Commercial
RLV Operations and Maintenance
Preliminary Guidelines

July 1, 2004

Federal Aviation Administration

Office of the Associate Administrator for Commercial Space Transportation

RLV Maintenance Preliminary Guidelines

1. **The applicant shall submit a maintenance program plan to facilitate maintenance and repair actions in the anticipated RLV operations environments. The maintenance program plan should be systematically formulated in the early conceptual design phase of the program to minimize problems during the operational phase.**

Rationale:

This guideline is to assure continuous flightworthiness of RLVs (similar to FAA Aviation airworthiness approach). The maintenance program plan should include scheduled and unscheduled maintenance to ensure public safety. Scheduled maintenance is intended to maintain the vehicle or hardware at the same level of safety as when it was approved. A properly maintained vehicle is less likely to experience an operational problem that would adversely affect public safety. Unscheduled maintenance takes care of unforeseen problems and is used to return a vehicle to the same safety level as when it was approved. Unscheduled maintenance can also be used to correct design or other problems in systems and components. Incorporating maintenance into the design phase results in hardware that is easier to maintain. Access panels and component access are good examples of this concept. A piece of hardware that is easy to maintain is more likely to be maintained correctly. If maintenance is too difficult, short cuts and omissions can occur, thereby compromising public safety. A side benefit is streamlined maintenance with reduced operational costs.

2. **The maintenance program plan should include:**

a) Locations and facilities where maintenance will be accomplished.
b) Level of components such as systems, sub-systems that will be maintained.
c) Storage plan for spare parts, material and all limited shelf life components.

Rationale:

Identifying the locations and facilities where maintenance will be accomplished allows AST to make a determination of the adequacy of such facilities and locations for a given maintenance operation. It also allows AST inspectors to verify that the facilities and locations are adequate and that they remain adequate for the purpose of an approved RLV maintenance operation. One concern is that the maintenance operation be conducted without affecting public safety. Blast and toxic release hazards are the main contributors to this concern. Proximity of the public and weather conditions are factors in determining the suitability of a location or facility for a maintenance operation. Another concern is that the location and facilities are sufficient to ensure the maintenance being performed meets the requirements of the approval for that maintenance operation. For example, if a facility lacks the necessary Ground Support Equipment (GSE) to perform maintenance in a safe manner, public safety could be compromised if an accident occurs due to the failure of the GSE. It is important to know the level at which component maintenance will be performed. This knowledge enables inspection of subsystems and parts at the appropriate level so that effort is reduced and public safety is ensured. A storage plan for limited shelf life items provides a way to document and inspect the usability of such items.

3. **A maintenance plan shall include the types of tasks to be performed, frequency of maintenance, preventive and corrective maintenance actions, personnel numbers and skill levels, tools, and test equipment required to sustain a maintenance program.**

Rationale:

Initial review of such a plan results in a credible maintenance plan that ensures public safety throughout the operation. The plan is also a useful inspection tool. A list of tasks to be performed will enable the reviewer to highlight tasks that affect or can potentially affect public safety. The list also serves to ensure tasks are performed in a manner that will not affect public safety and that all the necessary hazard controls are in place. A list of tasks will be helpful by allowing the inspector to review and prioritize, without omission, the tasks to be inspected. Frequency of maintenance is important to public safety because parts and systems that experience wear over time need to be maintained or replaced at given intervals. The interval between maintenance cycles is important to ensure no failures occur before the part in serviced or replaced. The frequency of maintenance is also an important inspection tool to make sure failures do not occur. Preventive maintenance actions ensure public safety by avoiding failures before they occur. Corrective maintenance actions ensure public safety by returning a failed part, system, or vehicle to the approved state. The operator should have a plan for both preventive and corrective maintenance actions. Personnel numbers and skill levels are important to ensure public safety. Specifying the skill levels of people involved in the maintenance ensures that qualified people are assigned to a maintenance task. Personnel assigned to a maintenance task should be required to sign-off once the task is completed. This ensures safety through accountability. An operator must have enough qualified people to ensure the maintenance program plan can be implemented. If there are not enough qualified people to support an operation, public safety may be compromised by having work done by inexperienced or fatigued personnel. Inexperience and fatigue contribute to a higher probability of failure. Tools and test equipment are also important in a maintenance program plan because the right tool is needed to do the job right. For example, improperly torqued bolts can pose a public safety threat such as loose connections to the engine, etc. Having the tools properly calibrated and periodically inspected is critical to ensuring a safe operation. The calibration program should be consistent with standards issued by the National Institute of Standards and Technology (NIST).

