# Guide to Commercial Reusable Launch Vehicle Operations and Maintenance

**Federal Aviation Administration**
Office of Commercial Space Transportation
800 Independence Avenue, Room 331
Washington, DC 20591

# Guide to Commercial Reusable Launch Vehicle Operations and Maintenance

# Version 1.0

March 2005

**Federal Aviation Administration**
Office of Commercial Space Transportation
800 Independence Avenue, Room 331
Washington, DC 20591

## TABLE OF CONTENTS

## 1. Introduction

With the enactment of the Commercial Space Launch Act of 1998, the Department of Transportation, Federal Aviation Administration, (DOT/FAA) was given statutory authority to regulate reentry and reusable launch vehicle (RLV) activities. The DOT/FAA recognized that RLVs would require operations and maintenance safety criteria and standards to ensure that public safety was maintained at an acceptable level. Unlike expendable launch vehicles (ELVs), which are only flown once, RLVs are intended to be flown repeatedly by the RLV operator. The DOT/FAA must ensure that the RLV operator has procedures and processes that return an RLV to a safe condition for reflight. In 1999 the FAA, Associate Administrator for Commercial Space Transportation (AST), developed a White Paper on Commercial RLV Operations and Maintenance Considerations and submitted it to the Commercial Space Transportation Advisory Committee (COMSTAC) RLV Working Group for comments. In addition, the FAA/AST has used an outside contractor, RTI International, to help inform the process of developing RLV Operations and Maintenance guidance. The DOT/FAA developed and published a Final Rule on Commercial Space Transportation Reusable Launch Vehicle and Reentry Licensing Regulations on September 19, 2000, with an effective date of November 20, 2000. This Final Rule addressed operational flight restrictions, but it did not provide regulations for maintenance of an RLV. The preamble to this Final Rule stated that several commentators pointed out the need to begin addressing, through regulations the need for operations and maintenance standards that will facilitate reflight approval. In May 2003, the FAA/AST published Draft Guidelines for Commercial Reusable Launch Vehicle Operations and Maintenance and asked the COMSTAC RLV Working Group for comments. Taking into consideration these comments, the FAA/AST revised the Draft Guidelines and published Preliminary Guidelines for Commercial Reusable Launch Vehicle Operations and Maintenance in July 2004. The FAA/AST asked the COMSTAC RLV Working Group for comments and received consensus comments to the Preliminary Guidelines. These consensus comments were very helpful in compiling this guide.

## 2. Purpose

This guide was developed to provide industry with insight into what the DOT/FAA views as important considerations for operations and maintenance of RLVs. It also addresses what the FAA/AST may expect to review and evaluate in an application for a license or permit[1] concerning RLV operations and maintenance.

[1] Under the Commercial Space Launch Amendments Act (CSLAA) of 2004, a person may apply for an experimental permit for reusable suborbital rockets only for purposes of research and development to test new design concepts, equipment, or operating techniques; showing compliance with regulatory requirements; and crew training prior to obtaining a license. The DOT/FAA must decide whether to issue a permit within 120 days after receipt of a permit application, compared to 180 days, which is the time the DOT/FAA has to make a licensing determination.

## 3. Scope

This guide addresses RLV operations and maintenance for both suborbital and orbital RLVs, including flights with and without humans onboard. Although developers may find the information in this document helpful, many years of RLV flight experience are required before an appropriate set of regulations for RLV operations and maintenance can be developed.

## 4. Applicability

The information in this guide applies to any RLV operator licensed or permitted under 49 U.S.C. Chapter 701. FAA/AST recognizes the commercial RLV industry is in its infancy and believes that the guidance in this document represents reasonable and appropriate practices that will ensure public safety.

