ORBITER SUBSYSTEM

HARDWARE/SOFTWARE INTERACTION ANALYSIS

VOLUME VIII: FORWARD REACTION CONTROL SYSTEM

January 1980
The Orbiter subsystem hardware/software interaction analysis examines software interaction with hardware failure modes. Each failure mode identified in subsystem FMEA (failure mode and effects analysis) is examined for interaction with software. The analysis is based upon key questions which identify potential issues. These potential issues are to be resolved by providing rationale for retention or identifying and implementing changes to eliminate the issue.

The figure on the following page illustrates the relationship of the hardware/software interaction analysis to the verification process which leads to the statement of flight readiness. As shown, the analysis is a supporting item which is a portion of the data base utilized by the FRAT's (flight readiness assessment teams) and the associated SEAM (Systems Engineering Assessment Meeting) teams in planning and controlling the verification process. The overall issue of hardware/software interface compatibility is addressed by the verification process itself. The analysis scope is limited to examination of single failure modes, as identified in the FMEA, and the interaction of these failure modes with the software as reflected by the software requirements.

The hardware/software interaction analysis is performed on a preliminary basis by the JSC Reliability Division. Results are then coordinated with JSC engineering and Rockwell/Space Systems Group engineering and reliability to obtain inputs and approval signatures. The approval sheet for the Forward Reaction Control System are presented below. The Rockwell signatures represent their review of the open issues and risks, if any, performed against the summarization of the analysis. Section 5.0 presents the analysis summary which groups the failure modes by similar retention rationale and is a convenience in identifying groups of failure modes in which the analysis is similar. The reviews with Rockwell did not cover each checklist. The minutes presented in the appendix document the nature and depth of the Rockwell analysis review.

This analysis verified that no open issues remain.

Approved:  
Joseph H. Levine 1/14/80

Chief, Reliability Division
The hardware/software interaction analysis is prepared by reliability. It is one of many analyses and documents used by the SEAM teams and FRAT's in the planning and management of the verification process. The overall verification process leads up to the final flight readiness statement for each subsystem and the vehicle as a whole.
HARDWARE/SOFTWARE INTERACTION ANALYSIS

Forward Reaction Control System
SUBSYSTEM

FMEA # SD75-SH-0016A
ANALYSIS DATE June 25, 1979

APPROVED:

JSC Reliability
JSC Engineering - FRAT Sponsor

Rockwell Reliability
Rockwell Engineering - FRAT Sponsor
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>2.0 SCOPE</td>
<td>1</td>
</tr>
<tr>
<td>3.0 APPLICABLE DOCUMENTS</td>
<td>1</td>
</tr>
<tr>
<td>4.0 DESCRIPTION</td>
<td>2</td>
</tr>
<tr>
<td>5.0 ANALYSIS SUMMARY SHEETS</td>
<td>9</td>
</tr>
<tr>
<td>6.0 ANALYSIS CHECKLIST SHEETS</td>
<td>11</td>
</tr>
</tbody>
</table>

## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-1</td>
<td>HARDWARE/SOFTWARE ANALYSIS CHECKLIST</td>
<td>3</td>
</tr>
<tr>
<td>4-2</td>
<td>CHANGE/RETENTION RATIONALE</td>
<td>6</td>
</tr>
<tr>
<td>4-3</td>
<td>HARDWARE/SOFTWARE ANALYSIS SUMMARY</td>
<td>7</td>
</tr>
</tbody>
</table>

Appendix: A-1
1.0 INTRODUCTION. This report documents the results of the analysis of the hardware/software interaction analysis for the Forward Reaction Control System. This analysis examines the interaction between hardware failure modes and software in order to identify associated issues/risks. These issues/risks are resolved through changes to software requirements to remove them, or surfaced to project/program management with appropriate retention rationale.

2.0 SCOPE. All Orbiter subsystems and interfacing program elements which interact with the Orbiter computer flight software are analyzed. The analysis for each subsystem or interfacing element is presented in a separate volume of this report (see section 3.1).

The analysis examines failure modes identified in the subsystem/element FMEA (failure mode and effects analysis). Potential interaction with software is examined through evaluation of the software requirements, not detailed implementation. The analysis is restricted to flight software requirements only, and excludes utility/checkout software. The BFS (backup flight system) software is considered only as necessary, and only as it differs from the primary; the basic thrust of the analysis is keyed to the primary system.

The analysis is based upon the hardware design and software requirements as they existed as of the date of the analysis. Future updates will be published as necessary to incorporate changes to either the hardware or software.

3.0 APPLICABLE DOCUMENTS.

3.1 HARDWARE/SOFTWARE INTERACTION ANALYSIS REPORT VOLUMES. The hardware/software interaction analysis results are reported on a subsystem basis, each in a separate volume. The separate volumes which make up this report are as follows:

<table>
<thead>
<tr>
<th>Volume</th>
<th>Subsystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Purge, Vent, and Drain</td>
</tr>
<tr>
<td>II</td>
<td>Payload Deployment and Retention</td>
</tr>
<tr>
<td>III</td>
<td>Payload Bay Doors</td>
</tr>
<tr>
<td>IV</td>
<td>Main Propulsion</td>
</tr>
<tr>
<td>V</td>
<td>Data Processing Subsystem</td>
</tr>
<tr>
<td>VI</td>
<td>Hydraulics</td>
</tr>
<tr>
<td>VII</td>
<td>Auxiliary Power Unit</td>
</tr>
<tr>
<td>VIII</td>
<td>Reaction Control</td>
</tr>
<tr>
<td>IX</td>
<td>Electrical Power</td>
</tr>
<tr>
<td>X</td>
<td>Orbital Maneuver</td>
</tr>
<tr>
<td>XI</td>
<td>Environmental Control and Life Support</td>
</tr>
<tr>
<td>XII</td>
<td>Integrated Avionics</td>
</tr>
<tr>
<td>XIII</td>
<td>Electrical Power Distribution &amp; Control</td>
</tr>
<tr>
<td>XIV</td>
<td>GNC (Guidance, Navigation &amp; Control) Support</td>
</tr>
<tr>
<td>XV</td>
<td>Displays &amp; Controls</td>
</tr>
<tr>
<td>XVI</td>
<td>Communications &amp; Tracking</td>
</tr>
<tr>
<td>XVII</td>
<td>Instrumentation</td>
</tr>
</tbody>
</table>
3.2 REFERENCE DOCUMENTS. The primary documents used in performing the analysis included the following:


g. SD75-SH-0010E, "Functional Subsystem Software Requirements, Redundancy Management," June 1, 1979.

4.0 DESCRIPTION.

4.1 GROUND RULES. The hardware software analysis is performed according to the following ground rules:

a. The hardware/software analysis will be limited to investigating the software interaction with the failure modes of the hardware as delineated in the subsystem FMEA's.

b. Software interaction will be limited to involvement of software of the onboard computers.

c. Only failure modes of hardware with software interfaces (software monitoring and/or software control) are analyzed.

d. The software detection must be considered with respect to each phase of the mission [prelaunch (OPS 1 only), ascent, onorbit, and entry].

4.2 ANALYSIS CHECKLIST. The basic tool for the analysis is the checklist (figure 4-1). A separate checklist is used for each failure mode analyzed. Note that the "FMEA Number" in the heading refers to the FMEA document number, not the page number on which the failure mode is treated.

The checklist consists of three sections: Body, change/retention rationale summary, and explanation/comments. Each of these sections is discussed below.
<table>
<thead>
<tr>
<th>SUBSYSTEM</th>
<th>FMEA NUMBER</th>
<th>FAILURE MODE</th>
</tr>
</thead>
</table>

### HARDWARE/SOFTWARE ANALYSIS CHECKLIST

<table>
<thead>
<tr>
<th>Item Failure Mode</th>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?</td>
<td>[ ]</td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>1a. If not, does the hardware provide information that the flight software could use to detect the failure?</td>
<td>*Yes</td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>2. Are the answers to questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?</td>
<td>Yes</td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>3. Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>3a. If not, does the capability exist for the software to compensate for this failure mode (either by commanding hardware action or implementing alternate program logic)?</td>
<td>*Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>4. As a result of this failure mode, can the software over-stress the hardware or induce another failure?</td>
<td>*Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>5. Can this failure mode, in combination with software logic, adversely affect other functions?</td>
<td>*Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>6. How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)? Note change to FMEA criticality.</td>
<td>N/A</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>7. If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?</td>
<td>A. Can the BFS be engaged after occurrence?</td>
<td>YES</td>
<td>[ ]</td>
</tr>
<tr>
<td>B. Will BFS tolerate failure without loss of crew/vehicle?</td>
<td>YES</td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>8. If the answer to either 1 or 3 is yes:</td>
<td>*Explanation required (see below)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CHANGE/RETENTION RATIONALE SUMMARY

<table>
<thead>
<tr>
<th>Change/Retention Rationale Summary</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. No H/S Issues</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Hardware Accepts Risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. No Software Detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Detection During Checkout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Acceptance Rationale Below</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Recommended Changes Below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**EXPLANATION/COMMENTS:**

---

**Figure 4-1. Hardware/Software Analysis Checklist.**
The questions in the checklist body are answered using the following guidelines:

a. Question 1. Will the information provided to the onboard software and the processing of that information cause annunciation of the failure and/or initiation of a corrective action in response to this failure mode?

b. Question 1a. Answer question 1a. if the answer to question 1 is "no." Information available to the software could be in the form of (1) sensor data used by onboard software but not for automatic fault detection (data used in software routines or fault detection available through callup or dedicated displays); (2) system and/or subsystem performance parameters; or (3) measurements which are downlisted. Answer "yes" if such information could be used to annunciate the failure condition or initiate responsive action. In explanation comments, specifically identify the information available for software detection.

c. Question 2. If all of the following questions are answered "no," check the "no" block and explain the difference in the explanation/comments section:

(1) Are the master measurements listed under "Failure Detectability In-flight" on the FMEA (1) used by the onboard software in detecting time critical failures (if routed to GPC), or (2) used by the onboard software in annunciating non-time critical failures via callup displays, or (3) downlisted for non-time critical failures?

(2) Are other measurements, dedicated displays, crew detection, and system/subsystem parameters available or able to detect this failure mode?

