CONTRACT NAS9-12004
DRL NO. 3

MSC-04477
SD 72-SA-0094-4

FINAL REPORT

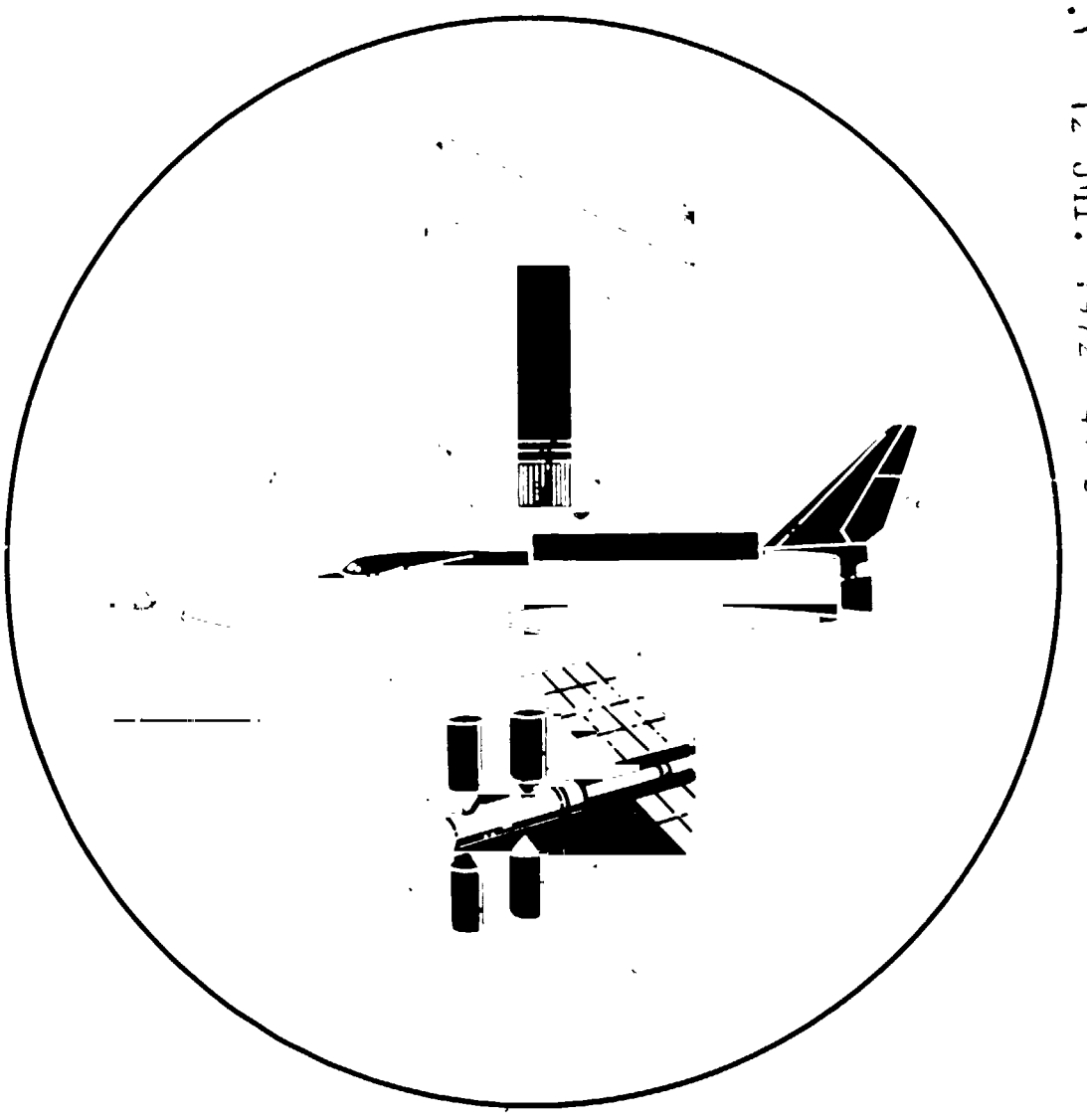
CR-128510

Safety in Earth Orbit Study

Volume IV – Space Shuttle Orbiter

Safety Requirements and Guidelines

On-Orbit Phase



JULY 12, 1972

Space Division
North American Rockwell

12214 Lakewood Boulevard Downey, California 90241

MSC-04477
SD 72-SA-0094-4

FINAL REPORT

Volume IV

Space Shuttle Orbiter

Safety Requirements and Guidelines

On-Orbit Phase

Safety in Earth Orbit Study

JULY 12, 1972

Contract NAS9-12004

Approved by

G. S. Canetti
Study Manager

Space Division
North American Rockwell

Space Division
North American Rockwell

PRECEDING PAGE BLANK NOT FILMED

FOREWORD

Final documentation of the Safety in Earth Orbit Study is submitted by the Space Division of North American Rockwell Corporation to the National Aeronautics and Space Administration, Manned Spacecraft Center, Houston, Texas, in compliance with DRL Line Items 3 and 4 of NASA-MSC Contract NAS9-12004.

The 12-month study was performed for the NASA Manned Spacecraft Center by the Space Applications Programs organization at the Space Division of North American Rockwell. Mr. P. E. Westerfield of the Safety Office was the NASA technical manager.

Documentation of the study results is as shown in the following table.

DRL Line Item	Title	NR-SD Report No.
4	Contract Summary	SD 72-SA-0095
3	Final Report	
	Volume I - Technical Summary	SD 72-SA-0094-1
	Volume II - Analysis of: Hazardous Payloads Docking On-Board Survivability	SD 72-SA-0094-2
	Volume III - Analysis of: Tumbling Spacecraft Escape and Rescue	SD 72-SA-0094-3
	Volume IV - Space Shuttle Orbiter Safety Requirements and Guidelines On-Orbit Phase	SD 72-SA-0094-4
	Volume V - Space Shuttle Payloads Safety Requirements and Guidelines On-Orbit Phase	SD 72-SA-0094-5

ACKNOWLEDGMENTS

The guidance of Mr. P. E. Westerfield, the NASA technical manager, is gratefully acknowledged. His efforts were directed constantly at helping the study team to improve the quality of the study.

The comments, always constructive, of Mr. H. Schaefer, NASA Headquarters, and of Mrs. R. N. Weltmann, Lewis Research Center, also significantly improved the quality and readability of the study outputs.

Personnel at North American Rockwell who participated in the study are:

All tasks	-	R. E. Altenbach
Hazardous Payloads	-	L. K. Relyea
Docking	-	G. O. Mount, Jr.
On-board Survivability	-	B. L. Felmet J. W. Patrick
Tumbling Spacecraft	-	A. Cormack III A. N. Moore B. U. Mahr
Escape and Rescue	-	C. N. Harshbarger B. U. Mahr

PRECEDING PAGE BLANK NOT FILMED

CONTENTS

1.0 INTRODUCTION

This volume of the final report contains a listing of the safety requirements and guidelines for the space shuttle orbiter generated during the study. Similar requirements and guidelines for space shuttle payloads, including the space station, are contained in Volume V. These volumes are intended for use in performance specifications in Phases C and D of these programs.

The requirements and guidelines presented here are specific to the hazards and emergencies analyzed in the study tasks, and must not be interpreted as a complete list of safety requirements and guidelines for the various programs. It is hoped, however, that these volumes can be amplified as further safety studies are performed, so that eventually they will represent a complete system safety specification, covering the safety aspects of all mission phases of each vehicle.

The requirements and guidelines are listed in two sections. Section 3.0 contains the requirements and guidelines which must be implemented on the shuttle (specifically, the shuttle orbiter, since the study covers safety in earth orbit only). Section 4.0 contains the interface safety requirements and guidelines with the space station, upper stage vehicles and sortie payloads; i.e., the requirements and guidelines which must be imposed on those vehicles in order to ensure the safety of the shuttle orbiter. The inclusion of a requirement or guideline for a particular vehicle, say the orbiter, must not be taken as a decision that the requirement or guideline must be implemented by that particular program (the shuttle orbiter in this case), or charged to that program. It indicates that the provisions will physically be implemented on that vehicle.

The source of these requirements and guidelines is Appendix B of Volume II of this report, which contains the hazard/emergency analyses performed during the study. The wording of each requirement or guideline recommended in that volume is used verbatim in this volume. A minor exception occurs in a few cases when two or three practically identical statements in the hazard/emergency analyses (e.g., one dealing with flammable, toxic and corrosive fluids) are combined into one statement (dealing with flammable, toxic, or corrosive fluids). Traceability to the hazard/emergency analysis of Appendix B of Volume II is provided for each requirement and guideline through two letters and a number or number/letter combination (e.g., RP-1.2.004 or GD-1.b) shown in parentheses after each requirement and guideline. This numbering system, as well as the definitions and format used, are described in the following sections. These are consistent with the definitions and methodology used in performing the hazard/emergency analyses.