4. **The applicant shall develop and implement a system that will identify, track and report problems related to maintenance activities of flight hardware and software. The applicant shall establish a data collection system that can be used to identify failure trends and to communicate "lessons learned" from maintenance experience.**

Rationale:

Due to the nascent nature of the RLV industry, data collection is imperative in order to develop meaningful regulations that will provide adequate inspection periods and identify which parts/subsystems require maintenance to ensure public safety. The data can also be used to adjust the maintenance program plan based on lessons learned.

5. **If subcontractors are used, the applicant shall develop appropriate maintainability requirements to impose on each subcontractor. The applicant must have continuous or periodic review, inspection, and assessment to assure that each subcontractor is implementing his maintainability program effectively.**

Rationale:

The operator is ultimately responsible. Regardless of who performs the maintenance, the operator is responsible to ensure that it is accomplished in a way that ensures public safety. It is the operator that is liable for any damages resulting from improper maintenance. Following this draft guideline is beneficial to the operator because it is the operator who is protected by making sure the subcontractor performs maintenance in a proper manner.

6. **The applicant shall have a Configuration Management system to ensure that flight configuration correlates to a known, tested configuration of parts, systems, sub-systems, and software.**

Rationale:

This draft guideline will contribute to ensuring public safety by having the correct parts used for each configuration and prevent usage of unauthorized parts/components. In addition, this guideline will ensure traceability of the part/component. This draft guideline will facilitate the tracking of a part/component in support of a failure investigation. Configuration management is standard industry practice and is supported by ISO 9001 certification. Other configuration management recommended practices include participation in a fastener integrity program and Government Industry Data Exchange Program (GIDEP).

7. **The applicant shall submit an inspection schedule to the Associate Administrator for Commercial Space Transportation for approval. This schedule must include the items to be inspected and specify the periodicity of the inspections. Once approved by the Associate Administrator for Commercial Space Transportation, the applicant must adhere to this schedule**.

Rationale:

Since RLV concepts are widely different, it is not practical for the FAA to determine the inspection criteria for RLV equipment. The manufacturer is the best entity to determine the required inspection periodicity and associated rationale for each system or component. The FAA expects that initial RLV flights will have many systems or components that are inspected after every flight. Once sufficient experience exists to determine the reliability of various components, sub-systems, and/or systems, the applicant may submit a new inspection schedule to reflect the revised periodicity and associated rationale based on real data for FAA approval. The new inspection schedule will be used once the FAA approves it. FAA will require documentation to verify the justification for the proposed inspection periodicities. This draft guideline will ensure that the applicant has put forth a well-documented inspection plan based on the design and operation of the RLV that contributes to ensuring public safety is adequately protected.

<u>RLV Support Personnel Preliminary Guidelines</u>

General Notes:

A. *One person may perform more than one task/responsibility concurrently.*
B. *Collaborative Decision Making Team (CDM): Users that are necessary to provide equitable service and safe operations for all National Airspace System (NAS) stakeholders.*
C. *These positions are hypothetical and fulfill the functions of an RLV operations and maintenance program.*

1. Vehicle Mission Coordinator (VMC) - The VMC is the mission planner. The VMC shall define and file mission profiles according to FAA's established procedures, including nominal and emergency procedures. The VMC shall collaborate with FAA ATC for access to the National Airspace System (NAS). The VMC shall coordinate with the Launch Site Operator (LSO). The VMC shall have the subject knowledge of the FAA Air Traffic Control (ATC) rules and regulations and the National Airspace System (NAS) operational requirements. The VMC shall understand the operational limitations, restrictions and capabilities of the space vehicle, and the launch and reentry operations and their associated regulatory requirements. Additionally, the VMC shall have task knowledge of notification procedures and processes. Furthermore, the VMC shall be able to perform the task of collaborating with the LSO to plan and develop a mission profile, coordinate with LSO and FAA ATC personnel to meet mission milestone dates and activities, and collaborate with all NAS entities as required. The RLV operator shall create a VMC training plan and maintain records that show training received. All records and related activities shall be subject to FAA/AST safety inspection.