(3) If "failure detectability in-flight" specifies only software action, does the software actually initiate the corrective action as called out in the "corrective action" portion of the FMEA?

d. Question 3. The question considers only the cases wherein the software determines a failure.

e. Question 3a. Answer question 3a if the answer to 3 is "no." If the answer to 3a is "yes," call out the possible corrective action in the explanation/comments section.

f. Question 4. The question is considered for both the detected and the undetected failure. The overstress or inducement of another failure may be acceptable action. Overstress by software is improper commands, sequencing, or timing resulting in action exceeding hardware design requirements or exposing hardware to excessive environments.

g. Question 5. The question is considered for both the detected and the undetected failure. Limit adverse effects to effects directly resulting from software commands or subsequent actions resulting from erroneous inputs as a result of the failure.

h. Question 6. The hardware/software may change the method of detection and/or correction after the first or the second failure; consider this in answering the question. Determine if the software will be able to use the redundancy of the hardware. If the hardware/software interaction following the particular failure mode changes the criticality, in comparison to the FMEA, check the box provided in the summary section of the checklist.
i. Question 7. If crew action is not required to respond to the failure, check the "N/A" block. Cues which provide inputs to the crew include but are not limited to cathode-ray tube annunciation, caution and warning, visual cues, audible cues, callup and dedicated displays, subsystem status data, panel meters, etc.

j. Question 8.A and 8.B. Answer these questions only if either question 1 or 3 is "yes."

(1) Question 8.A. Consider that the failure occurs while the vehicle is being flown using the primary system. What will happen if the BFS must be engaged subsequent to the failure? Will the fact that the failure has occurred prevent the BFS from operating properly, under any conditions? A "no" answer is a potential issue (requiring explanation) only if the BFS can normally tolerate the failure (when it occurs during BFS operation).

(2) Question 8.B. Consider that the failure occurs while the vehicle is under BFS control. A "no" answer is an issue (requiring explanation) only if the BFS response differs from that for the primary system.

4.2.2 Change/Retention Rationale Summary. Each failure is assigned to one of six possible groups, based upon the answers obtained in the checklist body. Boxes are provided to indicate the category assigned. Figure 4-2 presents the criteria for group assignment.

A box is also provided to indicate that changes are required to the FMEA. The FMEA evaluation of in-flight detectability is sometimes inaccurate and requires change. In addition, other errors (e.g., incorrect criticality assignment or incorrect evaluation of redundancy screens) are occasionally noted during the analysis and are documented here.

A space is provided to detail acceptance rationale, change recommendations, or suggested FMEA changes. This space may also be used to provide a short general comment to expand the retention rationale grouping.

4.2.3 Explanation/Comments. Each question answered by checking a box identified with an asterisk is discussed in this section. The circumstances for checking a box not identified with an asterisk are discussed, and the rationale for not making such a change is presented, if applicable. This section may also be used to explain, expand, or qualify answers. Each discussion is identified with the corresponding question number.

4.3 ANALYSIS SUMMARY. The analysis results are summarized on the basis of retention rationale grouping and recommended changes/retention rationale. Figure 4-3 depicts the form utilized for this purpose. A particular retention rationale definition, acceptance rationale statement, or recommended change is listed in the left column, with the applicable failure modes listed on the right. The issue/risk is briefly described with acceptance rationale or software requirements change recommendation. The summary provides a basic overview of the total analysis results.

5.0 ANALYSIS SUMMARY SHEETS. The analysis results are summarized on the following sheets. The failure modes have been grouped by issue/retention rationale (or change), affording an overview of the results for the entire subsystem.
CHANGE/RETENTION RATIONALE

1. NO * CHECKED - NO HARDWARE/SOFTWARE ISSUES ARE APPARENT FROM THE ANALYSIS. SYSTEM IS FAIL OPERATIONAL/FAIL SAFE WITH RESPECT TO THIS FAILURE MODE UNDER CURRENT DESIGN.

2. ONLY * CHECKED ON QUESTION 6 - NO HARDWARE/SOFTWARE ISSUES ARE APPARENT FROM THE ANALYSIS. RISK HAS BEEN ACCEPTED VIA HARDWARE CIL.

3. ONLY * (YES) CHECKED ON QUESTION 1a - NO SOFTWARE DETECTION IS PROVIDED. FAILURE EFFECT IS NOT TIME CRITICAL. FAILURE MAY BE DETECTED BY OTHER MEANS OR FUNCTION IS NOT MISSION/SAFETY CRITICAL.

4. * CHECKED ON QUESTION 3a - * ON 1a MAY OR MAY NOT BE CHECKED - SOFTWARE DOES NOT TAKE CORRECTIVE ACTION FOR FAILURE. FAILURE EFFECT IS NOT TIME CRITICAL. CORRECTIVE ACTION MAY BE INITIATED BY CREW. PLANNED CHECKOUT ACTIVITIES WILL DETECT FAILURE. SYSTEM IS FAIL OPERATIONAL/FAIL SAFE WITHOUT SOFTWARE DETECTION AND CORRECTION.

5. STANDARD RETENTION RATIONALE DOES NOT APPLY. SPECIFIC RETENTION RATIONALE IS SUMMARIZED FOR THIS FAILURE.

6. ISSUES IDENTIFIED AND CHANGES ARE DESIRABLE. SPECIFIC CHANGES ARE SUMMARIZED.

NOTE: DO NOT CONSIDER ANSWER TO QUESTION 2 IN DETERMINATION OF CHANGE/RETENTION RATIONALE SUMMARY CODE. CONSIDER RESPONSES TO BOTH QUESTION 2 AND 6 IN DETERMINING WHETHER AN FMEA CHANGE IS REQUIRED.

Figure 4-2. Change/Retention Rationale
<table>
<thead>
<tr>
<th>SUBSYSTEM</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>ANALYSIS RESULT</th>
<th>ITEM/FAILURE MODE</th>
</tr>
</thead>
</table>

Figure 4.3: Hardware/Software Analysis Summary
<table>
<thead>
<tr>
<th>HARDWARE ACCEPTS RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ITEM/Failure Mode</strong></td>
</tr>
<tr>
<td>Helium Storage Tank - Rupture (03-2F-101010-1)</td>
</tr>
<tr>
<td>Helium Feedline - External Leakage (03-2F-101013-1)</td>
</tr>
<tr>
<td>Quick Fill Disconnect, He - Fails Open, Cap Leaks (03-2F-101070-1)</td>
</tr>
<tr>
<td>Test Quick Disconnect, Propellant - Ext. Leakage/Flight (03-2F-101090-1)</td>
</tr>
<tr>
<td>Propellant Line Flex Assy. - External Leakage (03-2F-102106-1)</td>
</tr>
<tr>
<td>Feedline and Fittings - External Leakage (03-2F-102108-1)</td>
</tr>
<tr>
<td>AC Motor Operated Valve (Tank) - Fails Closed (03-2F-102120-1)</td>
</tr>
<tr>
<td>Quick Disconnect - External Leakage (03-2F-102150-1)</td>
</tr>
<tr>
<td>DC Solenoid Operated Valve - Fails Closed - Premature Operation (03-2F-102170-1)</td>
</tr>
<tr>
<td>Tank Assembly and Propellant Acquisition Device - Small Crack - External Leakage (03-2F-111110-2)</td>
</tr>
<tr>
<td>Tank Assembly and Propellant Acquisition Device - Restricted Flow (03-2F-111110-3)</td>
</tr>
<tr>
<td>Tank Assembly and Propellant Acquisition Device - Loss of Gas in Propellant Acquisition Device (03-2F-111110-4)</td>
</tr>
<tr>
<td>Flex Line and Fittings - External Leakage (03-2F-121308-1)</td>
</tr>
<tr>
<td>Thrust Chamber - Burn Through (03-2F-121312-1)</td>
</tr>
<tr>
<td>Nozzle Extension - Burn-Through (03-2F-121313-1)</td>
</tr>
<tr>
<td>Vernier Thruster - Erratic Operation (03-2F-131310-3)</td>
</tr>
<tr>
<td>Vernier Thruster - Burn-Through (03-2F-131310-4)</td>
</tr>
<tr>
<td>Helium Pressure Regulator - Fails Closed (03-2F-101030-2)</td>
</tr>
<tr>
<td>Tank Assembly and Propellant Acquisition Device - Large Rupture (03-2F-111110-1)</td>
</tr>
<tr>
<td>Purge Quick Disconnect, Propellant - External Leakage During Flight (03-2F-101080-1)</td>
</tr>
<tr>
<td>Helium Quad Check Valve - Fails Closed (03-2F-101095-2)</td>
</tr>
<tr>
<td>Vernier Thruster - Loss of Output (03-2F-131310-1)</td>
</tr>
<tr>
<td>ANALYSIS RESULT</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>NO HARDWARE/SOFTWARE ISSUES</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
HARDWARE/SOFTWARE ANALYSIS SUMMARY

<table>
<thead>
<tr>
<th>ANALYSIS RESULT</th>
<th>ITEM/FAILURE MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>OUT OF SCOPE - GROUND ONLY</td>
<td>Manual Valve - Fails Closed or Open (03-2F-101050-1)</td>
</tr>
<tr>
<td></td>
<td>Manual Valve - Internal Leakage (03-2F-101050-2)</td>
</tr>
<tr>
<td></td>
<td>Quick Fill Disconnect, He. - Fails Closed/Ground OPS (03-2F-101070-2)</td>
</tr>
<tr>
<td></td>
<td>Purge Quick Disconnect, Propellant - Fails Closed/Ground OPS. (03-2F-101080-2)</td>
</tr>
<tr>
<td></td>
<td>Test Quick Disconnect, Propellant - Fails Closed/Ground Ops (03-2F-101090-2)</td>
</tr>
<tr>
<td></td>
<td>Quick Disconnect - Fails Closed/Ground Ops. (03-2F-102150-2)</td>
</tr>
</tbody>
</table>
6.0 ANALYSIS CHECKLIST SHEETS

Following are the analysis checklist sheets for each failure mode evaluated.
### HARDWARE/SOFTWARE ANALYSIS CHECKLIST

**SUBSYSTEM:** Fwd Reaction Control  
**ITEM:** Helium Storage Tank  
**FMEA NUMBER:** SD75-SH-0016A  
**FAILURE MODE:** Rupture

<table>
<thead>
<tr>
<th>Question</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?</td>
<td>*YES</td>
<td>NO</td>
</tr>
<tr>
<td>2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?</td>
<td>YES</td>
<td>*NO</td>
</tr>
<tr>
<td>3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?</td>
<td>*YES</td>
<td>NO</td>
</tr>
<tr>
<td>3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?</td>
<td>YES</td>
<td>*NO</td>
</tr>
<tr>
<td>4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?</td>
<td>YES</td>
<td>*NO</td>
</tr>
<tr>
<td>5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?</td>
<td>YES</td>
<td>*NO</td>
</tr>
<tr>
<td>6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?</td>
<td>H/A</td>
<td>YES</td>
</tr>
</tbody>
</table>
| 8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:  
  A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?  
  B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE? | YES | *NO | |

*EXPLANATION REQUIRED (SEE BELOW)*

#### CHANGE/RETENTION RATIONALE SUMMARY

1. **[ ]** NO H/S ISSUES  
2. **[X]** HARDWARE ACCEPTS RISK  
3. **[ ]** NO SOFTWARE DETECTION  
4. **[ ]** DETECTION DURING CHECKOUT  
5. **[ ]** ACCEPTANCE RATIONALE BELOW  
6. **[ ]** RECOMMENDED CHANGES BELOW  
7. **[ ]** FMEA CHANGE RECOMMENDED

#### EXPLANATION/COMMENTS:

1. GAX will give a class 2 alert upon sensing an out-of-tolerance condition. (≤500 psi)  
Gross leak detection will give a class 2 alert.