Section 5.0 discusses the rationale for the requirements and guidelines in this volume. A second parenthesis after certain requirements and guidelines indicates a cross-reference to the rationale in Section 5.0.

1.1 REQUIREMENTS AND GUIDELINES

The first letter in the parentheses after each requirement and guideline indicates whether it is a requirement (R) or a guideline (G).

The difference between a requirement and a guideline is as follows:

- o A requirement (R) is regarded as a "must implement" item from the safety point of view. It eliminates an appreciable element of risk from the total spectrum of risks associated with the particular hazard or emergency. If recommended, a requirement is therefore not considered as an item to be rejected for cost, weight or similar reasons, since it significantly impacts safety.

- o A guideline (G) is regarded as a "strongly recommended" item from the safety point of view. It does not eliminate any appreciable element of risk, although it may reduce the occurrence or the resulting effects of the hazard. The increase in safety from a guideline in certain circumstances may not be commensurate with the penalties of implementing it, and therefore it may be traded off against cost, weight, etc. There is, in all cases, a safety penalty (in the form of exposure to some additional risk) whenever a guideline is not implemented, and this must be recognized whenever such a decision is taken.

The requirements and guidelines which were generated were carefully worded so as to satisfy three criteria that were considered very important. These criteria are that the requirements and guidelines should:

(a) Be verifiable -- i.e., it should be possible to unambiguously verify whether each requirement or guideline has been met in the design or in the planned operations. Ambiguous or non-verifiable words such as "to the maximum extent possible" or "adequate" have therefore been avoided.

(b) Meet the mathematician's "necessary but sufficient" criterion -- i.e., they should specify every condition that must be met to satisfy the safety objective, but they should not specify more than is required for safety. The latter point is particularly important since the tendency is to select particular design or operational solutions which restrict the designer's choice, rather than stating only the requirement in general terms.

(c) Be written in precise and unambiguous language, suitable for incorporation into preliminary requirements specifications for Phases B or C.

1.2 REMEDIAL OR PREVENTIVE

The second letter in the parentheses after each requirement or guideline indicates whether this particular requirement or guideline contributes toward

preventing (P) the hazard/emergency, or toward remedying (R) the situation after the hazard or emergency has occurred. This does not refer to whether or not the requirement or guideline prevents injury or damage following the occurrence of the hazard or emergency.

1.3 HAZARD/EMERGENCY ANALYSIS

The particular hazard/emergency analysis or analyses which originated each particular requirement or guideline, is identified by the number or number/letter combination in the parentheses following each requirement or guideline. The reference is to Volume II of this report, Hazard/Emergency Analyses. The hazard/emergency analyses are listed in numerical order in that volume. A letter, such as in 1.B, indicates that the requirement or guideline appears in more than one hazard/emergency analysis; such requirements and guidelines are listed alphabetically by the identifying letter in Volume II at the beginning of each section.

1.4 HAZARD REDUCTION PRECEDENCE SEQUENCE

The requirements and guidelines were developed in the hazard/emergency analyses by using the hazard reduction sequence of OMSF Safety Project Directive SPD-1A. The sequence is explained in Volume II, Hazard/Emergency Analyses, in which it is used. The resulting requirements and guidelines fall into four categories as a result of this, and they are grouped together in this volume into four sections, as follows:

3.1 Design Requirements and Guidelines
3.2 Safety Devices
3.3 Warning Devices
3.4 Operational Procedures

The four sections correspond to the first four steps (Numbers 1-4) on the hazard reduction precedence sequence (see Volume II). Each of the above four sections therefore contains all the requirements and guidelines which satisfy each of the four hazard reduction precedence sequence steps, as identified against each requirement and guideline in the hazard/emergency analyses in Volume II.

The interface requirements and guidelines, in Section 4.0 of this volume, have not been separated into this sequence because of their relatively small numbers.

1.5 RESIDUAL HAZARDS

The last step of the hazard reduction precedence sequence (No. 5) calls for the identification of a particular hazard as a residual hazard. This occurs when injury or loss of personnel or damage to or loss of equipment is still possible from this hazard or emergency even when the recommended requirements and guidelines have been implemented.

Residual hazards were identified in the hazard/emergency analyses in Volume II. These are listed in Section 3.5 of this volume as applicable to the shuttle orbiter. The number in parentheses identified the hazard/emergency analysis in Volume II.

Some residual hazards are designated as acceptable risks. These are hazards or emergencies in which the risk, after implementing the recommended requirements and guidelines, is small enough that no further action is considered necessary.

Other residual hazards are labeled with the term SRT Requirements. This means that Supporting Research and Technology (SRT) requirements have been identified to aid in resolving these hazards. These SRT requirements are described in Volume II.

The remaining residual hazards are designated as unresolved safety issues. These are hazards or emergencies for which the residual risk (after implementing the recommended requirements and guidelines) is not acceptable, and for which no adequate means for resolving the issue (such as defining supporting research and technology requirements) has been identified.

Residual hazards which were identified as acceptable risks and as residual safety issues in the hazard/emergency analyses (Volume II) are identified as such in Section 3.5.

It is suggested that procedures should be set up in the course of a program for the periodic review of residual hazards. Different levels of management should be involved, with the lowest level reviewing the acceptable risks, and the unresolved safety issues being exposed to the highest management level.

2.0 BASELINE MODEL

The baseline model considered in the analyses included the vehicles shown in Figure 1.

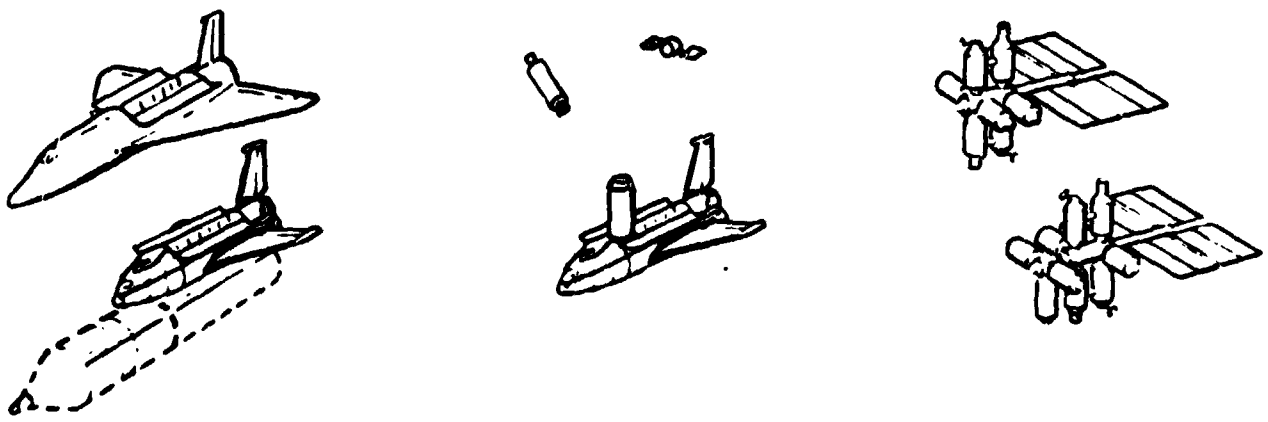


Figure 1. Vehicles Considered

Initial analysis was based on the integral tank shuttle orbiter, but emphasis was later switched to the drop tank orbiter as this concept developed. The assumptions made were broad enough that no results were invalidated this change.

Shuttle payloads considered included manned and unmanned sortie payloads (i.e., attached to the orbiter), satellites delivered to earth orbit, and potential upper stage vehicles used to deliver unmanned payloads to orbits beyond the orbiter's capabilities.

Upper stage vehicles specifically considered included the following:

- Agena
- Centaur
- Transtage
- Burner II
- Apollo Service Module
- Orbit-to-Orbit Shuttle (OOS)/Tug

These were considered as typical of potential upper stage vehicles in order to identify potential hazards. They were only considered as they operated in or near the orbiter while in earth orbit.

A typical shuttle mission, generated from NR Phase B shuttle data, is shown in Fig. 2. The boxed area shows the mission phases considered in the study. Only potential hazards occurring in these on-orbit phases have been considered. Sortie modules, satellites and upper stage vehicles were considered and hazards identified only while these vehicles were transported in orbit, deployed and retrieved by the orbiter, or operated in the vicinity of the orbiter.

