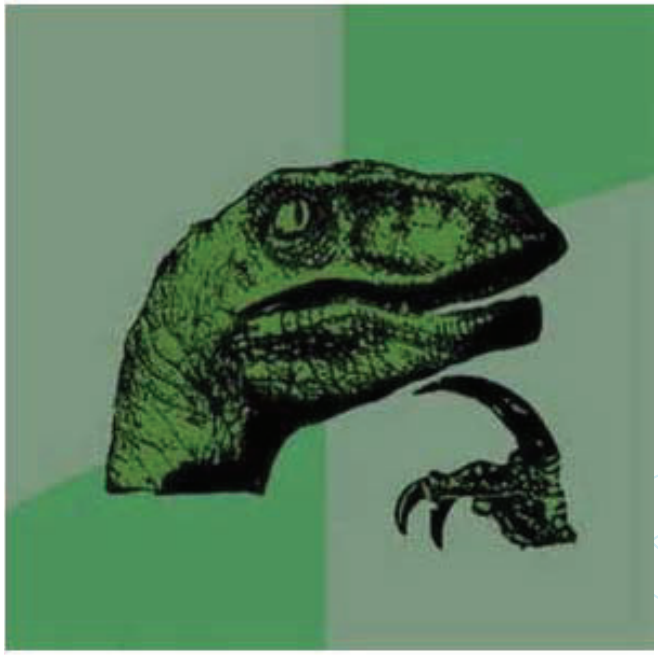
Risk Management

KEEP OUT AREAS

- NOTAM issue for areas where aircraft hit probability exceed 1 x 10^-6 (1 in one million)
- NOTMAR usually issue for Areas where debris capable of causing a casualty impacting waterborne Vessel would exceed probability of 1E-05 (1 in 100,000)



End of Day 1:
1st Section Safety Criteria under Part 450



- Q&A