Rationale:

Efficient coordination with various requisite air traffic entities will be critical to bring about safe, routine aerospace operations. Effective filing of mission profiles according to established procedures, including nominal and emergency procedures, is essential to facilitate a safe, smooth transition of the NAS for commercial space launches. The inclusion of the VMC within the collaborative process promotes safe and efficient operations of the NAS.

Responsible Party: Reusable Launch Vehicle Operator

2. **RLV Aerospace Maintenance Technician (RAMT) - The RAMT shall be familiar with theory and demonstrate practical and hands-on knowledge of: systems/subsystems functions and operational tests that relate to the operations and maintenance of a particular vehicle(s). The RAMT must demonstrate proficiency in each of the systems/subsystems identified in the proposed ratings matrix, if the systems/subsystems are used in the vehicle or support equipment.**
The RAMT for the proposed matrix shall have the following skills and qualifications:
Subject Knowledge (SK)
Understand the function and operation of the applicable system/subsystem
Task Knowledge (TK):
Know how to predict, isolate, and resolve problems
Know step-by-step procedures of the technician documents
Know why and when the task must be done
Task Performance (TP):
Perform and complete all tasks

Proposed Ratings Matrix for RAMTs & Proposed Required Skill Sets:
(A RAMT approval may entail one or any combination of ratings below)

Propulsion Rating	Aerospace Systems Rating	Avionics/Electronics Rating
• Propulsion • Hydraulics • Pneumatics • Flight Safety Systems • Environmental Systems • Propellant Management Systems • Health Monitor & Data System • Land/Recovery Systems • Power Systems • Pressure Vessels • Hazard Materials • Ordnance • Engine Controllers	• Thermal Protection Systems • Structures • Hydraulics • Pneumatics • Crew Systems (if manned) • Payload Systems • Environmental Systems • Health Monitor & Data System • Land/Recovery Systems • Pressure Vessels • Ordnance	• Navigation and Guidance • Avionics • Flight Control • Communications • Electrical/Wiring • Software • Flight Safety Systems • Environmental Systems • Tracking Systems • Propellant Management Systems • Health Monitor & Data System • Land/Recovery Systems • Power Systems • Crew Systems *(if manned)* • Ordnance

The RLV operator shall create a RAMT training plan and maintain records that show training received. All records and related activities shall be subject to FAA/AST safety inspection.

Rationale:

RLV aerospace maintenance technicians ensure compliance with safety-critical operations and safety-critical maintenance activities in support of safe RLV operations.

Responsible Party: Reusable Launch Vehicle Operator.

3. **RLV Aerospace Maintenance Inspector (RAMI) - The RAMI responsibilities shall include quality assurance of RLV scheduled and unscheduled maintenance, including interface activities within RLV operator operations and processing plans. The RAMI shall ensure compliance with all of the maintenance requirements developed by the RLV operator.**
The RAMI shall have the following skills and qualifications:
<u>Subject Knowledge</u> (SK)
Understand the requirements, criteria, specifications and policies regarding the vehicle's systems and subsystems
<u>Task Knowledge</u> (TK):
Know the location of and be able to identify and interpret the vehicle's systems and subsystems procedures
<u>Task Performance</u> (TP): Perform vehicle, facilities and housekeeping inspections regarding the vehicle's systems and subsystems
The RLV operator shall create a RAMI training plan and maintain records that show training received. All records and related activities shall be subject to FAA/AST safety inspection.

Rationale:

RLV aerospace maintenance inspectors ensure compliance with safety-critical operations and safety-critical maintenance activities in support of safe RLV operations.

Responsible Party: Reusable Launch Vehicle Operator

4. Mission Safety Organization (MSO) - The MSO supports the Safety Official defined in the RLV Final Rule §431.33. The MSO shall monitor all factors related to the hold or go/no-go decision, execute the functions necessary to ensure public safety and the safety of property during nominal flight and contingency operations. The MSO ensures flight safety system readiness.
Members of the MSO shall have the following skills and qualifications:
<u>Subject Knowledge</u> (SK):
Understand all aspects of the operations with respect to safety of their RLV mission activities

Task Knowledge (TK):
Know the Launch Checklist, Communications and Mission Constraints Document, and Mission Rules Document
Know the Anomaly and Contingency Plan for the overall safety program
Task Performance (TP):
Be responsible for all aspects of the Flight Safety System (FSS)
Examine all aspects of RLV operations, including mission activities, with respect to public safety
Coordinate and provide overall mission safety operations adequate to maintain the required level of public safety
The RLV operator shall create a MSO training plan and maintain records that show training received. All records and related activities shall be subject to FAA/AST safety inspection.