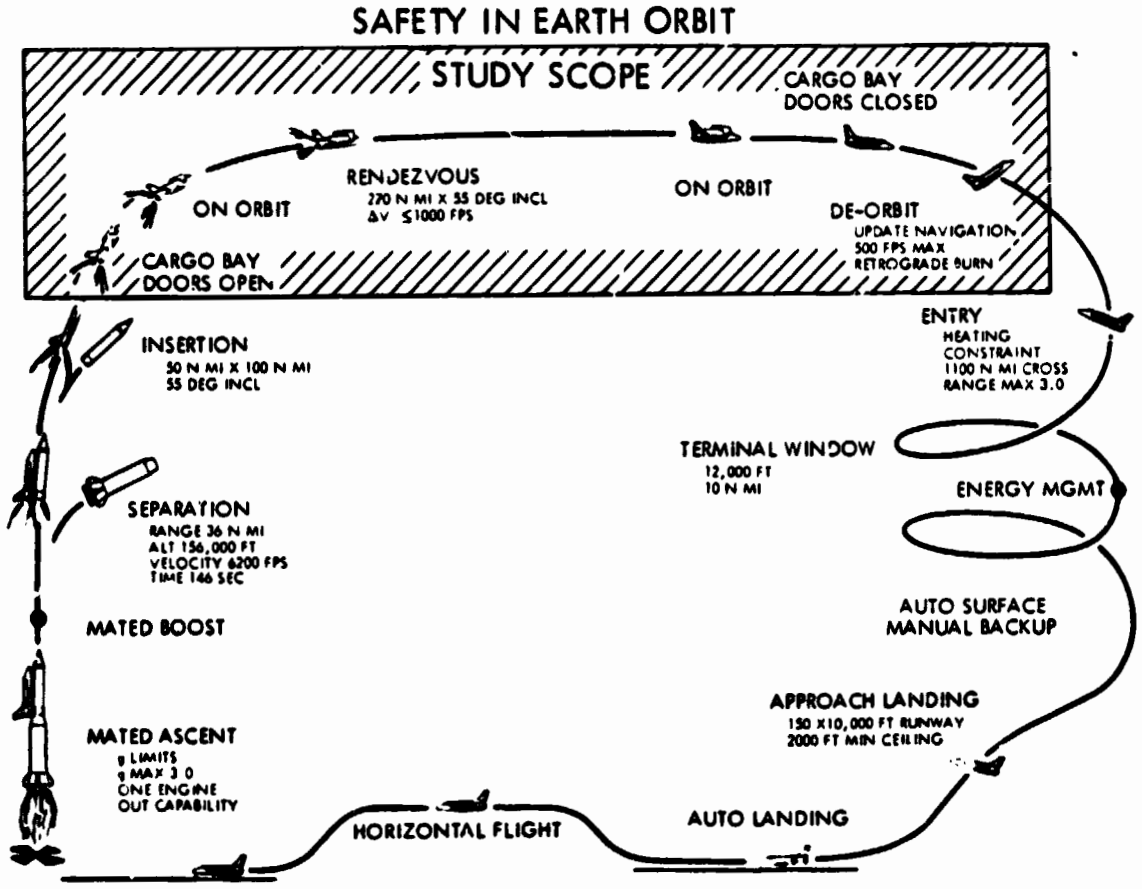


Figure 2. Typical Shuttle Mission

The space stations considered were modular stations delivered to earth orbit and assembled by the orbiter. Initial 6-man versions and growth versions with up to 12 men, as defined in recent Phase B studies, were studied. Assembly of the space station, independent operation in earth orbit, and normal resupply by the orbiter were considered.

3.0 SAFETY REQUIREMENTS AND GUIDELINES

This section contains safety requirements and guidelines developed from analyses of specific safety issues. The requirements and guidelines are grouped into five sub-sections, corresponding to the five steps of the hazard reduction precedence sequence. These five sub-sections are:

3.1 Design Requirements and Guidelines
3.2 Safety Devices
3.3 Warning Devices
3.4 Operational Procedures
3.5 Residual Hazards

3.1 DESIGN REQUIREMENTS AND GUIDELINES

Hazardous Payloads

3.1.1 Shuttle hardware required for abort shall be located remotely from the cargo bay, or protected against the potential effects of upper stage vehicle explosions which would not cause primary shuttle structure failure. (RR-1.J, 1.1.001) (5.1)

3.1.2 Always-open cargo bay vents to space shall be provided on the shuttle which limit internal cargo bay pressures from upper stage vehicle leakage to the cargo bay allowable limits. (RR-1.K, 1.1.001) (5.2)

3.1.3 Capability shall be provided on the shuttle for automatic cargo bay venting when the always-open vents are inadequate, in order to increase the allowable flow from inside to outside and to protect against re-entry ingestion through always-open vents. (GR-1.L, 1.1.001) (5.2)

3.1.4 All shuttle hardware contained in and near the shuttle cargo bay shall be capable of being functionally isolated from those components necessary for de-orbit, re-entry and landing so that an accident in the cargo bay shall not prevent shuttle abort. (RR-1.N, 1.1.001) (5.1)

3.1.5 Vented gases from the shuttle cargo bay shall not be allowed to flow past the shuttle propellant tanks. (RR-1.0, 1.1.001)

3.1.6 Cargo bay surface materials which may be exposed to leaking corrosive fluids from payload shall be constructed or protected against corrosion. (GR-1.V, 1.1.006) (5.5)

3.1.7 Always-open cargo bay vents to space shall be provided on the orbiter which limit internal cargo bay pressures from the combustion products of a single upper stage vehicle reaction control rocket engine to the cargo bay allowable limits. (RR-1.1.007)

3.1.8 The factors of safety for the upper stage vehicle and orbiter attachment point shall be at least equal to the normal orbiter structure factors of safety. (GP-1.1.008)

3.1.9 The upper stage vehicle shall be supported in the orbiter so that failure of any one structural support member will not jeopardize support of the upper stage vehicle during return to earth. (RP-1.1.008)

3.1.10 The upper stage vehicle shall be extended and released outside of the cargo bay such that upper stage vehicle rotation about any one attachment point or about its center of gravity in any direction upon release, will not impact any part of the orbiter. (RR-1.W, 1.1009) (5.3)

3.1.11 No torques shall be imparted to the upper stage vehicle by the separation mechanism. (GP-1.1.009)

3.1.12 Redundancy shall be provided in the means for separating the upper stage vehicle. No single failure shall result in unprogrammed motion of the upper stage vehicle. (RP-1.1.010)

3.1.13 Orbiter to upper stage vehicle connections shall be designed for emergency manual release by orbiter crew member in extravehicular activity. (RR-1.1.010) (5.4)

3.1.14 Emergency release of the extension mechanism shall be possible in order to save the orbiter at the expense of the upper stage vehicle. (RR-1.1.010)

3.1.15 A backup means shall be provided for the orbiter crew to vent or pressurize upper stage vehicles with a pressure stabilized structure. (RP-1.1.012) (5.6)

3.1.16 The support structure of a pressure stabilized upper stage vehicle in the shuttle shall allow shuttle de-orbit, re-entry and landing following loss of pressurization in the upper stage vehicle while in the orbiter cargo bay in orbit. (GR-1.1.012)

3.1.17 A backup means of dumping propellants and pressurants from a retrieved upper stage vehicle shall be available. (RP-1.1.013)

3.1.18 The orbiter shall have the capability to de-orbit, re-enter and land with a fully loaded upper stage vehicle as payload. (RR-1.1.014) (5.7)

3.1.19 Means shall be provided for re-opening the cargo bay doors from any partially closed position. (RR-1.1.015)

3.1.20 Capability shall be provided to purge or vent the orbiter airlock and tunnel to space following emergency egress of passengers from a toxic payload environment, or following IVA personnel entry for inspection and subsequent return to prevent the toxic environment from contaminating the orbiter crew and passenger compartment. (RP-1.e, 1.2.001)

3.1.21 Emergency capability shall be provided in the orbiter to purge the orbiter pressurized volumes of a toxic environment that may result from toxic contamination of a payload, and to sustain orbiter personnel during the purging operation. (RP-1.2.001)

3.1.22 The orbiter cargo bay shall be vented to space or the orbiter cargo bay doors shall be opened at all times while on-orbit to preclude buildup of pressures in the cargo bay of supporting combustion. (RP-1.2.002) (5.10)

3.1.23 Capability to release, eject, or extend the payload shall be provided so as to prevent damage to the orbiter at the expense of the payload. (RR-1.h, 1.2002)

3.1.24 Capability shall be provided for the orbiter crew to vent and dump pressurized, flammable or hazardous payload fluids to space within the time constraints imposed by an abort situation. This capability shall be available with the cargo bay doors open or closed. (RR-1.i, 1.2.002)

3.1.25 Capability shall be provided to switch off all electrical loads to payload from the orbiter. (RP-1.j, 1.2002)

3.1.26 Thermal insulation shall be provided between orbiter cargo bay/payload attach points and other physical interfaces to minimize thermal conduction to orbiter structure. (RP-1.1, 1.2002)