8. Backup flight system same as primary.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 1C2

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: MC282-0082-0031/-0032
P/N VENDOR: ELD-999040
QUANTITY: 2
FAILURE DETECTABLE IN FLIGHT?: YES
PRESSURE INDICATION: V42P-1110C
GROUND TURNAROUND?: YES
SAME AS FLIGHT

PREPARED BY: DES J TAGGART
APPROVED BY: DES R DIEHL

ITEM: TANK
FUNCTION:
TO STORE HELIUM AT A MAX WORKING PRESSURE OF 4000 PSI FOR PRESSURIZATION OF THE FWD RCS MODULE PROPELLANT SUPPLY SYSTEM. TANK CONSISTS OF A DOUBLE MELT Ti LINER WITH DUPONT 49 FISER AND EPOXY RESIN FONDING OVER WRAP.

FAILURE MODE: RUPTURE, EXTERNAL LEAK (S)
RUPTURE - LARGE CRACK WHICH PROPAGATES AROUND TANK IMMEDIATELY.
LEAKAGE - FRACTURE WHICH DOES NOT PROPAGATE TO RUPTURE.

CAUSE(S):
VIBRATION, STRESS CORROSION, TEMP. RISE, FATIGUE, INADVERTENT OVER-PRESSURIZATION (GROUND OPS).

EFFECT(S): ON (A) SYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF PRESSURIZATION TO FUEL OR OXIDIZER. (B) EXPLOSIVE EXPANSION OF HELIUM WITHIN RCS MODULE. (C) POTENTIAL LOSS OF MISSION-ABORT DECISION DEPENDANT ON EXTENT OF DAMAGE. (D) POTENTIAL LOSS OF CREW/VEHICLE.

CORRECTING ACTION:
NONE AVAILABLE EXCEPT POSSIBLE RESCUE IF VEHICLE STILL INTACT.

REMARKS/HAZARDS:
HAZARD OF SHRAPNEL PROPAGATION, HOWEVER, UTILIZATION OF FILAMENT WOUND TANK MINIMIZES OR ELIMINATES THIS HAZARD. ADDITIONAL HAZARD OF MODULE OVER-PRESSURIZATION STILL EXISTS. NO REDUNDANCY PROVIDED FOR THIS ITEM - REFERENCE HAZARD 1YXX-0302-02.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N RS: 4262/000/0031/-0032
P/N VENDOR: BLD-999040
QUANTITY: 2

FUNCTION:
1. ASSEMBLY: PRESSURIZATION ABORT CRIT. FUNC: 1
2. P/N Ri: M4C282--OC82-0031/-0032
3. IT: M, HW: I
4. P/N VENDOR: BLD-999040
5. MISSIONS: HF VF X FF OF SM
6. QUANTITY: 2
7. PHASE(S): PL X LO X DO X DO X LS
8. REDUNDANCY SCREEN: A-N/A B-N/A C-N/A

PREPARED BY:
DEP: D. J. TAGGART
REL: R. DIEHL

DES: J. TAGGART
REL: R. DIEHL

ITEM: TANK
HELIUM STORAGE, FILAMENT WOUND.
FUNCTION:
1. TO STORE HELIUM AT A MAX WORKING PRESSURE OF 4000 PSI FOR
   PRESSURIZATION OF THE FWD RCS MODULE PROPellant SUPPLY SYSTEM. TANK
   CONSISTS OF A DOUBLE MELT Ti LINER WITH DUPONT 49 FIBER AND EPOXY RESIN
   BONDING OVER WRAP.
2. FAILURE MODE: RUPTURE, EXTERNAL LEAK (S)
3. RUPTURE - LARGE CRACK WHICH PROPAGATES AROUND TANK IMMEDIATELY.
4. LEAKAGE - FRACTURE WHICH DOES NOT PROPAGATE TO RUPTURE.
CAUSE(S):
1. VIBRATION, STRESS CORROSION, TEMP. RISE, FATIGUE, INADVERTENT
   OVER-PRESSURIZATION (GROUND OPS).
EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
1. (A) LOSS OF PRESSURIZATION TO FUEL OR OXIDIZER. (B) EXPLOSIVE
   EXPANSION OF HELIUM WITHIN RCS MODULE. (C) POTENTIAL LOSS OF
   MISSION-ABORT DECISION DEPENDANT ON EXTENT OF DAMAGE. (D) POTENTIAL
   LOSS OF CREW/VEHICLE.

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
1. (A) FILAMENT WOUND TANKS ARE DESIGNED TO LEAK BEFORE RUPTURE WHICH
   LIMITS FAILURE PROPAGATION DUE TO SCHRAPNEL. INCREASED STRAIN
   CAPABILITY IS PROVIDED BY THE COMPRESSIVE LOAD ON AN UNPRESSURIZED
   LINER. THE FACTOR OF SAFETY IS 1.5 X MAX WORKING PRESSURE OF 4000 PSI.
   DUAL SEALS ARE PROVIDED AT TANK FLANGE. (B) TANKS ARE SUBJECTED TO
   PROOF PRESSURE (1.6X WORKING PRESSURE) DURING ACCEPTANCE TESTING. QUAL
   TESTS INCLUDE 1000 PRESSURE CYCLES EQUAL TO 4 TIMES LIFE REQUIREMENT, 30
   DAY CREEP TEST AT MAX WORKING PRESSURE PLUS RANDOM VIBRATION AT
   ANTICIPATED MISSION LEVELS FOR 48 HOURS IN EACH AXIS. (C) IN PROCESS
   INSPECTION INCLUDES RADIO GRAPHIC INSPECTION OF WELDS & FLUORESCENT
   PENETRATION INSPECTION FOR SURFACE FLAWS. TURNAROUND CYCLE FOR EVIDENCE
   OF RUPTURE. AUDIT CONDUCTED 3/9/78 VERIFIED SUPPLIER RECEIVING
   INSPECTION CONTROLS RAW MATERIAL AND PURCHASED COMPONENTS AND IN-HOUSE
   INSPECTION CONTROLS CORROSION PROTECTIVE PROVISIONS, TEST HANDLING
   STORAGE ENVIRONMENTS, MEASUREMENT STANDARDS, TEST EQUIPMENT, NDE
   TESTING, PARTS PROTECTION, MFG PROCESSES AND FINISHES. CHEMICAL ETCHING,
   X-RAY AND PROOF TEST OF LINER AND MECHANICAL PROPERTIES AFTER HEAT
   TREAT ALSO VERIFIED BY INSPECTION. (D) NO HISTORY AVAILABLE. TANK IS
   BEING DEVELOPED FOR SHUTTLE PROGRAM.
HARDWARE/SOFTWARE ANALYSIS CHECKLIST 03-2F-101013-1

SUBSYSTEM Fwd Reaction Control

ITEM Helium Feedline

FMEA NUMBER SD75-SH-0016A

FAILURE MODE External Leakage

| 1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNOUNCE OR TAKE ACTION IN RESPONSE)? |
|--------------------------------------------------|--------------------------------------------------|
| YES [x] NO □ | *YES □ NO □ |

| 1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE? |
|--------------------------------------------------|--------------------------------------------------|
| YES □ NO [x] | *YES □ NO □ |

| 2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY? |
|--------------------------------------------------|--------------------------------------------------|
| YES □ NO [x] | *YES □ NO □ |

| 3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)? |
|--------------------------------------------------|--------------------------------------------------|
| YES □ NO [x] | *YES □ NO □ |

| 3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)? |
|--------------------------------------------------|--------------------------------------------------|
| YES □ NO [x] | *YES □ NO □ |

| 4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE? |
|--------------------------------------------------|--------------------------------------------------|
| YES □ NO [x] | *YES □ NO □ |

| 5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS? |
|--------------------------------------------------|--------------------------------------------------|
| YES □ NO [x] | *YES □ NO □ |

| 6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY. |
|--------------------------------------------------|--------------------------------------------------|
| YES [x] □ □ | *YES [x] □ □ |

| 7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION? |
|--------------------------------------------------|--------------------------------------------------|
| YES [x] □ □ | *YES [x] □ □ |

| 8. IF THE ANSWER TO EITHER 1 OR 3 IS YES: |
|--------------------------------------------------|--------------------------------------------------|
| A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE? |
| YES [x] □ □ | *YES [x] □ □ |

| B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE? |
|--------------------------------------------------|--------------------------------------------------|
| YES [x] □ □ | *YES [x] □ □ |

*EXPLANATION REQUIRED (SEE BELOW)

CHANGE/RETENTION: RATIONALE SUMMARY

<table>
<thead>
<tr>
<th>1. NO H/S ISSUES</th>
<th>3. NO SOFTWARE DETECTION</th>
<th>5. ACCEPTANCE RATIONALE BELOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. HARDWARE ACCEPTS RISK</th>
<th>4. DETECTION DURING CHECKOUT</th>
<th>6. RECOMMENDED CHANGES BELOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>[x]</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>

1. GAX will give a class 2 alert upon sensing an out-of-tolerance condition. (<500 psi)
Gross leak detection will give a class 2 alert.