## 5. Definitions

| | |
|---|---|
| Crew | Any employee of a licensee or transferee, or of a contractor or subcontractor of a licensee or transferee, who performs activities in the course of that employment directly relating to the launch, reentry, or other operation of or in a launch vehicle or reentry vehicle that carries human beings. [49 U.S.C. § 70102(2)] |
| Flight crew | Any employee of a licensee or transferee, or of a contractor or subcontractor of a licensee or transferee, who is onboard a launch or reentry vehicle and performs activities in the course of that employment directly relating to the launch, reentry, or other operation of the launch vehicle or reentry vehicle.[2] |
| Space flight participant | An individual, who is not crew, carried within a launch vehicle or reentry vehicle. [49 U.S.C. §70102(17)] |
| Suborbital rocket | A vehicle, rocket-propelled in whole or in part, intended for flight on a suborbital trajectory, and the thrust of which is greater than its lift for the majority of the rocket-powered portion of its ascent. [49 U.S.C. §70102(19)] |
| Suborbital trajectory | The intentional flight path of a launch vehicle, reentry vehicle, or any portion thereof, whose vacuum |

[2] Because the CSLAA does not distinguish between ground crew and crew onboard a vehicle, the FAA/AST guidelines use the term "flight crew" to identify the crew onboard a vehicle.

instantaneous impact point does not leave the surface of the Earth. [49 U.S.C. §70102(20)]

## 6. RLV Maintenance

**6.1. The applicant should have a maintenance program plan to facilitate maintenance and repair actions in the anticipated RLV operation 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:* Having a maintenance program plan can help to assure continuous flightworthiness of RLVs. The maintenance program plan should include scheduled and unscheduled maintenance. 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. It 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.

**6.2. A recommended maintenance program plan should include the following items:**

- **Locations and facilities where maintenance will be accomplished.**
- **Level of components, such as systems and subsystems, that will be maintained.**
- **Storage plan for spare parts, materials, and all limited shelf life components, to the extent practical.**

*Rationale:* Identifying the locations and facilities where maintenance will be accomplished allows an evaluation to be made of the adequacy of such facilities and locations for a given maintenance operation. Conducting maintenance operation without affecting public safety is important. 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. In addition, the location and facilities need to meet the appropriate requirements for that maintenance operation. For example, if a facility lacks the necessary Ground Support Equipment to perform maintenance in a safe manner, public safety could be compromised if an accident occurs. Determining the level at which component maintenance will be performed is also important. Finally, the use of a storage plan for limited shelf life items provides a way to document and inspect the usability of such items. At the outset of a program, the storage plan may be rudimentary. This plan should be expanded as operational experience shows what parts and subsystems are consumed and what failure rates are experienced.

**6.3. A maintenance plan should 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 to the extent practical.**

*Rationale:* Providing a list of tasks to be performed will enable a reviewer to identify 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 the necessary hazard controls are in place. 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 is serviced or replaced. The frequency of maintenance is also an important inspection tool to make sure failures do not occur.

Preventive maintenance ensures 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. Specifying the numbers and 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 expected to perform maintenance tasks according to standard industry practice. For example, have an inspector approve safety-critical maintenance and document it. 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.

Specifying tools and test equipment is also an important part of 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. If special tools are used, 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. Establishing plans for such items as maintenance, schedule, and spare parts may be a long, slow process, and these plans should be modified as more data is gathered and more flights are attempted. However, vehicle operators should have an understanding of their vehicle systems and subsystems that require maintenance, and thus the spare parts required to maintain such systems and subsystems (e.g. through bench testing, engineering tests, etc.).

**6.4. The applicant should develop and implement a system that will identify, track, and report problems related to maintenance activities of flight hardware and software, if any. The applicant should establish a data collection system that can be**

**used to identify failure trends and to communicate "lessons learned" from maintenance experience.**

*Rationale:* Because of the nascent nature of the RLV industry, data collection is imperative to determine adequate inspection periods and identify which parts, subsystems, or both, require maintenance to ensure public safety. The data can also be used to adjust the maintenance program plan based on lessons learned.