Rationale:

A safety organization of designated individuals to coordinate the performance of safety- related tasks during launch/reentry operations is essential. Efficient coordination between the Mission Safety Organization and the Safety Official provides the appropriate accountability of respective tasks to enable continued mission readiness during launch and re-entry activities.

Responsible Party: Reusable Launch Vehicle Operator.

RLV Operations Preliminary Guidelines

1. Systems Engineering-1 (SYS-1)
The RLV operator shall consider using functional redundancy for safety-critical systems, and where employed shall submit processes and procedures for switching from primary to secondary systems.

Rationale:

Redundant safety critical systems provide an additional level of safety for operations involving RLVs. Although a redundant system might not always lower the severity of a catastrophic event, it does allow an operator to reduce the probability or frequency of occurrence of that event. If employed it may ultimately reduce the overall risk to the public during the conduct of the operator's proposed operations. If redundancy is not employed, the operator shall submit justification for not utilizing redundant safety-critical systems (e.g. a good rationale for not using a redundant system would be that the probability of failure is extremely low).

2. Systems Engineering-2 (SYS-2)
The RLV operator shall perform systems integration testing to verify that each individual subsystem performs as expected and does not produce any unintentional interference with the system as a whole.

Rationale:

In years past, emphasis was placed on equipment design requirements, as the system was considered the sum of the components (equipment). Today, equipment quality has generally improved and manufacturers have become more aware of product safety and liability. Comprehensive industry standards now exist and are used for most apparatus. This is allowing the review emphasis to shift towards a systems approach. Evaluations of equipment should consider overall safety comparability. With today's limited resources for plan review and inspection, concentration should be on proper application of equipment, effect of failures on required system functions, and on vital safety features.

Example: The electrical engineering safety guidelines are a combination of equipment and system requirements designed to ensure that electrical installations are both safe and functional. They consist of general guidelines related to across-the-board "good aerospace practice," and specific requirements related to the various apparatus, their proper design, installation and use. For safety critical power sources and electrical equipment, emphasis should be on evaluating the "system"

- Is the apparatus enclosure appropriate for the location?
- Is the fixture adequately grounded to reduce the shock hazard? -
- Is the fixture enclosure fire retardant and not surrounded by combustibles?
- Will the first upstream over current device safely clear a fault in the fixture so that other parts of the electrical system are not needlessly affected?
- If it is a vital safety system, is the failure indicated and an alternative or back-up provided?
- Do the components go together?

This is the "systems" approach for the electrical subsystem. This does not imply that individual equipment design details are not important, but stresses that where there are limiting constraints, the system should be given a higher priority.

3. Flight Safety System-1 (FSS-1)
The RLV operator shall operate the vehicle such that its explosive potential will be minimized on the ground during any attempted landing, including abort and contingency landings.

Rationale:

Limiting the explosive potential will enable the RLV to land with less risk to the public. The operator should demonstrate how operating procedures minimize explosive potential upon landing, including abort and contingency landings. Explosive potential may be caused by items such as, but not limited to, liquid propellants, solid propellants, pressure vessels, and ordnance. In the event of a vehicle failure that prevents a normal landing, for public safety, the operator should operate the vehicle so that the vehicle has lower explosive potential in the event of an impact with the ground. If a crash of the RLV would be more hazardous to the public with liquid propellants on board, the operator should vent or disperse onboard liquid propellants during flight. Venting propellants will enable the RLV to safely dispose of its fuel and oxidizer in the

event of an anomaly. An FTS system that ruptures the propellant tank(s) may also satisfy this requirement. If the vehicle uses solid rocket motors, they could be jettisoned, if it is feasible and safe to do so. Pressure vessels should be vented, and ordnance should be safed, if practical.
A vehicle that does not overfly populated areas (such as an oceanic flight path) and has no abort-landing capability would not need this capability, as an explosive landing would not increase the risk to the public.