8. Backup flight system same as primary.
SUBSYSTEM : FWD - REACTION CONTROL
ASSEMBLY : PRESSURIZATION HELIUM -
P/N RI : VG70-421701
P/N VENDOR:
QUANTITY : 2

FAILURE DETECTABLE IN FLIGHT?: YES
HELIUM TANK PRESSURE DROP AT OFF-NOMINAL RATE:
FUNCTION:

PREPARED BY:
APPROVED BY:

ITEM: HELIUM FEED LINE AND FLUID FITTINGS.
FUNCTION:

FAILURE MODE: EXTERNAL LEAKAGE

CAUSE(S):
MECHANICAL SHOCK, VIBRATION/FAILIUG, IMPROPER INSTALLATION.
FLUID FITTING SEAL FAILURE.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF HELIUM SUPPLY IF NOT ISOLATABLE. (IE. IF UPSTREAM OF SCLNDIC VALVE).
(B) POTENTIAL OVERPRESSURIZATION OF FORWARD TANK FROM GROSS LEAK.
(C,D) POTENTIAL MODULE DAMAGE RESULTING IN LOSS OF MISSION/CREW/VEHICLE IF GROSS LEAK OCCURS DURING CRITICAL MANEUVERS.

CORRECTING ACTION:
INITIATE ABORT. CHECK VALVES MAINTAIN PROPELLANT TANK RESIDUAL GAS PRESSURE TO ALLOW POTENTIAL FLIGHT DOWN MODE UTILIZATION.

REMARKS/HAZARDS:
NO REDUNDANCY PROVIDED FOR LINES. IF LEAK RATE IS EXCESSIVE PRESSURE BUILD-UP IN MODULE MAY RESULT IN HAZARDOUS. SEE HAZARD IYXX-0402-002.
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM : FWO - REACTION CONTROL

ASSEMBLY : PRESSURIZATION HELIUM

P/N RI : V070-421701

P/N VENDOR : ABCRT:

QUANTITY : 2

FUNCTION : CRIT.

P/N CRIT. HON:

MISSIONS: HF VF X FF OF SH

PHASE(S): PL X LO X CG X CO X LS X

ONE SET PER PROPELLANT

REDUNDANCY SCREEN: A-N/A B-N/4A C-N/A

PREPARED BY:

DES A SIEGELIN

REL R DIEHL

APPROVED BY:

APPROVED BY (NASA):

SSM

APPROVED WITH CHANGES

DES A SIEGELIN

REL R DIEHL

ITEM: HELIUM FEED LINE AND FLUID FITTINGS.

FUNCTION:

TO PROVIDE FEED LINE FROM HELIUM TANKS TO HELIUM REGULATION/PRESSURIZATION SYSTEM AND TO PROPELLANT TANKS.

FAILURE MODE: EXTERNAL LEAKAGE (S)

CAUSE(S):

MECHANICAL SHOCK, VIBRATION/FATIGUE, IMPROPER INSTALLATION (WELD), FLUID FITTING SEAL FAILURE.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:

(A) LOSS OF HELIUM SUPPLY IF NOT ISOLATABLE. (IE. IF UPSTREAM OF SOLENOID VALVE). (B) POTENTIAL OVERPRESSURIZATION OF FORWARD MODULE FROM GROSS LEAK. (C,D) POTENTIAL MODULE DAMAGE RESULTING IN LOSS OF MISSION/CREW/VEHICLE IF GROSS LEAK OCCURS DURING CRITICAL MANEUVERS.

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:

(A) FACTOR OF SAFETY OF 4.0 WILL MINIMIZE FAILURE POTENTIAL. FLUID FITTINGS HAVE DUAL SEALS. WELD CONSTRUCTION REDUCES JOINTS AND POSSIBLE LEAK PATHS. FASTENING CLAMPS AND TUBE BEND DESIGN ALLOWS DEGREE OF MOVEMENT WHICH HELPS PREVENTING LEAKS. (B) POST INSTALLATION TEST AND OPERATIONAL CHECKOUTS WILL VERIFY SYSTEM INTEGRITY. ALL LINES SUBJECTED TO 1.25 PROOF TEST. (C) IN PROCESS INSPECTION INCLUDES NOT L LEAK CHECKS DURING INSTALLATION. TURNAROUND INSPECTION INCLUDES MONITORING FUNCTIONAL TESTS DURING PRESSURIZATION CYCLE FOR EVIDENCE OF LEAKS WHERE ACCESSIBLE VISUALLY INSPECT FOR DAMAGE. HARDWARE INSPECTION IN ACCORDANCE WITH PLANNING REQUIREMENTS APPROVED BY NASA. (D) MINOR FAILURE HISTORY-CORROSION AND FAB PROBLEMS REPORTED DURING APOLLO PROGRAM AND CORRECTED.

WITH APPLICABLE TMO/TPC REQUIREMENT. HARDWARE INSPECTION IN ACCORDANCE WITH PLANNING REQUIREMENTS APPROVED BY NASA. (D) MINOR FAILURE HISTORY-CORROSION AND FAB PROBLEMS REPORTED DURING APOLLO PROGRAM AND CORRECTED.
SUBSYSTEM  Fwd Reaction Control  FMEA NUMBER  SD75-SH-0016A
ITEM  D, C. Solenoid Valve - Helium  FAILURE NODE  Fails to Close

1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY
  ANNUNCIATE OR TAKE ACTION IN RESPONSE)?  YES ☐ NO ☒ X
1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD
  USE TO DETECT THE FAILURE?  *YES ☐ NO ☒
2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA. EVALUATION OF
  IN-FLIGHT DETECTABILITY?  YES ☐ *NO ☒
3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE
  (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
  YES ☒ NO ☐
3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS
  FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE
  PROGRAM LOGIC)?  *YES ☐ NO ☒
4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR
  INDUCE ANOTHER FAILURE?  *YES ☒ NO ☐
5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT
  OTHER FUNCTIONS?  *YES ☒ NO ☐
6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW
  ACTION AND HARDWARE/SOFTWARE OPERATION)?  NOTE CHANGE TO FMEA CRITICALITY.
  *0 ☐ *1 ☒ 2 ☒
7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED
  TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?
  N/A ☒ YES ☐ NO ☐
8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:
   A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?  YES ☐ X ☒*NO ☐
   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?  YES ☐ X ☒*NO ☐
*EXPLANATION REQUIRED (SEE BELOW)

CHANGE/RETENTION RATIONALE SUMMARY
1. ☒ NO H/S ISSUES  3. ☒ NO SOFTWARE DETECTION  5. ☐ ACCEPTANCE RATIONALE BELOW
2. ☐ HARDWARE ACCEPTS RISK  4. ☐ DETECTION DURING CHECKOUT  6. ☐ RECOMMENDED CHANGES BELOW

EXPLANATION/COMMENTS:

1. Switch scan will detect failure in OPS-2 only and only on demand.
   May not be used on STS-1.
ITEM: VALVE, D.C. SOLENOID

OPERATED, HIGH PRESSURE. HE (2600-4000 PSI) SOLENOID ACTUATED, 51 STABLE, (1/2") (LV 101/102/103/104).

FUNCTION:

THESE VALVES ARE UTILIZED TO CONTROL HELIUM PRESSURIZATION OF THE RCS MODULE. IN THE OPEN POSITION A FLOW PATH IS PROVIDED FROM THE HELIUM SUPPLY TANK(S) TO THE REGULATOR(S). TWO PARALLEL PATHS ARE PROVIDED FOR FUEL AND OXIDIZER. ONE PATH IS NORMALLY OPEN PER TANK. THE VALVE IS CLOSED AND PARALLEL VALVE OPENED SUBSEQUENT TO A DOWNSTREAM FAILURE.

FAILURE MODE: FAILS TO CLOSE (F)

WHEN COMMANDED TO ISOLATE DOWNSTREAM FAILURES

CAUSE(S):

CONTAMINATION, VIBRATION, LOSS OF ELECTRICAL INPUT, IMPROPER OPENING ACTUATION, PIECE PART FAILURE.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:

(A, C, D) NO EFFECT, VALVE IS FUNCTIONED (CLOSED) ONLY SUBSEQUENT TO A 2ND ORDER FAILURE. (B) NO EFFECT, DOES NOT INTERFACE WITH OTHER SUBSYSTEMS.

CORRECTING ACTION:

NONE

REMARKS/HAZARDS:

NONE
HARDWARE/SOFTWARE ANALYSIS CHECKLIST

SUBSYSTEM  Fwd Reaction Control  FMEA NUMBER  SD75-SH-0016A
ITEM  D. C. Solenoid Valve - Helium  FAILURE MODE  Fails Closed

1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNOUNCE OR TAKE ACTION IN RESPONSE)?
   \[\text{YES} \quad \text{NO}\]

1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?
   \[\text{YES} \quad \text{NO}\]

2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?
   \[\text{YES} \quad \text{NO}\]

3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
   \[\text{YES} \quad \text{NO}\]

3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
   \[\text{YES} \quad \text{NO}\]

4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?
   \[\text{YES} \quad \text{NO}\]

5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?
   \[\text{YES} \quad \text{NO}\]

6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.
   \[\text{NO} \quad \text{YES} \quad \text{NO}\]

7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?
   \[\text{YES} \quad \text{NO}\]

8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:
   A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?
      \[\text{YES} \quad \text{NO}\]
   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?
      \[\text{YES} \quad \text{NO}\]

*EXPLANATION REQUIRED (SEE BELOW)

CHANGE/RETENTION RATIONALE SUMMARY

1. [ ] NO H/S ISSUES
2. [X] HARDWARE ACCEPTS RISK
3. [ ] NO SOFTWARE DETECTION
4. [ ] DETECTION DURING CHECKOUT
5. [ ] ACCEPTANCE RATIONALE BELOW
6. [ ] RECOMMENDED CHANGES BELOW

FMEA CHANGE RECOMMENDED

EXPLANATION/COMMENTS:

1. Switch scan will detect failure in OPS-2 only and only on demand. May not be used on STS-1.
SUBSYSTEM : FW5 - REACTION CONTROL
ASSEMBLY : PRESURIZATION
P/N : MC284-0419-0011/-0012
P/N VENDOR : 73E35
QUANTITY : 4
P/N VENDOR : 73E35
MISSIONS: HFVF XM F F OF SM
PHASE(S) : PL X LG X CG X OU X LS
2UG10D PER PRESSURANT
NUMBER OF SUCCESS PATHS REMAINING
AFTER FIRST FAILURE:
1
RELIABILITY SCREEN: A-PASS B-PASS C-FAIL
FAILURE DETECTABLE IN FLIGHT?: YES
TIME TO EFFECT:
MONITOR TANK PRESSURE AND POSITION INDICATION
V=2X-1120X, 1122X, 1124X, 1126X
GROUND TURNAROUND?: .............YES
SAME AS FLIGHT INSTR.