**6.5. If subcontractors are used, the applicant should develop appropriate maintenance requirements to impose on each subcontractor. The applicant should have continuous or periodic review, inspection, and assessment to assure that each subcontractor is implementing its maintenance program effectively.**

*Rationale:* Regardless of who performs the maintenance, the operator is ultimately responsible to ensure that the work is accomplished in a way that ensures public safety. The operator is liable for any damages resulting from improper maintenance.

**6.6. The applicant should have a Configuration Management System (CMS) to ensure that flight configuration correlates to a known, tested configuration of parts, systems, subsystems, and software.**

*Rationale:* Use of a CMS contributes to public safety by helping to ensure that the correct parts are used for each configuration and preventing the use of unauthorized parts or components. In addition, a CMS ensures traceability of the part or component and facilitates tracking items 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. The CMS may be rudimentary during the initial development stages of an RLV program, but this system should become increasingly formal and extensive as the RLV program matures.

**6.7. The applicant should have an inspection schedule. This schedule should include the items to be inspected and specify the periodicity of the inspections. As the applicant gains experience, the inspection schedule should be updated to reflect actual experience.**

*Rationale:* Because 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, subsystems, and systems, the applicant should update its inspection schedule. An up-to-date inspection schedule will ensure that the applicant has a well-documented inspection plan based on the design and operation of the RLV that contributes to public safety and meets the operational needs of the RLV developer.

## 7. RLV Support Personnel

*General Notes:*

- *One person may perform more than one task/responsibility concurrently.*
- *These positions are hypothetical and fulfill the functions of an RLV operations and maintenance program.*

### 7.1. Training Plan

**The RLV operator should create a support personnel training plan and maintain records that show training received.**

*Rationale:* Implementation of a training plan for RLV support personnel is critical for making effective RLV operations and maintenance public safety-related decisions.

### 7.2. RLV Aerospace Maintenance Technician (RAMT)

**The RAMT should be familiar with and demonstrate practical and hands-on knowledge of system and subsystem functions and operational tests that relate to the operations and maintenance of particular vehicles. The RAMT should demonstrate proficiency in each system or subsystem of the vehicle if that system or subsystem is used in the vehicle or support equipment. Each system and subsystem RAMT should be identified by name and should have the following skills and qualifications for his/her system or subsystem:**

**<u>Subject Knowledge</u>**
**Understand the function and operation of the applicable system or subsystem.**

**<u>Task Knowledge</u>**
**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.**

**<u>Task Performance</u>**
**Perform and complete maintenance tasks.**

**The RLV operator may use one or any combination of the following programs and models for RAMT approval during its rating assessment process:**

- **FAA Airframe, Power Plant Mechanic, or both, certification programs.**
- **SpaceTEC Aerospace Technician Certification program.**
- **Automotive Service Excellence Certification model.**

*Rationale:* RLV Aerospace Maintenance Technicians ensure compliance with safety-critical operations and safety-critical maintenance activities in support of safe RLV operations.

**7.3. RLV Aerospace Maintenance Inspector (RAMI)**

**The RAMI responsibilities should include quality assurance of RLV scheduled and unscheduled maintenance, including interface activities within RLV operator operations and processing plans. The RAMI should ensure compliance with all of the maintenance requirements developed by the RLV operator. The RAMI should have the following skills and qualifications:**

**Subject Knowledge**
**Understand the requirements, criteria, specifications, and policies regarding the vehicle systems and subsystems.**

**Task Knowledge**
**Know the location of and be able to identify and interpret the vehicle's systems and subsystems procedures.**

**Task Performance**
**Perform vehicle, facilities, and housekeeping inspections regarding the vehicle's systems and subsystems.**

*Rationale:* The RAMI ensures compliance with safety-critical operations and maintenance activities in support of safe RLV operations.

