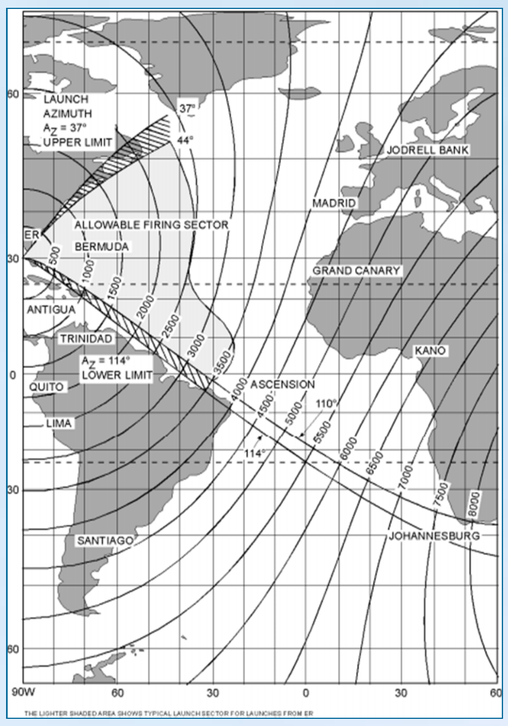
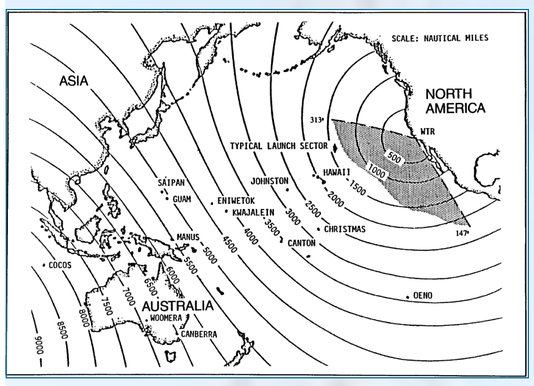
Range Safety Software IV&V — The Other Flight Safety Software

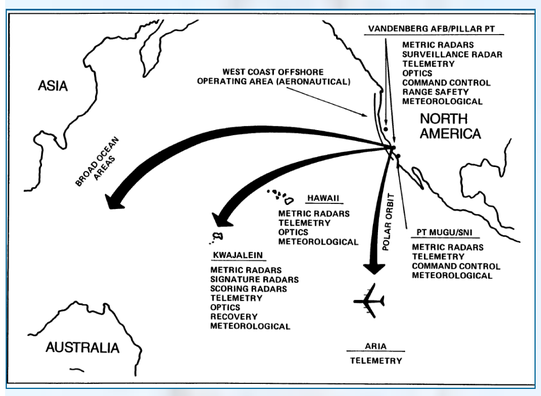
Range & Flight Safety Software Capabilities

- Launch vehicle, spacecraft, and space object tracking with respect to corridor azimuth Limits
- Launch vehicle and spacecraft propulsion system health monitoring and reporting
- Attitude control subsystem performance monitoring and control
- Ground system telemetry, command, communications.
- Secure Command & Communications





Launch Vehicle	Range Safety Coverage (seconds)
Atlas	0—750
Delta	0—670
Titan	0—660
Scout	0 - 650



Range and Flight Safety Requirements

1. AFSPC Manual 91-710 Range Safety User Requirements, Vol. 2 Flight Safety Requirements
2. FAA Rule 417 Commercial Space Transportation Regulations Licensing and Safety Requirements for Launch
3. RCC 313-01 Test Standards for Flight Termination Receivers/ Decoders
4. RCC 319-07 Flight Termination Commonality Standard
5. RCC 321-07 Common Risk Criteria Standards for National Test Ranges
6. RCC 323-99 Range Safety Criteria for Unmanned Air Vehicles
7. RCC 324-01 Global Positioning and Inertial Measurements Range Safety Tracking Systems' Commonality Standard
8. NPR 8705.5 Probability Risk Assessment (PRA) Procedures for NASA Programs and Projects
9. NPR 8715.5 Range Safety Program
10. NASA-STD-8719.13B Software Safety Standard
11. NSTISSP-12 National Information Assurance (IA) Policy for U.S. Space Systems