3.1.27 Fire and heat resistant protection of orbiter to payload command and instrumentation interfaces shall be provided. (RP-1.m, 1.2002) (5.11)

3.1.28 Ignition sources in the orbiter bay, such as switches and relays, shall be sealed or otherwise contained so as to prevent ignition of flammable fluids. (RP-1.n, 1.2.002)

3.1.29 Capability shall be provided to isolate orbiter environmental control system from payload to prevent toxic fumes from entering the orbiter. (RR-1.2.003)

3.1.30 Access for visual inspection by intravehicular activity or remotely by instrumentation shall be provided to all primary structure inside the cargo bay or equipment in the cargo bay required for return to earth. (GR-1.2.004)

3.1.31 Vented gases from the orbiter cargo bay shall not be allowed to flow past the orbiter propellant tanks. (RR-1.0, 1.1.001) (5.5)

3.1.32 Capability shall be provided to purge or vent the orbiter airlock and tunnel space following emergency egress of passengers from a corrosive payload environment, or following IVA personnel entry for inspection and subsequent return to prevent the corrosive environment from contaminating the orbiter crew and passenger compartment. (RP-1.e, 1.2.001)

3.1.33 Orbiter hardware required for abort shall be located remotely from the cargo bay, or protected against the potential effects of payload explosions which would not cause primary shuttle structure failure. (RR-1.2.005)

3.1.34 Always-open cargo bay vents to space shall be provided on the orbiter which limit internal cargo bay pressures from leakage to the cargo bay allowable limits. (RR-1.2.005)

3.1.35 Cargo shall be packaged during transfer so as to have no exposed sharp edges or corners. (RR-1.3.004)

3.1.36 Crew controlled cargo transfer velocity shall be limited so that the cargo can at all times be stopped within the visible range. (RP-1.3.004)

3.1.37 Cargo beyond the limits allowed for hand transfer shall be transferred on guide rails or other mechanisms which positively constrain the angular and linear motion of the cargo except in the direction of motion. (RP-1.3.004)

3.1.38 Cargo handling mechanisms shall allow for stoppage of the motion, reversal of the motion, or release of the cargo at any point along the transfer path. (RP-1.dd, 1.3.002)

3.1.39 Cargo handling mechanisms shall be designed to withstand the propulsive forces that would result from a leaking or ruptured fluid cargo. (RR-1.hh, 1.3.002)

Docking

3.1.40 The reflectance of surfaces on docking vehicles and the docking system that are visible to the controlling crew and T.V. cameras shall be below eye and vidicon damage levels. (RP-2.1.001)

3.1.41 The vidicon tubes for docking shall be designed for low sensitivity to tube image burn. (GP-2.1.001)

3.1.42 Redundant or replaceable lighting provisions shall be provided for docking. (RP-2.1.001)

3.1.43 Redundant or replaceable vidicon tubes shall be provided for docking. (RR-2.1.001)

3.1.44 Redundant or replaceable video monitors shall be provided. (RR-2.1.001)

3.1.45 The reaction jet control system shall provide redundancy to preclude "jet stuck off" conditions. (RP-2.A, 2.1.002)

3.1.46 The rate command and rate/attitude feedback loops of the rotational control system shall provide redundancy to preclude "open loop" failures. (RP-2.B, 2.1.002)

3.1.47 The translational command circuits shall provide redundancy to preclude "open circuit" failures. (RP-2.1.002)

3.1.48 The docking system shall be designed to operate with continuous command of the control system in the event that minimum impulse command has been lost. (RR-2.1.002)

3.1.49 Docking system rapid emergency release capability shall be provided. (RR-2.1.003)

3.1.50 The docking system shall be designed to withstand normal jackknifing vehicle dynamics and will limit attitude excursions to within prescribed limits as determined by vehicle geometry to prevent inadvertent vehicle contact. (RR-2.1.003)

3.1.51 The docking system shall be capable of withstanding vehicle oscillation and loads generated by inadvertent attitude control system activity of either or both vehicles during draw down to rigidize the capture interface. (RR-2.1.004)

3.1.52 Thermal protection shall be provided to prevent jet plume impingement damage from docking vehicles within the design angular and linear misalignments. (RR-2.1.004)

3.1.53 Capability shall be provided to recycle both capture and seal latches on the docking system from any phase of their status. (RR-2.1.005)

3.1.54 Translation acceleration command minimum impulse capability shall be provided to permit station keeping drift to a minimum and reduce attenuation requirements. (GP-2.1.005)

3.1.55 Bore sight alignment of video or direct visual view with the center line or the docking interface from a point not greater than 2.0 meters from the docking plane shall be provided to reduce contact misalignment. (GP-2.1.005)

3.1.56 Docking port environmental covers shall be deployed and not jettisoned. (RP-2.1.005)

3.1.57 Positive means for jettisoning the payload module shall be provided in the event of a failure of the payload deployment mechanism. (RR-2.1.006)

3.1.58 Guiderails or similar devices shall be provided to prevent recontact between payload module and cargo bay in the event of deployment mechanism failure. (RR-2.1.006)

3.1.59 Positive means for jettisoning or collapsing payload deployment mechanism shall be provided if mechanism will at any point in the deployment obstruct the closure of the cargo bay doors. (RR-2.1.006)

3.1.60 All hardware in the docking tunnel will be flush mounted to interior walls of the cargo/crew transfer tunnel. (RP-2.1.007)

3.1.61 Emergency life support provisions shall be available to the docking crew during docking operations (RP-2.1.009)

3.1.62 Stops shall be provided on hatches to prevent uncontrolled opening if opened when a pressure differential exists. (RP-2.1.010)

3.1.63 All docking interface equipment shall be grounded. (RR-2.1.011)

3.1.64 Electrical umbilicals shall be grounded until connection of the docking interface. (RR-2.1.011)

3.1.65 Thermal blanket temperature control of hydraulic components shall provide proper operating temperature. (RP-2.2.002)

3.1.66 Redundant joint motor power supply circuits shall be provided on manipulators. (GP-2.4.003)

3.1.67 Two or more manipulators shall be provided in a manipulator docking system. Each manipulator shall be capable of performing docking by itself, and shall also be capable of continuing any docking function in the event of a failure of the other manipulator at any stage of the docking. (RR-2.4.003)

3.1.68 An emergency jettisoning capability shall be provided for manipulators, independent of the normal manipulator system. This shall be capable of jettisoning the manipulator and configuring the orbiter for reentry and landing following a failure or accident which does not allow stowage of the manipulator. (RR-2.4.003)

3.1.69 Redundant control feedback loops shall be provided each axis of computer aided control for the manipulator. (RP-2.4.004)

3.1.70 The manipulator computer aided control system shall fail to the "no command" mode. (GR-2.4.004)

3.1.71 Manual override of computer aided manipulator control shall be provided. (RR-2.4.004)

On-Board Survivability

3.1.72 Normally habitable compartments of more than 25 m^3 (880 ft^3) in volume shall have two or more exits into areas which provide for personnel survival. These exits shall be at least 3 m (10 ft) apart. (RR-3.C, 3.1.001)

3.1.73 Flammable, explosive or gas generating material shall be located so that the energy content which can be propagated at any one location shall not result in overpressurization of the compartment from heat and gas production. (RR-3.D, 3.1.001)

3.1.74 Flammable, explosive or gas generating material within 3 m (10 ft) of the entrance to compartments with only one entry/egress path shall be limited so that the energy content, if released, will not result in damage or an environment which prevents shirtsleeve access through the entrance. (RR-3.E, 3.1.001)

3.1.75 Emergency capability shall be provided on orbiter flights with a manned sortie module for the return to earth of all the passengers in the orbiter, without support from the sortie module. (RR-3.G, 3.1.002)

3.1.76 Orbiter equipment required for returning the orbiter to earth shall be capable of operating in a depressurized environment. The controls for this equipment shall be operable by crewmen in pressure suits. (RR-3.I, 3.1.004)

3.1.77 A backup EVA egress/ingress hatch which can be used for contingency EVA shall be available. Capability for depressurization and repressurization of the connecting compartment/module shall be provided. (RR-3.J, 3.1.008)

3.1.78 The orbiter shall be divided into two or more compartments which can be rapidly sealed off in an emergency to prevent the ingress of flames and contaminated atmosphere from the other compartment(s). Each of these compartments shall be capable of accommodating all on-board orbiter personnel until the fire and/or toxic environment can be eliminated and a habitable environment restored. (RR-3.1.001)

3.1.79 Two or more entrances into normally habitable compartments of more than 25 m^3 (880 ft^3) in volume shall be shirtsleeve accessible from each of the other normally inhabited compartments. These entrances shall be at least 3 m (10 ft) apart. (RR-3.1.002)