**7.4. Vehicle Mission Coordinator (VMC)**

**The VMC is the mission planner. His or her responsibilities include**

- **Defining and filing mission profiles.**
- **Collaborating with the responsible air traffic authority (FAA or DoD) having jurisdiction over the area of intended use.**
- **Coordinating with the launch site operator (LSO).**
- **Having the subject knowledge of the FAA air traffic control rules, regulations, and operational requirements.**
- **Understanding the operational limitations, restrictions, and capabilities of the space vehicle and the launch and reentry operations and their associated regulatory requirements.**
- **Having task knowledge of notification procedures and processes.**

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

## 8. RLV Operations

### 8.1. Flight Safety System-1

**The RLV operator should operate the vehicle such that its explosive potential on the ground will be minimized, consistent with safe vehicle operations, during any attempted landing, including aborts and contingency landings.**

*Rationale:* Limiting the explosive potential may enable the RLV to land with less risk to the public. The operator should demonstrate how operating procedures minimize explosive potential upon landing, including aborts and contingency landings. Explosive potential may be caused by such items as liquid propellants, solid propellants, pressure vessels, and ordnance. If a vehicle failure prevents a normal landing, the operator should operate the vehicle so that, if possible, the vehicle has low 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 onboard, the operator should vent or disperse onboard liquid propellants during flight. Venting propellants may enable the RLV to safely dispose of its fuel and oxidizer in the event of an anomaly. A Flight Termination System that ruptures the propellant tanks may also be considered as another approach. 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 because an explosive landing would not increase the risk to the public.

Note that if a vehicle is designed to have a powered landing, then the RLV operator is not required to empty the fuel tanks before landing. Safe vehicle operation requires sufficient fuel for a powered landing.

### 8.2. Flight Safety System-2

**The RLV operator's ability to control the location of the instantaneous impact point (IIP) should be extremely reliable unless the IIP cannot reach a densely 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 IIP.

### 8.3. Communications-1

**During launch and reentry, the RLV operator should transmit valid, verified safety-critical data from the RLV to the ground in real-time when practical. The RLV**

**operator should record and store data for later transmittal for periods when real-time communication with the ground is not practical.**

*Rationale:* The launch vehicle operator's safety official uses safety critical data 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.

**8.4. Communications-2**

**The RLV operator should ensure the continuous recording of safety-critical data during licensed operations. The data recording should not depend on the vehicle landing safely to retrieve the data.**

*Rationale:* Licensed operations may include preflight hazardous operations and post-flight vehicle safing. Recording data on the ground can assist emergency crews in responding if an emergency occurs. In the event of an anomaly that affects public safety, recorded data may help the licensee prove that the cause has been correctly determined and fixed**,** thus aiding in obtaining the 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 the high level of confidence regarding the cause of the accident to finding the data recorder.

**8.5. Communications-3**

**The RLV operator should maintain voice communication among flight crew, ground flight control personnel, and air traffic control during licensed operations.**

*Rationale:* The sharing of mission-related information via voice communication is vital to the safe operation of the vehicle, especially during off-nominal conditions. Experience has shown that voice communication between crew and ground flight control personnel greatly enhances the operator's ability to respond to emergency situations. Often, personnel on the ground are the first to become aware of developing safety-critical situations. Voice communication is one of many means of conveying this information to the flight crew. Voice communication should be maintained between the flight crew and the responsible air traffic authority (FAA or DoD) to ensure safe operations during a mission.

**8.6. Communications-4**

**The RLV operator should operate the vehicle during licensed operations such that it can be tracked.**

*Rationale:* 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 parameters of the vehicle. In addition, a vehicle sharing the resources of the NAS will have to be tracked by the FAA/ATO. Title 14 C.F.R. 91.215 provides the requirements for the reporting of altitude for all civil aircraft operating in the airspace. Unless otherwise authorized or directed by FAA/ATO, aircraft operating in the NAS must be equipped with an operable coded radar beacon transponder having capabilities outlined in 14 C.F.R. 91.215.

**8.7. Thermal Protection System-1**

**The RLV operator should operate the vehicle within the design-heating flight envelope during the entire flight, including ascent and reentry, including a sufficient margin of safety.**

*Rationale:* Heat loads 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. 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 thermal protection system 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 thermal protection system in another section would result in a catastrophic failure of the vehicle, the margin of safety should be higher.