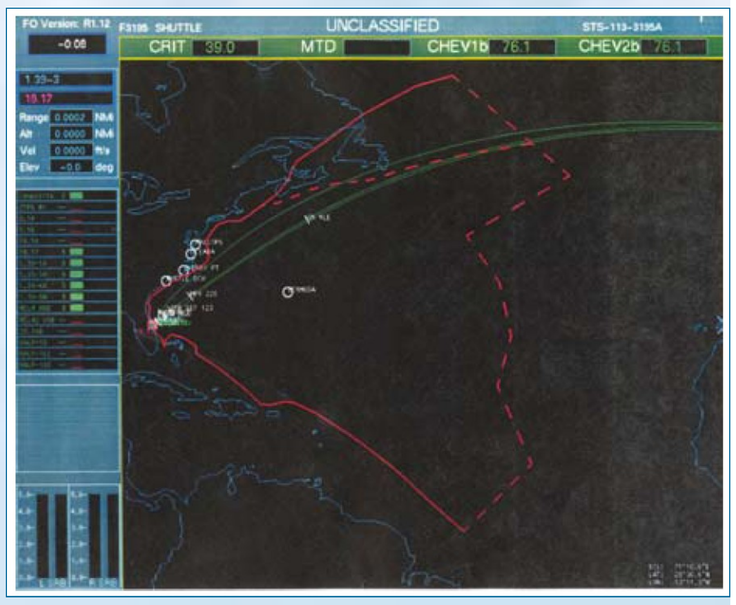
Range Safety Requirements Are Tailored to Fit Mission Needs, Geographic Locations, and Diverse Aerospace Architectures

- NASA Range Safety Program continues to evolve as spacecraft, launch vehicles, space transportation platforms, and range architectures change.
- Range requirements are tailored to fit spaceflight mission needs and spacecraft architectures such as:
  - Uninhabited/Unmanned Aerial Vehicles (UAV) or Unmanned Aerial Systems (UAS)
  - Autonomous Flight Safety Systems (AFSS)
  - The Constellation Program for both Ares 1-X and Ares 1
- Collision avoidance processes with respect to impact probabilities and miss distances change, impacting constraints on range safety requirements
- Frequency management issues and concerns impact range safety performance requirements and design constraints for telemetry, command, and communications in a dynamic environment
- NASA, FAA, and Air Force flight safety requirements are a shared responsibility that influence the language in flight safety requirements
- FAA's commercial space transportation licensing regulations are being amended in order to clarify its license application process general, and for launches from federal launch ranges, specifically.

Apply IV&V processes encompassing the following activities from RCC 319-07 Appendix A to assure an extremely high level of confidence in flight safety.

Independent Verification and Validation Analysis Support [RCC 319-07]

- **Requirements**—IV&V Process starts during the definition phase by using an independent group to verify requirements, evaluating specifications for completeness, accuracy, traceability, and testability.
- **Design and Development**—Once the requirements have been defined, support design and development activities to ensure the system meets all performance requirements.
- **Operational Evaluation and Test**—After the system development is complete, review program testing for completeness. Develop and conduct IV&V to identify any special tests required to verify any potential failure modes identified in the design and coding failure analysis.
- **Reporting** Anomalies—Report all anomalies throughout the development and operational implementation process. IV&V reporting processes and practices support the commonality standard's process steps listed in RCC 319-07, Appendix A, including anomaly severity classification.
- **Reviews**—Conduct design reviews and test readiness reviews for IV&V processes, criteria and tools. IV&V participates in technical interchange and program management meetings as required with the developer. Provide briefings and written reports as required to support the certification process.
- **Configuration Audit**—IV&V assesses configuration control of test and evaluation configuration items to assure test articles are representative of the final delivered configuration. Participate in Functional Configuration Audit / Physical Configuration Audit.
- **Reliability Analysis**—Analyze selected design reliability and verify that the design meets or exceeds the requirements of the system requirements documents and Range user needs when operated in an environment representative of the actual operating conditions. Evaluate Failure Mode, Effects, and Criticality Analysis (FMECA) and single point of failures analyses for the resulting impact on mission success, performance, staff safety, and maintainability.
- **Human Factors Analysis**—Analyze selected design as determined by the government to verify that the design is user friendly and can be easily operated without ambiguity in controls or operation. Identify and report design human factor deficiencies and recommended improvements.