PREPARED BY:
DES , R BURKHART
REL , R DIEHL

ITEM: VALVE, D.C. SOLENOID (Helium - Prcsürization System)
OPERATED, HIGH PRESSURE HE (3600-4000 PSIA) SOLENOID ACTUATED,
BY STAPLES, (1/2") (LV 101/102/103/104).

FUNCTION:
THESE VALVES ARE UTILIZED TO CONTROL HELIUM PRESSURIZATION OF THE RCS
MODULE. IN THE OPEN POSITION A FLOW PATH IS PROVIDED FROM THE HELIUM
SUPPLY TANK(S) TO THE REGULATOR(S). TWO PARALLEL PATHS ARE PROVIDED
FOR FUEL AND OXIDIZER. ONE PATH IS NORMALLY OPEN PER TANK. THE VALVE
IS CLOSED AND PARALLEL VALVE OPENED SUBSEQUENT TO A DOWNSTREAM
FAILURE.

FAILURE MODE: Fails Closed

CAUSE(S):
VIBRATION, CONTAMINATION CONTINUOUS INADVERTENT CLOSING SIGNAL DUE TO
SHORT CIRCUIT, PIECE PART FAILURE.

EFFECT(S): UN (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF REDUNDANT PRESSURIZATION PATH, (B, C) NO EFFECT, (C)
ABORT DECISION DEPENDENT ON MISSION PHASE AND BLOWDOWN CAPABILITY.

CORRECTING ACTION:
IF CAUSED BY VIBRATION, THE VALVE MAY BE CAPABLE OF OPENING WITH A NEW
COMMAND OR, SWITCH TO PARALLEL REGULATION PATH - COMMAND PARALLEL
ISOLATION VALVE OPEN.

REMARKS/HAZARDS:
POTENTIAL HAZARD IN ABORT SITUATION. SEE CONSOLIDATED CONTROLS FMEA
NUMBER 73835 FMEA 1.

ORIGINAL PAGE IS OF POOR QUALITY
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM: FWO - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N RI: MC284-0419-0011/-0012
P/N VENDOR: 73835
QUANTITY: 4
HOW: VENDOR: 73835 MISSIONS: HF VF X FF OF SM
QUANTITY: 4
FUNCTION: CRIT.
MISSION: HF VF X FF OF SM
QUANTITY: 4
PHASE(S): PL X LO X DD X DO X LS

PREPARED BY: R BURKHART DES
APPROVED BY: (NASA):
REL R DIEHL REL

ITEM: VALVE, D.C. SOLENOID
OPERATED, HIGH PRESSURE, H E (3600-4000 PSIA) SOLENOID ACTUATED, BI-STABLE, (1/2") (LV 101/102/103/104).
FUNCTION:

THESE VALVES ARE UTILIZED TO CONTROL HELIUM PRESSURIZATION OF THE RCS MODULE. IN THE OPEN POSITION A FLOW PATH IS PROVIDED FROM THE HELIUM SUPPLY TANK(S) TO THE REGULATOR(S). TWO PARALLEL PATHS ARE PROVIDED FOR FUEL AND OXIDIZER; ONE PATH IS NORMALLY OPEN PER TANK, THE VALVE IS CLOSED AND PARALLEL VALVE OPENED SUBSEQUENT TO A DOWN STREAM FAILURE.

FAILURE MODE: FAILS CLOSED (F)

CAUSE(S):

VIBRATION, CONTAMINATION CONTINUOUS INADVERTENT CLOSING SIGNAL DUE TO SHORT CIRCUIT, PIECE PART FAILURE.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:

(A) LOSS OF REDUNDANT PRESSURIZATION PATH. (B, D) NO EFFECT. (C) ABD TO DEPENDENT ON MISSION PHASE AND BLOWDOWN CAPABILITY.

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:

(A) SERIES CONTROL CIRCUITRY PROVIDED TO MINIMIZE FAILURE MODE, 100 MICRON FILTER IS PROVIDED. MEDIA HAS BEEN FILTERED TO 25 MICRON PRIOR TO ENTERING TANK. SPECIAL EMPHASIS PLACED ON THE DESIGN AND LAYOUT OF SOLENOID WIRING TO PRECLUDE SHORTS. (B) QUAL TEST INCLUDES 48 MINUTES PER AXIS OF RANDOM VIBRATION AT ANTICAPTED MISSION LEVELS AND LIFE TESTING CONSISTING OF 2200 OPERATING CYCLES. ITEM IS USED DURING SYSTEM EVALUATION AT WHITE SANDS TESTING. (C) TURNAROUND INSPECTION INCLUDES MONITORING TESTS TO VERIFY ELECTRICAL POWER TO SOLENOID VALVE FOR EVIDENCE OF SHORT CIRCUIT. SUPPLIER AUDIT CONDUCTED 8-31-77 verified SUPPLIER INSPECTION EXERCISED CONTROL OF PARTS ID, PARTS PROTECTION, MFG PROCESSES, CONTAMINATION CONTROL, AND CORROSION PROTECTION VERIFICATION. (D) THERE IS NO FAILURE HISTORY FOR THIS SPECIFIC DESIGN.
**HARDWARE/SOFTWARE ANALYSIS CHECKLIST**

**SUBSYSTEM**: Fwd. Reaction Control  
**FMEA NUMBER**: SD75-SH-0016A  
**ITEM**: Helium Pressure Regulator  
**FAILURE MODE**: Fails Open

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>YES</th>
<th>NO</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNOUNCE OR TAKE ACTION IN RESPONSE)?</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?</td>
<td>*YES</td>
<td>NO</td>
<td>X</td>
</tr>
<tr>
<td>2. ARE THE ANSWERS TO QUESTIONs 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?</td>
<td></td>
<td><em>X</em></td>
<td><em>NO</em></td>
</tr>
<tr>
<td>3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?</td>
<td>*YES</td>
<td>NO</td>
<td>X</td>
</tr>
<tr>
<td>4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?</td>
<td>*YES</td>
<td>NO</td>
<td>X</td>
</tr>
<tr>
<td>5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?</td>
<td>*YES</td>
<td>NO</td>
<td>X</td>
</tr>
<tr>
<td>6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.</td>
<td>0</td>
<td><em>1</em></td>
<td><em>2</em></td>
</tr>
<tr>
<td>7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?</td>
<td>N/A</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?</td>
<td>YES</td>
<td><em>NO</em></td>
<td></td>
</tr>
<tr>
<td>B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?</td>
<td>YES</td>
<td><em>NO</em></td>
<td></td>
</tr>
</tbody>
</table>

**EXPLANATION/COMMENTS:**

1. Detection of this failure mode is not desired as these are redundant series regulators.

**CHANGE/RETENTION RATIONALE SUMMAR:**

1. **X** NO H/S ISSUES  
2.  
3. **X** NO SOFTWARE DETECTION  
4.  
5. **X** ACCEPTANCE RATIONALE BELOW  
6. **X** RECOMMENDED CHANGES BELOW  

**EXPLANATION/COMMENTS:**

Detection of this failure mode is not desired as these are redundant series regulators.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 102

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: MC284-0418
P/N VENDOR: 743390C1
QUANTITY: 4

FAILURE DETECTABLE IN FLIGHT? N/A
STANDBY UNIT

GROUNDCHECKOUTTEST PORTS

PREPARED BY: DES J. TAGGART
APPROVED BY: DES ____________

ITEM: REGULATOR, PRESS, HE,
SERIES REDUNDANT, SET AT UNEQUAL OUTLET PRESSURES - PRIMARY SET LOWER THAN SECONDARY (PR 101/102/103/104).

FUNCTION:
TO REGULATE STORED HELIUM PRESSURE FROM 4300 PSIG MAX TO ULLAGE PRESSURE OF 245 (+ OR -3) PSIG FOR PURPOSE OF PROPELLANT FED TO THRUSTERS. TWO PARALLEL PATHS WITH TWO SERIES REGS ARE PROVIDED FOR EACH PROPELLANT TANK.

FAILURE MODE: FAILS OPEN (F)
OR LEAKS INTERNALLY.

CAUSE(S):
CONTAMINATION, VIBRATION, PIECE PART STRUCTURAL FAILURE-FLEXURES, SEALS, POPPET ASSY.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF ONE REGULATOR ELEMENT IN ONE PATH (PRIMARY) AND RISE IN PROPELLANT FEED PRESSURE TO SECONDARY REGULATOR ELEMENT PRESSURE SETTING. (B, C, D) NONE.

CORRECTING ACTION:
NONE REQUIRED - SERIES REGULATOR ELEMENT WILL AUTOMATICALLY TAKE OVER FUNCTION.

REMARKS/HAZARDS:
SEE FAIRCHILD FMEA # RR74339-12.
**HARDWARE/SOFTWARE ANALYSIS CHECKLIST** 03-2F-101030-2

<table>
<thead>
<tr>
<th>SUBSYSTEM</th>
<th>Fwd Reaction Control</th>
<th>FMEA NUMBER</th>
<th>SD75-SH-0016A</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITEM</td>
<td>Helium Pressure Regulator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAILURE MODE</td>
<td>Fails Closed</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNOUNCE OR TAKE ACTION IN RESPONSE)?
   - YES X NO

1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?
   - YES X NO

2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?
   - YES X NO

3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
   - YES X NO

3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
   - YES X NO

4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?
   - YES X NO

5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?
   - YES X NO

6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.
   - YES X NO

7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?
   - N/A YES X NO

8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:
   A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?
      - YES X NO
   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?
      - YES X NO

*EXPLANATION REQUIRED (SEE BELOW)*

**CHANGE/RETENTION RATIONALE SUMMARY**

1. ☐ NO H/S ISSUES
2. ☑ HARDWARE ACCEPTS RISK
3. ☐ NO SOFTWARE DETECTION
4. ☐ DETECTION DURING CHECKOUT
5. ☐ ACCEPTANCE RATIONALE BELOW
6. ☐ RECOMMENDED CHANGES BELOW

FMEA should be changed from "NA" to "yes" for in-flight detectability via V42P1115C and 1116C.