4. Flight Safety System-2 (FSS-2)
The RLV operator's ability to control the location of the instantaneous impact point (IIP) in the event of any credible vehicle failure shall be extremely reliable unless the IIP cannot reach a substantially populated area.

Rationale:

Being able to control the IIP allows the operator to decrease the risk to the public by preventing the vehicle from crashing in a populated area. An example of this is a pilot controlling the flight with a highly-reliable, remotely-operated, backup thrust termination system. Thrust termination provides one means of stopping the movement of the instantaneous impact point.

5. Communications-1 (COM-1)
During launch and reentry, the RLV operator shall transmit valid, verified safety critical data from the RLV to the ground in real-time, when practical. The RLV operator shall record and store data for later transmittal for periods when real-time communication with the ground is not practical.

Rationale:

Safety critical data is used by the launch vehicle operator safety official to monitor the health of the vehicle. Telemetry verifies whether or not the vehicle is operating within approved parameters. In the event of a vehicle failure, a detailed understanding of the state of the vehicle at the time of the failure may be crucial to determine the proper emergency response.

6. Communications-2 (COM-2)
The RLV operator shall ensure the continuous recording of all safety-critical data during all licensed operations. The data recording shall not depend on the vehicle landing safely to retrieve the data.

Rationale:

Licensed operations may include pre-flight hazardous operations and post-flight vehicle safing. Recording data on the ground can assist emergency crews in responding in the event of an emergency. In the event of an anomaly that affects public safety, recorded data will help the licensee prove to AST that they have correctly determined and fixed the cause to the anomaly, thus aiding in their next flight authorization. Recorded data can be replayed to aid in determining what events led to the mishap, thus aiding the mishap investigation team. The Columbia

Accident Investigation Board clearly credits their high confidence of the cause of the accident to finding the data recorder.

7.Communications-3 (COM-3)
The RLV operator shall maintain voice communication among flight crewmembers and between flight crew and ground flight control personnel during all licensed operations.

The sharing of mission-related information via voice communication is vital to the safe operation of the vehicle, especially during off-nominal conditions. Past experience has shown that voice communication between crewmembers and ground flight control personnel greatly enhances operator's ability to respond to emergency situations. Often it is the personnel on the ground that are the first to become aware of developing safety-critical situations, and voice communication is one of many means of conveying this information to the flight crew. It is recognized that the safe sharing of the National Airspace System or NAS resources requires voice communication between vehicles operating in the NAS and between these vehicles and Air Traffic Control.

8. Communications-4 (COM-4)
The RLV operator shall operate the vehicle during all licensed operations such that it can be tracked.

Tracking data will give flight control personnel real time data to monitor the vehicle predetermined trajectory profile and to alert the crew of the RLV, if manned, of the deviation from the mission profile and for corrective action. Such trajectory deviation could induce excessive environmental and loading parameters beyond the design capability of the vehicle, its systems and subsystems which may be catastrophic to crew and public safety. A vehicle sharing the resources of the National Airspace System will have to be tracked by Air Traffic Control (ATC). Title 14 CFR 91.215 provides the requirements for the reporting of altitude for all civil aircraft operating in the airspace. The FAA has determined that all aircrafts, unless otherwise authorized or directed by ATC, operating in the airspace must be equipped with an operable coded radar beacon transponder having capabilities outlined in 14 CFR 91.215.

9. Thermal Protection System-1 (TPS-1)
The RLV operator shall operate the vehicle within the design-heating flight envelope during the entire flight, including ascent and reentry, including a sufficient margin of safety.

The heat load associated with a launch, and in particular a reentry, can be substantial. Failure to protect a vehicle from heating loads can cause a catastrophic failure of the vehicle and a subsequent impact at an unintended, possibly inhabited, location. The operator must determine the flight envelope for the vehicle that ensures no thermal limits are exceeded during a flight including a sufficient margin of safety. The operator should keep the vehicle within this flight envelope to withstand the heat loads during nominal flight and all safe aborts. The operator should justify the margin of safety based on how well the launch environments, reentry environments, and thermal properties of affected materials are known. The margin of safety may vary for different portions of the vehicle based on risk and level of understanding. For example, if a failure of the TPS would result in damage to the vehicle structure that requires substantial repairs but does not jeopardize a safe landing, a smaller margin of safety could be used. If, on the other hand, a failure of the TPS in another section would result in a catastrophic failure of the vehicle, the margin of safety should be higher.