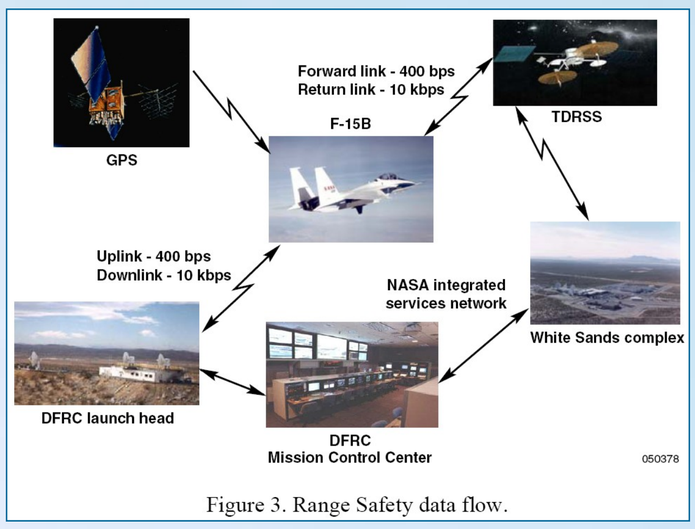
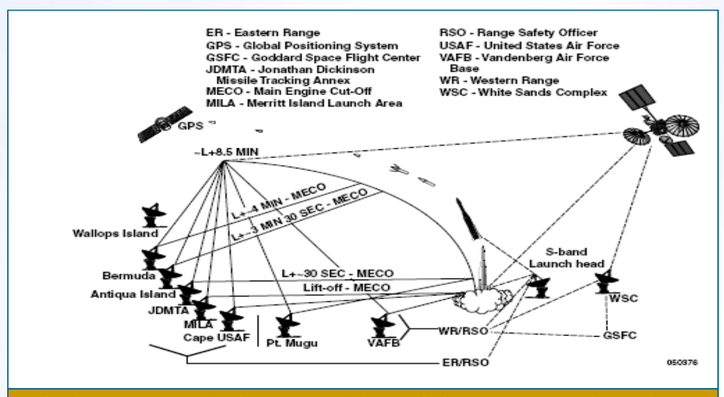
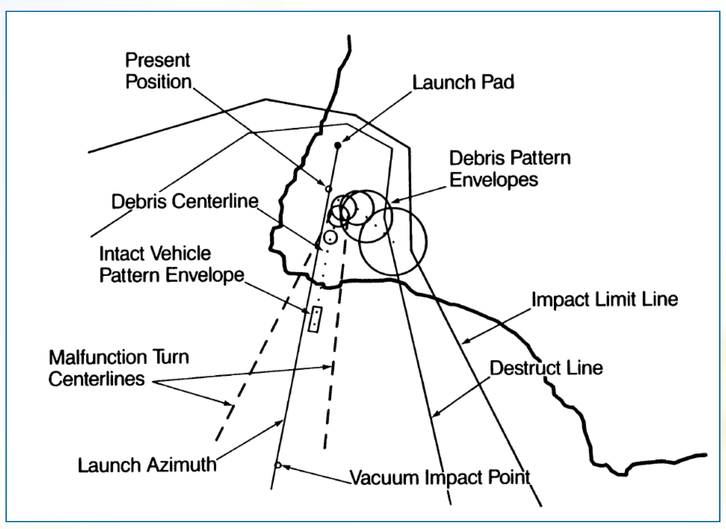


Figure 3. Range Safety data flow.

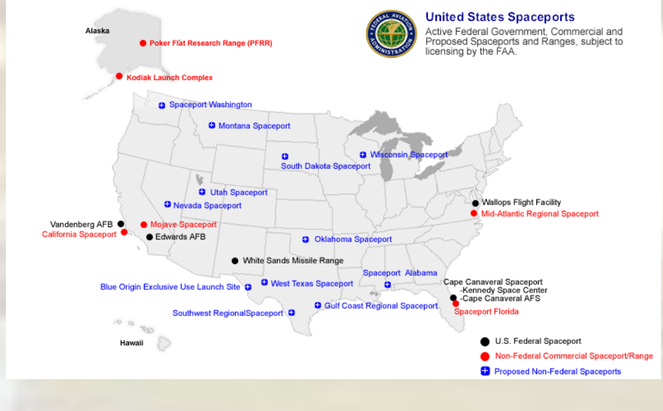


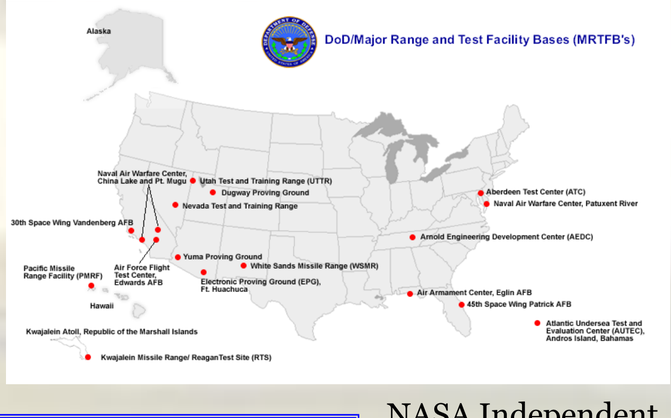
NASA/TM-2005-213662 Space-Based Range Safety and Future Space Range Applications