[X] FMEA CHANGE RECOMMENDED

**EXPLANATION/COMMENTS:**

1. V42P1115C, 1116C, will sense the pressure drop initiating a class 2 alarm from GAX.
2. Failure is "hardware detectable" by V42P1115C and V42P1116C pressure drop.
3. Upon regulator failure the redundant parallel "leg" can be utilized.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORDER 102

SUBSYSTEM: FWG - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: MC284-0419
P/N VENDOR: 74255001
QUANTITY: 4
TWO REQUIRED PER
PRESSURANT PATH NUMBER OF SUCCESS PATHS REMAINING
AFTER FIRST FAILURE:
REDUNDANCY SCREEN: A-PASS B-PASS C-PASS
TIME TO EFFECT: MINUTES
REFERENCE DOCUMENTS:
VS70-421601
MJU70-0921-01E
5D72-5H-0103-2

PREPARED BY: APPROVED BY:
DES J. TAGGART DES
REL R. DIEHL REL

ITEM: REGULATOR, PRESS, HE
SERIES REDUNDANT SET AT UNEQUAL OUTLET PRESSURES - PRIMARY SET LOWER THAN SECONDARY (PR 101/102/103/104).
FUNCTION:
TO REGULATE STORED HELIUM PRESSURE FROM 4000 PSI MAX TO COLLAGE PRESSURE OF 245 (+/- 3) PSI FOR PURPOSE OF PROPellant FED TO THRUSTERS. TWO PARALLEL PATHS WITH TWO SERIES REGS ARE PROVIDED FOR EACH PROPellant TANK.

FAILURe MODE: FAILS CLOSED (F)
(LOW PRESSURE)

CAUSE(S):
CONTAMINATION (PARTIAL BLOCKAGE OF PILOT SCREEN) FRUZY MOISTURE PIECE PART FAILURE, VIBRATION.
EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF ONE REGULATOR PATH. (B,C) POTENTIAL ABORT BECAUSE ONE ADDITIONAL FAILURE MAY CAUSE LOSS OF PRESSURIZATION AND SUBSEQUENT VEHICLE LOSS. (D) NONE. (E) FUNCTIONAL CRITICALITY EFFECTS - IF FAILURE OCCUR BEFORE E1 SEPARATION, LOSS OF HELIUM WOULD PREVENT E1 SEPARATION AND LOSS OF CREW/VEHICLE WOULD RESULT.

CORRECTING ACTION:
CLOSE HIGH PRESSURE ISOLATION VALVE IN EFFECTED PATH AND OPEN HIGH PRESSURE ISOLATION VALVE IN PARALLEL PATH.

REMARKS/HAZARDS:
POTENTIAL ABORT BECAUSE ONE ADDITIONAL FAILURE (CLOSED) MAY CAUSE LOSS OF PRESSURIZATION AND SUBSEQUENT VEHICLE LOSS (REQUIRES 2ND OR 3RD FAILURE) DEPENDENT ON MISSION PHASE. SEE FAIRCHILD FMEA'S RK 74235-1E.
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N RI: HC284-0413
P/N VENDOR: 74339001
QUANTITY: 4

MISSIONS: HF VF X FF SF SM
PHASE(S): PL LO X 00 X DO X LS

PREPARED BY: J. TAGGART
REL: R DIEHL

ITEM: REGULATOR, PRESS, HE,
SERIES REDUNDANT, SET AT UNEQUAL OUTLET PressURES - PRIMARY SET LOWER THAN SECONDARY (PR 101/102/103/104).

FUNCTION:
TO REGULATE STORED HELIUM PRESSURE FROM 4000 PSIG MAX TO ULLAGE PRESSURE OF 245 (+ OR -3) PSIG FOR PURPOSE OF PROPELLANT FEED TO THRUSTERS. TWO PARALLEL PATHS WITH TWO SERIES PEGS ARE PROVIDED FOR EACH PROPELLANT TANK.

FAILURE MODE: FAILS CLOSED (F)

CAUSE(S):
CONTAMINATION (PARTIAL BLOCKAGE OF PILOT SCREEN) FROZEN MOISTURE PIECE PART FAILURE, VIBRATION.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF ONE REGULATOR PATH. (B,C) POTENTIAL ABORT BECAUSE ONE ADDITIONAL FAILURE MAY CAUSE LOSS OF PRESSURIZATION AND SUBSEQUENT VEHICLE LOSS. (D) NONE.

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
(A) EXPERIENCE FROM PREVIOUS REGULATOR DESIGN TO BE APPLIED TO PRECLUDE PIECE PART FAILURE AND SELF GENERATED CONTAMINATION. ALSO, 25 MICRON INTEGRAL INLET FILTER PROVIDED TO MINIMIZE CONTAMINANTS. (B) QUAL TESTING INCLUDES 25 HOUR SAND AND DUST TEST, 48 MINUTES PER AXIS OF RANDOM VIBRATION AT ANTICIPATED MISSION LEVELS AND LIFE CYCLE TESTS OF 50,000 CYCLES FOR THE MAIN STAGE AND 100,000 CYCLES FOR PILOT STAGE. (C) TURNOVER INSPECTION INCLUDES MONITORING TESTS TO VERIFY FUNCTIONAL OPERATION IS WITHIN SPECIFIED LIMITS. SUPPLIER AUDIT CONDUCTED VERIFIES WITHIN SPECIFIED LIMITS. SUPPLIER AUDIT CONDUCTED VERIFIES SUPPLIER CONTAMINATION CONTROL, AND STORAGE ENVIRONMENT. (D) NEW DESIGN FOR SHUTTLE APPLICATION. NO FAILURE HISTORY DATA AVAILABLE FOR THIS DESIGN.
1. **Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?**
   - YES □ NO □
   1a. **If not, does the hardware provide information that the flight software could use to detect the failure?**
   - YES □ NO □
2. **Are the answers to Questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?**
   - YES □ NO □
3. **Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?**
   - YES □ NO □
3a. **If not, does the capability exist for the software to compensate for this failure mode (either by commanding hardware action or implementing alternate program logic)?**
   - YES □ NO □
4. **As a result of this failure mode, can the software overstress the hardware or induce another failure?**
   - YES □ NO □
5. **Can this failure mode, in combination with software logic, adversely affect other functions?**
   - YES □ NO □
6. **How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)? Note change to FMEA criticality.**
   - 0 □ 1 □ 2 □
7. **If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?**
   - N/A □ YES □ NO □
8. **If the answer to either 1 or 3 is yes:**
   - A. Can the BFS be engaged after occurrence? YES □ NO □
   - B. Will BFS tolerate failure without loss of crew/vehicle? YES □ NO □

**Explanation/Required (see below)**

**Change/Retention Rationale Summary**
1. □ No H/S issues
2. □ Hardware accepts risk
3. □ No software detection
4. □ Detection during checkout
5. □ Acceptance rationale below
6. □ Recommended changes below

**FMEA Change Recommended**

**Explanation/Comments:**

1. If valve is cracked open V42P1115A, 1116A would alarm.
6. There are no success paths remaining after first failure.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORPITER 102

SUBSYSTEM: FWO - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N RI: MC284-0460-001/002
P/N VENDOR: 5760015, 5760016
QUANTITY: 2

ATM. FUNC:

MISSIONS: UF VF X FF OF SM
PHASE(S): PL LD X GO X DG X LS

NUMBER OF SUCCESS PATHS REMAINING
AFTER FIRST FAILURE:

FAILURE DETECTABLE IN FLIGHT? Y
PROPELLANT TANK PRESSURE: V42P-1210, 1115, 1116, 1310

GROUND TURNAROUND? YES
SAME AS FLIGHT

PREPARED BY:

APPROVED BY:

DESG R. GONZALEZ
REL R DIEHL

ITEM: VALVE, MANUAL-OPERATED.
FUNCTION:
TO PROVIDE ISOLATION OF PROPELLANT TANK(S) FROM PRESSURE CYCLES WHILE PERFORMING GROUND C/O AND/OR SERVICING OF PRESSURIZATION SYSTEM.

FAILURE MODE: FAILS CLOSED OR OPEN ( _ )
STRUCTURAL FAILURE.

CAUSE(S):
SEVERE MECHANICAL SHOCK OR VIBRATION CAUSING DETENT MOVEMENT ON A DEFICIENT VALVE LOSS OF INTERLOCK BY FRACTURE OF DRIVE FINGER OR RUCKER, CORROSION, CONTAMINATION, IMPROPER USE.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) (B) LOSS OF FUNCTION (IN ABILITY TO PERFORM SYS C/O). (C) LAUNCH DELAY. (D) NO EFFECT.

CORRECTING ACTION:
NONE AVAILABLE.

REMARKS/HAZARDS:
NO HAZARDS IDENTIFIED.

REFERENCE DOCUMENTS:
SD72-2M-0103-2
VS70-421001

ORIGINAL PAGE IS OF POOR QUALITY
### HARDWARE/SOFTWARE ANALYSIS CHECKLIST 03-2F-101050-2

**SUBSYSTEM** Fwd. Reaction Control  
**FMEA NUMBER** SD75-SH-0016A  
**ITEM** Manual Valve  
**FAILURE MODE** Internal Leakage

1. **DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?**  
   - YES ☒ ☐ NO ☐

1a. **IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?**  
   - YES ☐ ☐ NO ☒

2. **ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?**  
   - YES ☒ ☐ NO ☐

3. **DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**  
   - YES ☐ ☐ NO ☒

3a. **IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**  
   - YES ☒ ☐ NO ☐

4. **AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?**  
   - YES ☐ ☐ NO ☒

5. **CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?**  
   - YES ☐ ☐ NO ☒

6. **HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)?**  
   - YES ☒ ☐ NO ☐

7. **IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?**  
   - YES ☒ ☐ NO ☐

8. **IF THE ANSWER TO EITHER 1 OR 3 IS YES:**  
   A. **CAN THE BFS BE ENGAGED AFTER OCCURRENCE?**  
      - YES ☒ ☐ NO ☐
   B. **WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?**  
      - YES ☒ ☐ NO ☐

<table>
<thead>
<tr>
<th>CHANGE/RETENTION RATIONALE SUMMARY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ☐ NO H/S ISSUES</td>
</tr>
<tr>
<td>2. ☒ HARDWARE ACCEPTS RISK</td>
</tr>
</tbody>
</table>

**EXPLANATION/COMMENTS:**

1. If valve is cracked open V42P1115A, 1116A would alarm.

6. There are no success paths remaining after first failure.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
PN RL: MC284-0480-0001/-0002
PN VENDOR: 5760015, 5760016
QUANTITY: 2
ONE REQ'D PER TANK

FAILURE DETECTABLE IN FLIGHT?: YES
PROPELLANT TANK PRESSURE V42P-1210,1115,1116,1310 SECONDS TO MINUTES
GROUND TURNAROUND? .......... YES
SAME AS FLIGHT