10. Electrical Power System-1 (EPS-1)
The RLV operator shall operate all safety critical power sources and electrical equipment such that it minimizes the risk of fire, explosion, electrostatic discharge or arcing, the emission of toxic gasses and electric shock.

Electrical safety on RLVs includes the prevention of shock, fire and panic. This is to ensure that electrical installations are designed, built and maintained in a manner to promote the safety of the vehicle, and its crew if manned. This is also necessary for safety under both normal and emergency conditions to protect both crewmembers and ground personnel from electrical hazards. While working in or around a metal-hulled RLV, such as during pre-launch and post-reentry phases, or within the vehicle if crewed, a person is usually walking on or touching ground at all times, and is usually within reach of power cables or electrical equipment in the vehicle containing lethal voltages. Currents that can flow from an energized conductor to ground can be very large, even in an ungrounded system; yet currents as low as twenty-five thousandths of an ampere (25 milliamps) that pass through the heart can cause death. A fire hazard can also exist wherever such electrical potential is present, and on an RLV, the electrical installation covers a far greater area than any other type of installation. The threat exists whenever the protective insulation of a wire or cable is damaged by heat, moisture, oils, corrosive materials, vibration, abrasion, or impact, or where faulty installation or operating conditions result in loose connections.

11. Electrical Power System-2 (EPS-2)
The RLV operator shall operate the vehicle such that the capacity of the power sources are sufficient for operations beyond normal mission time to include all credible contingency and emergency abort scenarios.

Rationale:

Once committed to flight, the RLV needs enough power to fulfill entire mission in the event of primary power source failure, including margin for credible contingency and emergency abort scenarios. It is not the intent of this guideline that any secondary power source for an RLV merely act as a mission reserve – ensuring only that, once committed to flight, the craft can continue on its nominal mission to perform a commercial function – from lift-off to landing, <u>but</u> to handle any emergency contingency scenarios as well as the primary power source would. For example, having a secondary power source will help mitigate the hazard of an uncontrolled vehicle landing.
The emergency loads should be supplied by the secondary or emergency power source(s). Additional safety devices and systems (i.e., critical) may be connected to the emergency power system provided the emergency source is sized to supply these loads at 100% load factor. Additional loads which are intended to improve the safety or survivability of the RLV in certain operating modes (i.e., non-critical) and which have not been considered in sizing the emergency

source (such as the addition of a secondary propulsion system), may be allowed to be connected to the emergency power supply when arranged to be functionally equivalent to a bus-tie - configuration.
Independency should also extend to physical placement. The compartments or other placement arrangements for the primary source and the secondary or emergency power source should not be adjoining, except where other arrangement is not practicable. The intent is to maintain the integrity of the emergency electrical distribution system if there is a fire, air or fluid leak, or other casualty in the location of the main power source. When the arrangement to physically separate has been shown to be impractical, the installation of bulkhead between the emergency primary sources may be acceptable. It is preferable to avoid any continuous boundaries between the location of a secondary/emergency power source and any primary power source location or a location containing the main source of electrical power's associated transforming equipment, if any, and the main switchboard.

12. Structures-1 (STR-1)
The RLV operator shall operate the vehicle within its structural design envelope, including approved factors of safety, safety margins, and maximum operating loads including credible contingency abort modes for which the RLV was designed.

The principal function of the structure is to protect the crew and vehicle components from the external environment. Some structural components include, but are not limited to, intertanks, fuselage, wings/control surfaces, engines thrust structure, payload bay and doors and the pressurized crew compartment. The vehicle structure should be designed to preclude failure by use of adequate design safety factors, relief provisions, or safe life and/or safe life characteristics. The vehicle manufacturer should establish a set of operational flight parameters and envelopes, and provide them to the RLV operator, that provide a margin of safety to greatest extent possible.

13. Propulsion-1 (PROP-1)
The RLV operator shall operate the vehicle such that the vehicle's safety-critical propulsion parameters such as quantity, pressure, temperatures, and flow rates are monitored and maintained within acceptable limits.

Rationale:

The safe operation of the propulsion system is normally verified by analysis involving the monitored parameters. Unsafe trends can be predicted from monitoring the propulsion performance and lead to a reconfiguration or malfunction procedures that result in a safe configuration prior to reaching a catastrophic condition.