IV&V Reference Catalog of Flight Safety Critical Capabilities

- Flight Termination
  - Pyrotechnics control
  - Guidance control
- Recovery
  - Save or preserve the flight vehicle in the event of a malfunction
  - Activate recovery without additional risk to people or property
- Contingency Management
  - Failover control
  - Health monitoring for hazard detection and failure recovery
  - Fail safe functionality
  - Fault detection and recovery
- Vehicle Tracking
  - Flight path position determination and reporting with independent sources
  - Debris footprint impact determination
- Telemetry— Pre-flight and flight time FTS and launch vehicle health and status needed to support a flight termination decision
- FTS Command and Control
  - Redundant and independent command paths
  - Pre-launch test to validate launch readiness
- Radiation— Radiation control (rf, microwave, optical emissions





Streamlining Space Launch Range Safety

- **Minimize the need for launch range monitoring of air traffic**—Air traffic controllers use surveillance radar and communication networks to communicate with civil and military aircraft under their control and keep them clear of hazardous airspace during launch operations.
- **Reduce the number of launch range tracking systems**—Global Positioning Satellites (GPS) provide launch vehicles with position data that is processed onboard to compute state vectors for trajectory determination. Inertial Navigation Systems onboard provide redundant and independent attitude measurements.
- **Reduce the footprint for range safety systems**– an autonomous range safety system provides trajectory information for flight termination decisions by incorporating rule-based algorithms coded onto redundant flight processors. The system augments or replaces the functions of traditional ground-based tracking and safety systems, and it provides for range safety beyond the radar horizon in the presence of Radio Frequency Interference and in situations requiring minimal response time. Onboard processors track launch vehicle flight path and assess launch vehicle trajectory, proximity to launch corridor hazard boundaries, and system health to make flight safety decisions.
- **Improve Launch Flexibility and Responsiveness**—Autonomous systems permit launches from locations without extensive ground-based assets and provide coverage for portions of flight beyond the normal range of ground stations

Terminology

Destruct Line—a line established to ensure that a launch vehicle's critical debris impact dispersion does not violate the impact limit line; destruct lines are displayed on the Range Safety Display and when the instantaneous impact point, based on valid tracking data, shows that the vehicle will cross the destruct lines, the Mission Flight Control Officer is authorized to terminate flight.

Errant Launch Vehicle—A launch vehicle that, during flight, violates established flight safety criteria and/or operates erratically in a manner inconsistent with its intended flight performance. Continued flight of an errant launch vehicle may grossly deviate from planned flight, with the possibility of increasing public risk to unacceptable limits. An errant vehicle is also one which has violated safety criteria (a destruct line) and cannot be destroyed.

Launch Azimuth—the horizontal angular direction initially taken by a launch vehicle at liftoff; measured clockwise in degrees from true North.

Launch Vehicle—a vehicle that carries and/or delivers a payload to a desired location; a generic term that applies to all vehicles that may be launched from the Eastern and Western ranges, including but not limited to airplanes; all types of space launch vehicles; manned space vehicles; missiles; rockets and their stages; probes, aerostats, and balloons; drones; remotely piloted vehicles; projectiles, torpedoes, and air-dropped bodies.

Mission Critical—Item or function that must retain its operational capability to assure no mission failure (i.e., for mission success).

Range Safety Critical Systems—includes all airborne and ground subsystems of the flight safety system.

Range Safety Launch Commit Criteria—hazardous or safety critical parameters, including, but not limited to, those associated with the launch vehicle, payload, ground support equipment, flight safety system, hazardous area clearance requirements, and meteorological conditions that must be within defined limits to ensure that public, launch area, and launch complex safety can be maintained during a launch operation.

Safety-Critical—Any condition, event, operation, process, equipment, or system that possesses the potential of directly or indirectly causing harm to humans, destruction of the system, damage to property external to the system, or damage to the environment.

Tom Hempler, Thomas.D.Hempler@ivv.nasa.gov, TASC, Inc.

NASA POC: William Stanton, William.M.Stanton@ivv.nasa.gov

"Protect the public, the workforce, and property during range operations such as launching, flying, landing, and testing launch/flight vehicles."

NASA Independent Verification and Validation Facility

Fairmont, WV