FAILURE MODE: EXCESSIVE INTERNAL LEAKAGE.
CAUSE(S):
SEVERE MECHANICAL SHOCK OR VIBRATION CAUSING DETENT MOVEMENT ON A DEFICIENT VALVE LOSS OF INTERLOCK BY FRACTURE OF UPVE FINGER OR RUCKER, CORROSION, CONTAMINATION, IMPROPER USE.
EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A,B) LOSS OF FUNCTION (IN ABILITY TO PERFORM SYS C/O), (C) LAUNCH DELAY, (D) NO EFFECT.
CORRECTING ACTION:
NONE AVAILABLE.
REMARKS/HAZARDS:
NO HAZARDS IDENTIFIED.
### HARDWARE/SOFTWARE ANALYSIS CHECKLIST

**SUBSYSTEM:** Fwd Reaction Control  
**FMEA NUMBER:** SD75-SH-0016A

<table>
<thead>
<tr>
<th>ITEM</th>
<th>Relief Valve</th>
<th>FAILURE MODE</th>
<th>External Leakage Overboard</th>
</tr>
</thead>
</table>

1. **DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?**
   - **YES** ✗ **NO**

1a. **IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?**
   - **YES** ☐ **NO**

2. **ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?**
   - **YES** ✗ **NO**

3. **DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**
   - **YES** ☐ **NO** ✗

3a. **IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**
   - **YES** ☐ **NO** ✗

4. **AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?**
   - **YES** ☐ **NO** ✗

5. **CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?**
   - **YES** ☐ **NO** ✗

6. **HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)?**
   - **0** ☐ **1** ☐ **2** ✗

7. **IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?**
   - **N/A** ☐ **YES** ✗ **NO**

8. **IF THE ANSWER TO EITHER 1 OR 3 IS YES: A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?**
   - **YES** ☐ **NO** ✗
   
   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?**
   - **YES** ☐ **NO** ✗

***EXPLANATION REQUIRED (SEE BELOW)***

### CHANGE/RETENTION RATIONALE SUMMARY

1. ☐ **NO H/S ISSUES**  
2. ✗ **HARDWARE ACCEPTS RISK**  
3. ☐ **NO SOFTWARE DETECTION**  
4. ☐ **DETECTION DURING CHECKOUT**  
5. ☐ **ACCEPTANCE RATIONALE BELOW**  
6. ☐ **RECOMMENDED CHANGES BELOW**

---

**EXPLANATION/COMMENTS:**

1. Leakage of helium will cause a class 2 alarm.
   Gross leak detection should occur first.
**SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORIENTEX 102**

**SUBSYSTEM** : FW - REACTION CONTROL  
**ASSY/MPLY** : PRESSURIZATION  
**P/N RI** : MC284-0421-0001/-0002  
**P/N VENDOR** : 5760060-9-101, 5760010-102

<table>
<thead>
<tr>
<th>QUANTITY</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHASE(S)</td>
<td>PL LG X 00 X GO X LS</td>
</tr>
<tr>
<td>MISSION(S)</td>
<td>HF VF X FF UF SM</td>
</tr>
</tbody>
</table>

**QTY: 0 /“/Z**

<table>
<thead>
<tr>
<th>ASSMFLY</th>
<th>PRFSSURIZATION ABORT: CRIT. FUNC:</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRIT. hnd: 5</td>
<td></td>
</tr>
</tbody>
</table>

**FUNCTION**: RELIEF VALVE PROVIDED TO PREVENT RISE OF TANK AND LINE PRESSURES TO LEVELS WHICH COULD BE DETERSIMENTAL TO SUBSYSTEM.

**FAILURE MODE**: EXTERNAL LEAK

**CAUSE(S)**:
- GALVANIC CORROSION
- IMPROPER INSTALLATION/HANDLING
- FATIGUE
- STRUCTURAL FAILURE

**EFFECT(S)**: ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
- (A&B) SUBSYSTEM DEGRADATION - HELIUM LEAKS OVERBOARD AT RATE CONTROLLED BY ORIFICE. (C&D) NO EFFECT UNLESS LEAK IS EXCESSIVE.

**CORRECTING ACTION**: MONITOR SYSTEM FOR HELIUM LOSS.

**REMARKS/HAZARDS**:
- NO HAZARD IDENTIFIED.
<table>
<thead>
<tr>
<th>HARDWARE/SOFTWARE ANALYSIS CHECKLIST</th>
<th>03-2F-101060-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUBSYSTEM</td>
<td>Fwd. Reaction Control</td>
</tr>
<tr>
<td>ITEM</td>
<td>Relief Valve</td>
</tr>
<tr>
<td>FAILURE MODE</td>
<td>Burst Disc Ruptures</td>
</tr>
</tbody>
</table>

1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?
   - YES [X] NO [ ]

1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?
   - YES [ ] NO [X]

2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?
   - YES [X] NO [ ]

3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
   - YES [X] NO [ ]

3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
   - YES [X] NO [ ]

4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?
   - YES [X] NO [ ]

5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?
   - YES [X] NO [ ]

6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.
   - 0 [ ] 1 [X] 2 [X]

7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?
   - YES [X] NO [ ]

8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:
   A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?
      - YES [X] NO [ ]
   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?
      - YES [X] NO [ ]

*EXPLANATION REQUIRED (SEE BELOW)

CHANGE/RETENTION RATIONALE SUMMARY
1. [ ] NO H/S ISSUES
2. [X] HARDWARE ACCEPTS RISK
3. [ ] NO SOFTWARE DETECTION
4. [ ] DETECTION DURING CHECKOUT
5. [ ] ACCEPTANCE RATIONALE BELOW
6. [ ] RECOMMENDED CHANGES BELOW

In-Flight Detectability

[ ] FMEA CHANGE RECOMMENDED

EXPLANATION/COMMENTS:

1. May see discrete drop in RCS quantity. V42P1115C, 1116C will give class 2 caution and warning alarm.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 1C

SUBSYSTEM: FWD - REACTION CONTROL

ASSEMBLY: PRESSURIZATION

P/N RI: MC284-0421-0001/-0002

P/N VENDOR: 5760100-9-101, 5760010-102

QTY: 2

P/N VENDOR: 5760100-9-101, 5760010-102

MISSIONS: HF VF X HF UF SM

PHASE(S): PL X LO X CU X DO X LS

MO: ONE REQ'D PER TANK

NUMBER OF SUCCESS PATHS REMAINING: 2

AFTE FIRST FAILURE:

REDUNDANCY SCREEN: A-PASS B-PASS C-PASS

FAILUE DETECTABLE IN FLIGHT: NO

GROUND TURNAROUND: NO

PREPARED BY: DES R GONZALEZ

APPROVED BY: DES R DIEHL

ITEM: VALVE, PRESS. RELIEF - CRCKNG PRESS 315 PSIG, FULL OPEN 346 PSIG, RESEAT 31C PSIG (RV 1C/102).

FUNCTION:

RELIEF VALVE PROVIDED TO PREVENT RISE OF TANK AND LINE PESSURES TO LEVELS WHICH COULD BE DETRIMENTAL TO SUBSYSTEM.

FAILURE MODE: FAILS OPEN

BURST DISC RUPTURES.

CAUSE(S):

REGULATOR PRESSURE SURGE, INCORRECT PRESSURE SETTING, FATIGUE, EXCESS PRESSURE CYCLING, VIB, MAT'L DEFECT PROP TEMP RISES.

EFFECT(S): ON (A) SUBSYSTEM (B)INTERFACES (C)MISSION (D)CREW/VEHICLE:

(A, B) LOSS OF REDUNDANCY (LEAKAGE OR OPEN MODE) (MAIN POPPET PROVIDES REDUNDANCY). (C, D) NO EFFECT.

CORRECTING ACTION:

MONITOR SYSTEM FOR POTENTIAL HELIUM LOSS OR PROP, TANK PRESSURE DECREASE. REPLACE VALVE AFTER LANDING.

REMARKS/HAZARDS:

NO HAZARDS IDENTIFIED.
**HARDWARE/SOFTWARE ANALYSIS CHECKLIST 03-2F-101060-3**

**SUBSYSTEM**  
Fwd Reaction Control

**ITEM**  
Relief Valve

**FMEA NUMBER**  
SD75-SH-0016A

**FAILURE MODE**  
Fails to Burst

---

1. **DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?**  
   - YES ✗ NO ☐

1a. **IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?**  
   - *YES* ☐ *NO* ☐

2. **ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?**  
   - YES ✗ *NO* ☐

3. **DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**  
   - *YES* ☐ *NO* ✗

3a. **IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**  
   - *YES* ☐ *NO* ✗

4. **AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?**  
   - *YES* ☐ *NO* ✗

5. **CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?**  
   - *YES* ☐ *NO* ✗

6. **HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)?**  
   - NOTE CHANGE TO FMEA CRITICALITY.  
   - ✗ *NO* *2* ☐

7. **IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?**  
   - N/A ✗ *YES* ☐ *NO* ☐

8. **IF THE ANSWER TO EITHER 1 OR 3 IS YES:**
   - A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?  
     - YES ✗ *NO* ☐
   - B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?  
     - YES ✗ *NO* ☐

*EXPLANATION REQUIRED (SEE BELOW)*

---

**CHANGE/RETENTION RATIONALE SUMMARY**

1. ☐ NO H/S ISSUES  
2. ☑ HARDWARE ACCEPTS RISK  
3. ☐ NO SOFTWARE DETECTION  
4. ☐ DETECTION DURING CHECKOUT  
5. ☐ ACCEPTANCE RATIONALE BELOW  
6. ☑ RECOMMENDED CHANGES BELOW

---

**EXPLANATION/COMMENTS:**

1. Over pressurization will cause class 2 alarm; >312 psi. (GAX)  
   V42P1115C, 1116C.
## Shuttle Failure Mode and Effects Analysis - Orbiter 102

**Subsystem:** FWD - Reaction Control  
**Assembly:** Pressure  
**P/N:** MC284-0421-0301/-CG02  
**P/N Vendor:** 5760009-101, 57600010-102  
**Quantity:** 2  
**One Req'd Per Tank**  
**Mission:** HF/VF/FF/OF/SN  
**Phase(s):** PL/LO/DO/XO/XL  
**Failure Detectable in Flight?** Yes  
**Ground Turnaround?** Yes  
**Turnaround Test Port Provided**  

---

### Correcting Action:
- Close helium isolation valves, however relief could be completed by firing thrusters.

### Remarks/Hazards:
- No hazards, unit is standby - backup for regulator failures. No redundancy provided.

---

**Prepared By:** DES R Gonzalez  
**Approved By:** DES R Diehl  

---

**Item:** Valve, Press. Relief  
**Function:** Relief valve provided to prevent rise of tank and line pressures to levels which could be detrimental to subsystem.  
**Failure Mode:** Fails to burst  
**Cause(s):** Improper installation or handling damage that causes disc to stick, piece part failure, pressure build up on reverse side.  
**Effect(s):** On (A) subsystem (B) interfaces (C) mission (D) crew/vehicle:  
(A) No effect unless multiple failures occur.  
(B) Degradation of interface subsystem. Prop tank ullage pressure may increase above working pressure limits.  
(C, D) None see (A) above.