3.1.80 Where only one shirtsleeve ingress/egress path is provided into a compartment or module, redundant means shall be available for opening the connecting hatch(es) from either side. (RR-3.1.005)

3.1.81 The space station shall be configured so that it always has at least two docking ports available which can accommodate a shuttle orbiter resupply or rescue mission. (RR-3.1.006)

3.1.82 Emergency life support capability shall be available on the space station following the non-arrival of the next planned orbiter until the following resupply or rescue orbiter flight. (RR-3.1.006)

3.2 SAFETY DEVICES

Hazardous Payloads

3.2.1 Capability shall be provided for the orbiter crew to vent and dump upper stage vehicle pressurized or hazardous fluids to space within the time constraints imposed by an abort situation. This capability shall be available with the cargo bay doors open or closed. (RP-1.G, 1.1.001) (5.7)

3.2.2 Orbiter equipment and structure exposed to vented gases from the cargo bay shall be protected against the effects of corrosion and be capable of inspection on the ground. (RR-1.P, 1.1.001) (5.1, 5.5)

3.2.3 Interlocks, redundancy, grounding and isolation devices shall be provided on explosive charges so that no single detectable failure or combination of undetectable failures shall result in premature detonation. (RP-1.1.003)

3.2.4 A restraint system shall be provided for the upper stage vehicles in the orbiter cargo bay which prevents contact of the vehicle with orbiter structure or equipment in the event of partial or total release of the attachment points. (RP-1.1.008)

3.2.5 Capability shall be provided for the orbiter crew to selectively pressurize or vent each tank of an upper stage vehicle using a common bulkhead. The capability shall be available with the orbiter cargo bay doors open or closed. (RP-1.1.011) (5.12)

3.2.6 Automatic means shall be provided for detecting interferences by the payload with the closing of the cargo bay doors and stopping the motion before damage results to the doors or the door mechanism. (RR-1.1.015)

3.2.7 Capability shall be provided for visual inspection of an orbiter payload in the orbiter cargo bay with the cargo bay doors open. (RP-1.1.015)

3.2.8 Capability for extra-vehicular activity shall be provided to disconnect, sever, or otherwise free cables, deployed mechanisms or other upper stage vehicle protruberances which could interfere with retrieval and stowage in the orbiter. (RP-1.1.015)

3.2.9 Means shall be provided to decontaminate personnel who have been exposed to a toxic or corrosive environment in the payload which can be propagated to the orbiter before entering the orbiter crew and passenger compartments. (RR-1.f, 1.2.001)

3.2.10 Manually and remotely controlled means shall be provided in pressurized orbiter payloads for controlling and extinguishing fires. (RR-1.2.003)

3.2.11 Means shall be provided for the local application of radiant or other type of heat remotely or by personnel in IVA or EVA activity to evaporate accumulations of frozen fluids from critical areas. (RR-1.2.004) (5.13)

3.2.12 Cargo of more than 45 kg (100 lb) mass, or hazardous cargo shall be tethered at all times during handling and transfer in pressurized areas either to the spacecraft structure or to the transfer mechanism so as to limit the possible travel of the cargo following a failure of the primary cargo attach mechanism. (RR-1.3.004) (5.14)

3.2.13 Automatic and/or crew controlled emergency means shall be provided for shutting off power and arresting the motion of cargo transfer mechanisms. (RR-1.3.004)

3.2.14 Packaging of hand-carried cargo shall be provided with multiple handholds, shall allow forward visibility by the controlling personnel, and shall be capable of surviving impact against a sharp object at 3 m/sec (10 ft/sec). (RP-1.aa, 1.3.001)

3.2.15 Provisions shall be made for rapidly securing hand-carried cargo to various structural points along the transfer path so as to prevent loss of control of the cargo in the event of an emergency. (RP-1.bb, 1.3.001)

Docking

3.2.16 Window, vidicon, and EVA visor filters shall be provided to protect eyes and camera from docking laser light damage. (RP-2.1.001)

3.2.17 Inhibit capability shall be provided to control the "jet stuck on" condition. (RR-2.C, 2.1.002)

3.2.18 Either manual and/or redundant automatic attitude hold inhibit functions shall be provided to the applicable docking vehicle on indication of capture. (RP-2.1.004)

3.2.19 Control system inhibit switches shall be protected from inadvertent activation or deactivation. (RP-2.1.004)

3.2.20 Docking latching systems recycle switches shall be protected from inadvertent activation. (RP-2.1.005)

3.2.21 Stowage or tie down shall be provided for crew and critical equipment during docking. (GP-2.1.008)

3.2.22 Means shall be provided to equalize pressures on both sides of a hatch before opening it. (RP-2.1.010)

3.2.23 Circuit breaker protection of all interface instrumentation shall be provided. (RR-2.1.011)

3.2.24 Control feedback loops shall be provided on each manipulator joint control which limit motion when excessive forces or torques are experienced. (RR-2.4.003)

3.2.25 Arm joint on manipulators shall be designed to lock on indication of joint control or motor failure. The lock shall incorporate a slip clutch capability to prevent structural failures. (RR-2.4.003)

3.2.26 Electrical or mechanical stops shall be provided to prevent the manipulator from being driven into surfaces of its own vehicle. (GR-2.4.003)

On-Board Survivability

3.2.27 Capability shall be provided to reduce the pressure in each compartment sufficiently, or increase it in the adjoining compartment(s) and to cut off air circulation, so that in an emergency the atmosphere in the affected compartment will not be propagated into adjoining compartments. This capability shall be controlled remotely from each compartment. (RR-3.A, 3.1.001)

3.2.28 Automatic venting capability shall be provided in each compartment so that in the event of a fire or release of gases within the compartment the pressure will not exceed the structural limits of the structure or the capability of seals to other compartments to exclude the contaminated atmosphere. (RR-3.B, 3.1.001)

3.2.29 Pressure suits and attendant life support shall be provided for the orbiter crew on every flight. (RR-3.1.004)

3.2.30 Pressure suits and attendant life support shall be provided for all orbiter/sortie module passengers on missions where the configuration does not provide two separate pressurizable compartments capable of returning all passengers to earth. (RR-3.1.004)

3.3 WARNING DEVICES

Hazardous Payloads

3.3.1 Capability shall be provided to detect potential tank failures by measurement of fluid pressures, temperatures, tank strains, or other means. (RF-1.F, 1.1.001)

3.3.2 Cargo bay pressure and selected wall temperatures shall be monitored. (GR-1.S, 1.1.002)

3.3.3 Upper stage vehicle monopropellant temperatures and pressures shall be monitored. (RR-1.1.004) (5.15)

3.3.4 Means shall be provided to indicate to the orbiter crew that a retrieved upper stage vehicle is positively secured at all attached points prior to deorbit and reentry. (RP-1.1.008)

3.3.5 For upper stage vehicles with propulsion tanks using common bulkheads, differential pressure between the two tanks, common bulkhead strain, or other indications of potential failure, shall be monitored by the orbiter crew. (RP-1.1.011)

3.3.6 Positive indication shall be provided to the orbiter crew that a retrieved payload has been properly secured in the cargo bay before closing the cargo bay doors. (RP-1.1.015)

3.3.7 Positive indication shall be provided to the orbiter crew that the cargo bay doors have closed and latched before initiating de-orbit. (RR-1.1.015)

3.3.8 Means shall be provided for determining the presence of an unacceptable toxic environment in the orbiter as a result of toxic contamination in a payload. (RP-1.2.001) (5.16)

3.3.9 Fire detection and location capability, such as distributed thermocouples, infrared detectors, or remote control TV, shall be provided in the cargo bay for use while the cargo bay doors are closed. (RR-1.2.002)

3.3.10 Means shall be provided for detecting the presence of a fire in pressurized shuttle payloads. (RR-1.2.003)

Docking

3.3.11 Positive, redundant indication of docking capture latch shall be provided the vehicle which is to inhibit its control system. (RR-2.1.004)

3.3.12 Positive indication of cargo bay door deployment and closure shall be provided. (RR-2.1.005)

3.3.13 Positive indication of docking capture latch status shall be provided to assure they are each (1) armed, (2) triggered, (3) engaged, and (4) locked. (RR-2.1.005)

3.3.14 Positive, redudant indication of docking port seal latch status shall be provided to assure they are each (1) armed, (2) triggered, (3) engaged, and (4) locked prior to opening transfer tunnel. (RR-2.1.005)

3.3.15 Annunciator warning to all personnel shall be provided prior to manned docking maneuvers. (RP-2.1.008)

3.3.16 Means shall be provided to verify the integrity of a docking hatch seal before separating a docked module or vehicle. (RP-2.1.010)