**8.8. Electrical Power System-1**

**The RLV operator should operate all safety-critical power sources and electrical equipment such that it minimizes the risk of fire, explosion, electrostatic discharge or arcing, emission of toxic gasses, and electric shock.**

*Rationale:* Electrical safety on RLVs includes the prevention of shock, fire, and panic. This prevention is to ensure that electrical installations are designed, built, and maintained in a manner to promote the safety of the vehicle and any humans who come in contact with the vehicle. This prevention is also necessary for safety under normal and emergency conditions to protect flight crew, ground crew, and space flight participants from electrical hazards. For instance, while working in or around a metal-hulled RLV during prelaunch and post-reentry phases a person is usually walking on or touching the ground at all times. In addition, the person 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 even very low currents that pass through the heart can cause death. A fire hazard can also exist wherever such electrical potential is present. The threat exists when 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.

**8.9. Electrical Power System-2**

**The RLV operator should 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 complete the entire mission, including a margin for credible contingency and emergency abort scenarios. In most cases, the RLV operator pursues a contingency or emergency abort scenario because of an anomaly. If the primary power source is not sized to accommodate contingency and emergency abort scenarios, then an additional risk may be posed by complications to the anomaly introduced by switching from a primary to a backup or secondary power system. Power sources considered for an RLV should be sized to handle not only the nominal mission but also any emergency contingency scenarios.

It is not the intended that all RLVs have both a primary source and a secondary power source at all times. The need for two power sources would depend on the specific vehicle and its operation. However, a secondary power source should function with the same capacity as the primary power source rather than merely act as a mission reserve.

**8.10. Structures-1**

**The RLV operator should not operate the vehicle beyond its analytically determined structural failure point, consistent with ensuring public safety.**

*Rationale:* The principal function of the structure is to protect the inhabitants and components of the vehicle from the external environment. Some structural components include, but are not limited to, intertanks, fuselage, wings and control surfaces, engine thrust structures, payload bays and doors, and pressurized crew compartments. The vehicle structure should be designed to preclude failure by use of adequate design safety factors, relief provisions, and safe life characteristics. The vehicle manufacturer should establish a set of operational flight parameters and envelopes which will allow the vehicle not to exceed its structural failure points.

**8.11. Propulsion-1**

**The RLV operator should operate the vehicle such that safety-critical propulsion parameters, if any, are monitored and maintained within acceptable limits.**

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

**8.12. Systems Engineering-1**

**The RLV operator should consider using functional redundancy for safety-critical systems, and where employed, should have 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 reduce the severity of a catastrophic event, such systems allow an operator to reduce the probability or frequency of occurrence of that event. If employed, redundancy 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 should have justification for not using redundant safety-critical systems. For example, a good rationale for not using a redundant system would be that the probability of failure is extremely low.

When implementing redundancy, designers should strive for independency. Independency should also extend to physical placement. For instance, the primary and secondary systems should not be placed in adjoining locations unless other arrangements are not practical. The intent is to maintain the integrity of that system if a problem occurs in the physical location of one of the systems. When physically separating the primary and secondary systems proves impractical, installation of a bulkhead between the two systems may be acceptable.

**8.13. Systems Engineering-2**

**The RLV operator should perform systems integration testing to verify that individual subsystems perform as expected and do not produce unintentional interference with the system as a whole.**

*Rationale:* In the past, emphasis was placed on equipment design requirements because 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 nearly all apparatus. This change allows the review emphasis to shift toward a systems engineering approach. Evaluations of equipment should consider overall safety comparability. With today's limited resources for plan review and inspection, concentration should focus on proper application of equipment, affect of subsystem failures on required system functions, and vital safety features.

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

- 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 subsystem are not affected?
- Is the failure indicated and an alternative or back-up provided if it is a vital safety system?
- Do the components go together?

This example shows how a systems engineering approach can be used for the electrical subsystem. It does not imply that individual equipment design details are not important, but rather that where there are limiting constraints, an assessment of the performance of the overall system should also be given a high priority.