3.3.17 Positive redundant indication of the pneumatic attenuation system status of the extendable docking system shall be provided. (RR-2.3.003)

3.4 OPERATIONAL PROCEDURES

Hazardous Payloads

3.4.1 Pressurizing gas on upper stage vehicles shall be turned off until immediately prior to release of the vehicle from the orbiter. (RP-1.H, 1.1.001) (5.17)

3.4.2 Cargo bay doors shall be open at all times in earth orbit. (GR-1.M, 1.1.001) (5.2)

3.4.3 Liquid propellants of retrieved upper stage vehicles shall be dumped to space before initiation of the shuttle orbiter deorbit maneuver. (RP-1.Q, 1.1.001)

3.4.4 Upper stage vehicle propella... tank pressures shall be reduced to the minimum operating value before retrieval into the orbiter cargo bay. (RP-1.R, 1.1.001)

3.4.5 Crew procedures for monopropellant dump shall be provided in case of rapid rise in pressure or temperature. (RR-1.1.004) (5.15)

3.4.6 Orbiter crew control of upper stage vehicle shall be provided until separation from the orbiter precludes possibility of recontact. (RP-1.U, 1.1.005) (5.18)

3.4.7 Orbiter orientation shall point the longitudinal axis toward the separated upper stage vehicle until a safe separation distance has been achieved. (RR-1.1.005) (5.18)

3.4.8 Procedures shall be available to apply unidirectional translational or rotational acceleration to the orbiter in the event of a partial or total release of the payload in the cargo bay until loose parts and the payload have settled sufficiently to allow further corrective action. (RR-1.1.008) (5.19)

3.4.9 Procedures shall be available for backing off the orbiter from an upper stage vehicle inadvertently separated in the orbiter cargo bay without contact of the upper stage vehicle with orbiter structure or equipment while in orbit. (RR-1.1.008) (5.20)

3.4.10 Emergency procedures shall be available for the release, handling, and transportation of remotely controlled cargo in the event of failure of the handling mechanism, or of damage to the packaging of the cargo. (GP-1.gg, 1.3.002)

3.4.11 The planned attitudes of the upper stage vehicle during release and separation from the orbiter shall be such that the attitude control engines at no time accelerate the vehicle towards the orbiter. (GR-1.1.009)

3.4.12 Orbiter shall be moved away from upper stage vehicle immediately on release. (RR-1.1.009)

3.4.13 Upper stage vehicle attitude and translation shall be monitored by the orbiter crew immediately following release (RR-1.1.009)

3.4.14 Upper stage vehicle attitude shall be controlled by command of the orbiter crew immediately following release. (RR-1.1.009)

3.4.15 Internal attitude control signal of the upper stage vehicle shall be monitored for accuracy by the orbiter crew before release (RP-1.1.009)

3.4.16 Upper stage vehicle shall be switched from command control to internal attitude control after orbiter has been sufficiently moved that no attitude change could result in collision. (RP-1.1.009)

3.4.17 Upper stage vehicle shall be switched from command control by the orbiter crew to internal translation control when sufficient time is available for the orbiter crew to execute evasive maneuvers following any main propulsion or guidance failure. (RR-1.1.009)

3.4.18 The trajectories of the orbiter and the upper stage vehicle shall be continually compared following release, and a means for shutting down the upper stage vehicle shall be provided if a collision appears imminent. (RR-1.1.009)

3.4.19 Special orbiter attitude and translation motions shall be planned to assist release of any single residual connection with the upper stage vehicle. (GR-1.1.010) (5.4)

3.4.20 Procedures shall be available for extra-vehicular inspection and release or re-attachment of partially released upper stage vehicles in orbit. (RR-1.X, 1.1.010) (5.4)

3.4.21 Dumping of propellants and pressurants from a retrieved upper stage vehicle shall be accomplished before initiation of the shuttle orbiter deorbit maneuver. (RP-1.1.013)

3.4.22 Dumping of propellants and pressurants from a retrieved upper stage vehicle shall be controlled by the orbiter crew. (RP-1.1.013)

3.4.23 An upper stage vehicle in which propellant and pressurants have not been dumped shall not be returned into the orbiter cargo bay. (RR-1.1.013)

3.4.24 Sufficient propellants for orbiter de-orbit and landing with on-board, fully loaded upper stage vehicle shall be retained on the orbiter until main engine ignition of the upper stage vehicle. (RR-1.1.014) (5.7)

3.4.25 Capability shall be provided for visual inspection of an orbiter payload before initiating retrieval and loading into the orbiter cargo bay. (RP-1.1.015)

3.4.26 Procedures shall be available for extravehiclular or remote inspection, extension, and release or re-positioning of improperly stowed upper stage vehicles in orbit. (RR-1.1.015)

3.4.27 Procedures shall be available for immediately initiating opening of the cargo bay doors if a fire is detected in the cargo bay while the doors are shut. (RR-1.2.002) (5.10)

3.4.28 Emergency procedures shall be available for releasing cargo which has become jammed in hatches or other restricted areas without causing damage to the spacecraft structure or equipment. (RR-1.3.004) (5.21)

3.4.29 Manual handling and transfer of hazardous fluids or materials shall be carried out by two or more personnel who shall have no other duties during this operation. (RP-1.u, 1.3.001)

3.4.30 Hand-carried cargo shall be limited to 45 kg (100 lb) mass, provided the center of mass is within 35 cm (14 in) of the handhold. Cargo which exceeds these limits shall be transported with mechanical assist. (RP-1.y, 1.3.001)

3.4.31 Cargo in which a rupture or leakage through the containers would result in uncontrolled motion of the cargo because of propulsive forces beyond a single man's capability to control, or because toxicity requires immediate abandonment and evacuation of the area,shall not be hand-carried. (GR-1.z, 1.3.001)

3.4.32 The transfer of cargo with mechanical assist shall either be visually monitored by personnel who are free of other duties, or shall be provided with sensing devices which automatically stop the motion if the cargo interfaces with structure or equipment. (RP-1.ee, 1.3.002)

3.4.33 Personnel shall not be located during cargo transfer in positions which can result in their entrapment if the cargo transfer mechanism fails. (RR-1.ff, 1.3.002)

Docking

3.4.34 Maneuvering procedures during docking shall preclude directing sunlight into controlling crew's eyes or into the vidicon tubes of the visual system. (RP-2.1.001)

3.4.35 The pressures on each side of a hatch shall be verified before opening the hatch. (RP-2.1.010)

3.4.36 Personnel will only be transferred between the orbiter and the station through a rigidly connected docking interface between the two vehicles. (RR-2.4.003)

On-Board Survivability

3.4.37 On orbiter missions without attached manned sortie modules in which EVA is planned as part of the normal mission, pressure suits shall be carried for all on-board personnel. (RR-3.K, 3.1.009)

3.4.38 The orbiter crew shall not enter manned sortie modules during the conduct of hazardous experiments. (RR-3.1.002)

3.5 RESIDUAL HAZARDS

		Acceptable Risk	Unresolved Safety Issues	SRT Reqmts
3.5.1	Explosion/rupture of a pressurized container in an upper stage vehicle inside or near shuttle. (1.1.001)		X	
3.5.2	Combination of mutually reactive upper stage vehicle fluids in explosion or fire inside or near shuttle. (1.1.002)		X	
3.5.3	Rapid decomposition of monopropellants located in or leaking from the upper stage vehicle while inside or near shuttle. (1.1.004)			X
3.5.4	Leakage of corrosive fluids from upper stage vehicle tanks while inside the orbiter. (1.1.006)			X
3.5.5	Inadvertent start of an upper stage vehicle rocket engine while inside shuttle cargo bay. (1.1.007)	X		
3.5.6	Inadvertent separation of any part of upper stage vehicle while attached to the shuttle. (1.1.008)	X		
3.5.7	Loss of attitude/translation control of upper stage vehicle upon release from shuttle. (1.1.009)	X		
3.5.8	Rupture of common bulkhead tanks in upper stage vehicles while in or near shuttle. (1.1.011)	X		
3.5.9	Loss of pressurization in pressure stabilized upper stage vehicle. (1.1.012)	X		
3.5.10	Inability to close cargo bay doors after retrieval of upper stage vehicle because of interference with upper stage vehicle. (1.1.015)	X		

		Acceptable Risk	Unresolved Safety Issues	SRT Reqmts
3.5.11	Exposure of the shuttle crew or passengers to a toxic environment released from a vessel in the payload containing a toxic fluid. (1.2.001)	X		
3.5.12	A fire in the cargo bay resulting from release and ignition of a flammable fluid in an unpressurized payload. (1.2.002)			X
3.5.13	A fire in a pressurized payload in the cargo bay resulting from release and ignition of a flammable fluid. (1.2.003)			X
3.5.14	A corrosive environment in the shuttle cargo bay resulting from leakage or rupture of a payload vessel containing a corrosive fluid. (1.2.004)			X
3.5.15	An explosion in the shuttle cargo bay of a potentially explosive payload vessel. (1.2.005)		X	
3.5.16	Spillage or leakage of hazardous fluid or material during manual transfer in pressurized modules. (1.3.001)			X
3.5.17	Spillage or leakage or hazardous fluids or materials during mechanically assisted or remote transfer in pressurized modules. (1.3.002)			X
3.5.18	Spillage or leakage of hazardous fluid or material during remote transfer in unpressurized area. (1.3.003)	X		
3.5.19	A radioactive environment in a sortie module or space station, resulting from exposure or escape or radioactive material during transfer and handling of radioactive materials. (1.3.005)	X		

		Acceptable Risk	Unresolved Safety Issues	SRT Reqmts
3.5.20	Loss of vehicle control prior to docking contact.			X
3.5.21	Loss of vehicle control after initial contact.			X
3.5.22	Loss of docking system function or control.	X		
3.5.23	Failure of orbiter payload module deployment mechanism.	X		
3.5.24	Loss of vehicle control in close proximity to other vehicle.			X
3.5.25	Loss of vehicle control prior to docking contact by extendable tunnel.			X
3.5.26	Loss of vehicle control after capture by extendable tunnel docking system.			X
3.5.27	Loss of vehicle control prior to capture by manipulator.			X
3.5.28	Loss of vehicle control after capture by manipulator.			X
3.5.29	Loss of manipulator joint motor control.			X
3.5.30	Loss of Communications/Command capability during docking by unmanned free flying module.	X		
3.5.31	Loss of propulsion or control capability during docking by manned free flying module.		X	
3.5.32	Loss of life support capability during docking by manned free flying module.	X		

PRECEDING PAGE BLANK NOT FILMED

4.0 INTERFACE SAFETY REQUIREMENTS AND GUIDELINES

This section contains interface safety requirements and guidelines required by the shuttle orbiter to be applied on interfacing vehicles. These interface requirements and guidelines were developed from analyses of specific safety issues, and are grouped in this section by interfacing vehicle, as follows:

4.1 Space Station
4.2 Upper Stage Vehicles
4.3 Sortie Payloads

4.1 SPACE STATION

Hazardous Payloads

4.1.1 Capability shall be provided to relieve atmospheric pressure from an orbiter payload so as to prevent pressurization beyond the payload structural limits. This capability shall be automatic when the payload is not manned, and under control of the occupants when manned. The maximum dump rate shall not exceed the venting capability of the orbiter cargo bay with the cargo bay doors closed. (RR-1.2.003)

4.1.2 Access for visual inspection by intravehicular activity or remotely by instrumentation shall be provided to all primary structure of pressurized payloads while in the orbiter cargo bay. (GR-1.2.004)

4.1.3 The factors of safety of pressure vessels while in or near the orbiter shall be at least equal to the orbiter tank factors of safety. (GP-1.2.005)

4.1.4 Relief capability shall be provided for pressurized tanks which automatically limit maximum pressure. Venting shall be to space or to a tank at lower pressure, and shall be arranged so that mutually reactive fluids cannot mix and result in a fire or explosion. (RP-1.2.005)

4.1.5 Capability shall be provided to detect potential tank failures by measurement of fluid pressures, temperatures, tank strains, or other means. (RP-1.F, 1.1.001)

4.1.6 Pressurized tanks shall be located or provided with shrapnel proof barriers so that orbiter crew and passenger compartments and equipment required for orbiter return to earth will be protected in the event of a tank explosion. (RR-1.2.005)

4.1.7 Capability shall be provided to rapidly evacuate personnel from and seal off radioactively contaminated modules until they can be returned to earth. (RR-1.3.005)

4.1.8 Means shall be available for decontaminating equipment and personnel exposed to radioactive material and for storing and returning to earth radioactively contaminated clothing and other material. (RR-1.3.005)

Docking

4.1.9 Thermal protection shall be provided to prevent jet plume impingement damage from docking vehicles within the design angular and linear misalignments. (RR-2.1.004)

On-Board Survivability

4.1.10 Personnel shall not be allowed in a sortie or space station module during repositioning of the module from one docking port to another. (RR-3.1.006)

4.1.11 Manned sortie modules and space station modules shall be designed so that they can be undocked, retrieved into the orbiter cargo bay and returned to earth unpressurized. (GR-3.1.007)

4.2 UPPER STAGE VEHICLE

Hazardous Payloads

4.2.1 Upper stage vehicle pressures shall be limited while in or near the shuttle such that the factors of safety are at least equal to the shuttle tank factors of safety. (GP-1.A, 1.1.001)

4.2.2 Gaseous content of upper stage vehicle tanks shall be small enough so that rapid isentropic expansion into the shuttle cargo bay will not result in overpressure. (GR-1.B, 1.1.001)

4.2.3 Tanks shall be designed so that failure due to overpressure will not produce shrapnel. (GR-1.C, 1.1.001) (5.22)

4.2.4 Relief capability shall be provided for the upper stage vehicle tanks which automatically limit maximum pressure. Venting shall be to space or to a tank at lower pressure, and shall be arranged so that mutually reactive fluids cannot mix and result in a fire or explosion. (RP-1.D, 1.1.001)

4.2.5 Housings of explosive charges shall be designed to prevent damage to equipment required for shuttle abort in the event of inadvertent detonation. (RP-1.1.003)

4.2.6 Destruct charges shall not be incorporated in upper stage vehicles when launched in the shuttle. (RP-1.1.003)

4.2.7 Propellant shut-off valves upstream from all start valves shall be provided so that inadvertent main valve opening would not start engines on upper stage vehicles while in or near the orbiter. (RP-1.1.007)

4.2.8 The design of the upper stage vehicle control system shall only allow supply of electrical energy to the start valves of the rocket engines following positive action by the orbiter crew during upper stage vehicle count-down in orbit. (RP-1.1.007)

4.2.9 The design of the upper stage vehicle control system shall only allow supply of electrical energy to the separation mechanism following positive action by the orbiter crew during upper stage vehicle count-down in orbit. (RP-1.1.008)

4.2.10 All venting of the upper stage vehicles while near the orbiter shall be non-propulsive or shall translate the vehicle away from the orbiter. (RP-1.1.009)

4.2.11 The capability shall be provided on upper stage vehicles for remote emergency jettisoning of deployable equipment to allow retrieval and stowage in the orbiter cargo bay. (GP-1.1.015)

4.3 SORTIE PAYLOADS

Hazardous Payloads

4.3.1 Access for visual inspection by intravehicular activity or remotely by instrumentation shall be provided to all primary structure of pressurized payloads while in the orbiter cargo bay. (GR-1.2.004)

4.3.2 The factors of safety of pressure vessels while in or near the orbiter shall be at least equal to the orbiter tank factors of safety. (GP-1.2.005)

4.3.3 Relief capability shall be provided for pressurized tanks which automatically limit maximum pressure. Venting shall be to space or to a tank at lower pressure, and shall be arranged so that mutually reactive fluids cannot mix and result in a fire or explosion. (RP-1.2.005)

4.3.4 Capability shall be provided to detect potential tank failures by measurement of fluid pressures, temperatures, tank strains, or other means. (RP-1.F, 1.1001)

4.3.5 Pressurized tanks shall be located or provided with shrapnel proof barriers so that orbiter crew and passenger compartments and equipment required for orbiter return to earth will be protected in the event of a tank explosion. (RR-1.2.005)

4.3.6 Capability shall be provided to rapidly evacuate personnel from and seal off radioactively contaminated modules until they can be returned to earth. (RR-1.3.005)

4.3.7 Means shall be available for decontaminating equipment and personnel exposed to radioactive material and for storing and returning to earth radioactively contaminated clothing and other material. (RR-1.3.005)

4.3.8 Capability shall be provided to relieve atmospheric pressure from an orbiter payload so as to prevent pressurization beyond the payload structural limits. This capability shall be automatic when the payload is not manned, and under control of the occupants when manned. The maximum dump rate shall not exceed the venting capability of the orbiter cargo bay with the cargo bay doors closed. (RR-1.2.003)

On-Board Survivability

4.3.9 Emergency capability shall be provided on manned sortie modules for the return to earth of all the passengers in the sortie module, without life support from the orbiter. (GR-3.H, 1.1.001)

4.3.10 The orbiter crew shall not enter manned sortie modules during the conduct of hazardous experiments. (RR-3.1.002)

4.3.11 Pressure suits and attendant life support shall be provided for all orbiter/sortie module passengers on missions where the configuration does not provide two separatc pressurizable compartments capable of returning all passengers to earth. (RR-3.1.004)

4.3.12 Personnel shall not be allowed in a sortie or space station module during repositioning of the module from one docking port to another. (RR-3.1.006)

4.3.13 Manned sortie modules and space station modules shall be designed so that they can be undocked, retrieved into the orbiter, cargo bay and returned to earth unpressurized. (GR-3.1.007)

5.0 RATIONALE FOR REQUIREMENTS AND GUIDELINES

This section discusses the rationale for some of the requirements and guidelines. This discussion is confined to cases in which the rationale may not be obvious, or where some clarifying explanations are in order. The discussion in general follows the order of the requirements and guidelines, and reference is made in parentheses, where appropriate, to specific requirements and guidelines.

5.1 In the event of accidents which cause some damage to the orbiter but which leave the basic structure and reentry capability intact, the equipment required for abort should be suitably protected. The level of protection will be determined by the level of tolerance of the primary structure to blast, heat, etc. In determining this requirement, rescue of the crew and passengers by another shuttle was not considered acceptable as the only means for safeguarding personnel. (3.1.1, 3.1.4, 3.2.2)

5.2 In sizing the orbiter always-open vents in the cargo bay, consideration must be given not only to cargo bay atmospheric venting during boost and reentry, but also to the possibility of orbiter payload leakage. A "worst case" leakage figure must be established for each payload. During boost and reentry these requirements will be additive to the cargo bay atmospheric venting. However, any additional venting arrangements for dealing with payloads must not cause excessive ingestion of hot gases during reentry. (3.1.2, 3.1.3, 3.4.2)

5.3 Following a deployment mechanism malfunction, the upper stage vehicle may be free to rotate about the remaining attach points, or, if completely unattached, may be rotating about its center of gravity. Under such circumstances the upper stage vehicle must not contact the orbiter. (3.1.10)

5.4 Hangup of an upper stage vehicle upon release may require only a small force or moment to free the vehicle. These forces and moments can be applied by programming appropriate orbiter accelerations, and the potential maneuvers should be defined in advance. These maneuvers should stay within structural capabilities and should allow clearance of the upper stage vehicle from the orbiter in the event of release or no release. EVA action is a backup operation to this. (3.1.13, 3.4.19, 3.4.20)

5.5 Vented gases from the cargo bay may be corrosive, and should not therefore be allowed to vent past propellant tanks or other equipment, where they may condense and cause corrosion. (3.1.6, 3.1.31, 3.2.2)

5.6 Even if a pressure stabilized upper stage vehicle loses its pressurization and callapses, it is still desirable to return the vehicle to earth for repair. The support structure in the orbiter bay must therefore be designed for this contingency. (3.1.15)

5.7 If an abort decision has been made, safety considerations on landing require the capability to dump upper stage vehicle propellants before landing, and hence before deorbit, to preclude dumping propellants during reentry (1.1.014-3). If, in addition, this capability is also lost (perhaps as a result of the abort cause), then the orbiter must be capable of deorbiting, reentering and landing with a fully loaded up payload (1.1.014-1, -2). Such a capability is currently provided in the NR orbiter design at a slightly reduced landing sink speed and factor of safety. A potential single cause which could both require abort and prevent dumping of upper stage vehicle propellants is a mechanical failure of the upper stage vehicle-to-orbiter dump provisions. In some designs the dump line goes through the cargo bay doors, and its failure could prevent the doors opening (thus leading to abort) and prevent propellant dumping. (3.1.18, 3.2.1, 3.4.24)

5.8 Because an improperly stowed recoverable upper stage vehicle can prevent return of the orbiter to earth, various precautionary measures are required. All of these measures are designed to provide step by step checks and operational flexibility to stop, reverse or abort the action. In the event of a major problem, the used upper stage vehicle would be sacrificed to save the orbiter and its personnel.

5.9 It is not currently known whether a fire is possible or can be sustained in the unpressurized environment of the orbiter cargo bay. Certainly, if the fluid leakage is in the form of directed jets, enough pressure could be generated where they impinge to sustain a fire. The relevant hazards/emergency analysis was based on the "fail safe" assumption that a fire <u>is</u> possible.

5.10 The current orbiter concepts call for the cargo bay doors to be opened shortly after orbit attainment, as the radiators are inside the doors, and to be closed shortly before deorbit. When the doors are open, no venting problems should arise. A risk of overpressurization in the event of massive release of a gas is possible, however, when the cargo bay doors are closed, and adequate venting should be ensured during that time. It is possible that the vents provided for boost and re-entry are quite adequate, but this should be checked for each payload. (3.1.22, 3.4.27)

5.11 Thermal insulation for protection against radiation from a fire and to reduce heat conduction into structure and equipment would considerably reduce the hazard from a fire in the cargo bay. This is not generally considered feasible, however, because of the weight and volume constraints, and is only recommended for essential instrumentation. (3.1.27)

5.12 While various capabilities are recommended to pressurize and vent tanks for upper stage vehicles with common bulkheads, the pressure differential between the two tanks must be maintained within the design limits at all times. An automatic capability for venting the tanks so as to maintain the allowable pressure differential has been considered. Such a device would be relatively complex, however, and would introduce very hazardous additional failure modes. This capability is therefore recommended to be under crew control. (3.2.5)

5.13 If a corrosive fluid leaks in the cargo bay, expansion and evaporation may cause some of the fluid to freeze, possibly attached to structure or equipment. This may remain frozen until re-entry or landing, when the solid may melt and increase its corrosive action. Means for applying heat to any solidified fluids are therefore required, possibly by IVA or EVA personnel, to evaporate and disperse the frozen fluids. (3.2.11)

5.14 Limitations should be placed on the mass and inertias of hand-carried cargo. The best available data has been used, but these limits should be updated if better human factors data become available. (3.2.12)

5.15 Chemical decomposition of unstable chemicals can be detected by a rise in temperature and pressure. If this is detected, the fluids can be dumped overboard before catastrophic damage occurs. (3.3.3, 3.4.5)

5.16 Some fluids are toxic in extremely small concentrations. A spillage in a pressurized payload, or in the cargo bay if EVa is performed, can propagate in small but toxic concentrations into the orbiter crew or passenger compartment. Means for determining that this has occurred have been required. This need not be a separate detection system in the orbiter, however. It can rely on measurements in the payload, or measurements of leakage of specific fluid vessels in the payload. (3.3.8)

5.17 Pressurized propellants have a potential for tank rupture. Pressurization should therefore be planned for the latest time possible. A tradeoff exists here between exposing the orbiter to this hazard for a short time by pressurizing before releasing the upper stage vehicle, and eliminating the hazard to the orbiter entirely by pressurizing the propellants when the upper stage vehicle is some distance away from the orbiter. In the latter case the risk is being taken

that a malfunction may occur which prevents pressurization which may have been correctible before release, thus losing the mission. On balance, the former risk was judged to be preferable. (3.4.1)

5.18 Various measures can be taken to prevent damage to the orbiter in the event of an upper stage vehicle reaction control engine malfunction. The best control of the hazard, however, is to provide capability for the orbiter crew to shut down the malfunctioning engines. Minimizing the exposed area of the orbiter is also considered a requirement. (3.4.6, 3.4.7)

5.19 A potential cause of damage in the event of a partial inadvertent separation of a payload is mechanical damage from unexpected motions and contact with structure. One means of preventing or minimizing such contact is to apply a small "ullage" type of acceleration on the orbiter, linear or angular, until the payload has "settled" into a stable position. While the desirability of doing this on any particular occasion must be left to the judgement of the crew, procedures for doing this should be worked out in advance. (3.4.8)

5.20 Similarly, procedures should be available for various other contingencies. Use of the procedures will depend on a balancing of risks in any individual situation. If the situation is critical, e.g., preventing reentry of the orbiter, then the procedures will be used, even if very risky. (3.4.9, 3.4.10)

5.21 Jamming of cargo in doors, hatches or other restricted areas can result in severe loss or damage if not handled with method and patience. Procedures for releasing such cargo should be developed ahead of time. Certain tools or other aids may also be found necessary by developing these procedures. (3.4.28)

5.22 The state-of-the-art is approaching the capability to design pressure tanks so that their failure mode when overpressurized does not produce shrapnel. This can be done, for example, by using appropriately large factors of safety, or by using fiberglass wound tanks. Shrapnel-free tanks would therefore be highly desirable. Because there is still doubt about the practicability of achieving this, it is called out as a guideline rather than a requirement. (4.2.3)

5.23 Relatively few uses of radioactive material are currently planned for sortie and solar-array powered space station missions. However, Atomic Energy Commission regulations call for strict safety measures to keep control of the radioactive material, and to minimize the possibility of exposing the general population on earth to excessive radiation as a result of an accident.