---

**Reference Documents:**
- MJ070-CC01-01E  
- S072-5H-CC01-01L  
- VST0-421061

---

**Notes:**
- Quantity: 2  
- One Req'd Per Tank  
- Failure Detectable in Flight? Yes  
- Ground Turnaround? Yes  
- Turnaround Test Port Provided  

---

**Failure Mode and Effects Analysis - Orbiter 102**

---

**Original Page Is Of Poor Quality**
1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNOUNCE OR TAKE ACTION IN RESPONSE)?  
   YES ☑  NO ☐
1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?  
   *YES ☐  NO ☑
2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?  
   YES ☑  *NO ☐
3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?  
   YES ☑  NO ☑
3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?  
   *YES ☑  NO ☑
4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?  
   *YES ☑  NO ☑
5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?  
   *YES ☑  NO ☑
6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDE CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.  
   *0 ☐  *1 ☑  *2 ☑
7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?  
   N/A ☐  YES ☑  *NO ☐
8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:
   A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?  
      YES ☑  *NO ☐
   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?  
      YES ☑  *NO ☐

*EXPLANATION REQUIRED (SEE BELOW)

CHANGE/RETIEMENT RATIONALE SUMMARY
1. ☐ NO H/S ISSUES  
2. ☑ HARDWARE ACCEPTS RISK  
3. ☐ NO SOFTWARE DETECTION  
4. ☐ DETECTION DURING CHECKOUT  
5. ☑ ACCEPTANCE RATIONALE BELOW  
6. ☑ RECOMMENDED CHANGES BELOW

EXPLANATION/COMMENTS:

1. Leakage of helium will cause an oxidizer/fuel imbalance of 12.6 percent. May get a gross leak detection alarm.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: MC284-0421-0001-0002
P/N VENDOR: 576000-9-101, 5760010-102
QUANTITY: 2
ONE REQ'D PER TANK
ABORT: CRIT. FUNK:
MISSIONS: HF, VF, FF, OH, SM
PHASE(S): PL, LU, DO, DO, X, LS
NUMBER OF SUCCESS PATHS REMAINING
AFTER FIRST FAILURE:
RELIABILITY SCREEN: A, E, C
FAILURE DETECTABLE IN FLIGHT? NO
UNLESS EXCESSIVE PRESSURE DROP IS EVIDENT IN TANKAGE
GROUND TURNAROUND?..............NO
SAME AS FLIGHT

PREPARED BY:
DES R GONZALEZ
REL R DIEHL
APPROVED BY:

ITEM: VALVE, PRESS. RELIEF
CRACKING PRESS 315 PSIG, FULL OPEN 240 PSIG, RESEAT 21C PSIG (RV 101/102).

FUNCTION:
RELIEF VALVE PROVIDED TO PREVENT RISE OF TANK AND LINE PRESSURES TO LEVELS WHICH COULD BE DETERIMENTAL TO SUBSYSTEM.

FAILURE MODE: PREMATURE/ERRATIC OPERATION
TION, INTERNAL LEAKAGE, OPEN BELOW NOMINAL CRACKING PRESSURE.
CAUSE(S):
VIBRATION, MECHANICAL SHOCK, CONTAMINATION, PIECE PART STRUCTURAL FAILURE OF POPPET.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CRAFT/VEHICLE:
(A) LOSS OF HELIUM OR PROPELLANT VAPORS OVERBOARD. (B) INABILITY TO PRESSURIZE PROPELLANT TANKS IF LEAK IS EXCESSIVE. (C) POTENTIAL ABORT IF EARLY IN MISSION, WOULD REQUIRE PRIOR FAILURE (BURST DISC OPEN). (D) NONE.

CORRECTING ACTION:
NONE.

REMARKS/HAZARDS:
WOULD REQUIRE BURST DISC FAILURE BEFORE LEAKS OVERBOARD. NO REDUNDANCY PROVIDED.

ORIGINAL PAGE IS OF POOR QUALITY
<table>
<thead>
<tr>
<th></th>
<th>HARDWARE/SOFTWARE ANALYSIS CHECKLIST 03-2F-101060-5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SUBSYSTEM</strong></td>
<td>Fwd Reaction Control</td>
</tr>
<tr>
<td><strong>ITEM</strong></td>
<td>Relief Valve</td>
</tr>
<tr>
<td><strong>FMEA NUMBER</strong></td>
<td>SD75-SH-0016A</td>
</tr>
<tr>
<td><strong>FAILURE MODE</strong></td>
<td>Fails to Open</td>
</tr>
</tbody>
</table>

1. **Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?**
   - Yes [ ]
   - No [ ]
2. **If not, does the hardware provide information that the flight software could use to detect the failure?**
   - Yes [ ]
   - No [ ]
3. **Are the answers to questions 1 and 2 consistent with the FMEA evaluation of in-flight detectability?**
   - Yes [ ]
   - No [ ]
4. **Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?**
   - Yes [X]
   - No [ ]
5. **If not, does the capability exist for the software to compensate for this failure mode (either by commanding hardware action or implementing alternate program logic)?**
   - Yes [ ]
   - No [X]
6. **As a result of this failure mode, can the software overstress the hardware or induce another failure?**
   - Yes [ ]
   - No [X]
7. **Can this failure mode, in combination with software logic, adversely affect other functions?**
   - Yes [ ]
   - No [X]
8. **How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)? Note change to FMEA criticality.**
   - Yes [ ]
   - No [X]
9. **If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?**
   - Yes [X]
   - No [ ]
10. **If the answer to either 1 or 3 is Yes:**
    - A. Can the BFS be engaged after occurrence? [X]
    - B. Will BFS tolerate failure without loss of crew/vehicle? [X]

**EXPLANATION REQUIRED**

**CHANGE/RETENTION RATIONALE SUMMARY**

1. [ ] No H/S issues
2. [X] Hardware accepts risk
3. [ ] No software detection
4. [ ] Detection during checkout
5. [ ] Acceptance rationale below
6. [ ] Recommended changes below

**EXPLANATION/COMMENTS:**

1. Over pressurization will cause a class 2 alarm, V42P1115C, 1116C.
SUBSYSTEM: REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: MC284-C421-0001/-0002
P/N VENDOR: 5760009-101, 5760010-102
QUANTITY: 2
PHASE(S): PL X LU X CO X CO X LS
ONE REQ'D PER TANK

FAILURE DETECTABLE IN FLIGHT? YES
TANK PRESSURE MONITOR V42P-1116C,1115C,121CC
GROUN TURNAROUND? YES
SAME AS FLIGHT

PREPARED BY: DES R GONZALEZ
APPROVED BY: DES R DIEHL

ITEM: VALVE, PRESS. RELIEF -
CRACKING PRESS 315 PSIG, FULL OPEN 340 PSIG, RESEAT 310 PSIG (RV 101/102).

FUNCTION:
RELIEF VALVE PROVIDED TO PREVENT RISE OF TANK AND LINE PRESSURES TO LEVELS WHICH COULD BE DETRIMENTAL TO SUBSYSTEM.
FAILURE MODE: FAILS TO OPEN - (F)
AT NOMINAL CRACKING PRESSURE .
CAUSE(S):
CONTAMINATION, PIECE PART STRUCTURAL FAILURE, POPPET GALLING.
EFFECT(S): ON (A) SUBSYSTEM (E) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF RELIEF PATH. (B,D) NONE. (C) POTENTIAL MISSION LOSS
(ABORT DECISION) IF EARLY IN MISSION WOULD REQUIRE 2 PRIOR FAILURES.
CORRECTING ACTION:
FIRE ALL THRUSTERS NON-PROPELLISIVELY.
REMARKS/HAZARDS:
POTENTIAL TANK RUPTURE ON 3RD ORDER FAILURE NO OTHER RELIEF PATH FOR SYSTEM.
1. **Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?**
   - **Yes** × No □
   - **1a.** If not, does the hardware provide information that the flight software could use to detect the failure?
   - **Yes** × No □

2. **Are the answers to questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?**
   - **Yes** □ No X

3. **Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?**
   - **Yes** □ No X
   - **3a.** If not, does the capability exist for the software to compensate for this failure (either by commanding hardware action or implementing alternate program logic)?
   - **Yes** □ No X

4. **As a result of this failure mode, can the software overstress the hardware or induce another failure?**
   - **Yes** □ No X

5. **Can this failure mode, in combination with software logic, adversely affect other functions?**
   - **Yes** □ No X

6. **How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)?** Note change to FMEA criticality.
   - **0** □ 1 X 2 □

7. **If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?**
   - **N/A** □ Yes X No □

8. **If the answer to either 1 or 3 is Yes:**
   - **A.** Can the BFS be engaged after occurrence?
     - **Yes** X *No □
   - **B.** Will BFS tolerate failure without loss of crew/vehicle?
     - **Yes** X *No □

*Explanation required (see below)*

**Change/Retention Rationale Summary**

1. □ No H/S issues
2. X Hardware accepts risk
3. □ No software detection
4. □ Detection during checkout
5. □ Acceptance rationale below
6. □ Recommended changes below

**Explanation/Comments:**

1 & 2. V42P1110C, V42P1112C, V42P1113C and V42P1114C will detect the failure when the pressure drops to 500 psi and issue a class 3 caution and warning alert.

Gross leak indication should occur first. (12.6% Δ)

6. Capped quick disconnect provides one redundant success path.
SUBSYSTEM: FWD - REACTION CONTROL

ASSEMBLY: PRESSURIZATION

P/N RI: MG276-0017-0402/0403

P/N VENDOR: 75372095-0402/0403

QUANTITY: 2

ONE REG'D PER TANK

MISSIONS: HF VF X FF CF SM

PHASE(S): PL X LO X 00 X DC X LS X

NUMBER OF SUCCESS PATHS REMAINING:

AFTER FIRST FAILURE:

REDUNDANCY SCREEEN: A-N/A B-N/A C-N/A

FAILRE DETECTABLE IN FLIGHT?: NO

GROUND TURNAROUND?: YES

VISUAL INSPECTION PRIOR TO LAUNCH

PREPARED BY:

DES C SCARLETT

APPROVED BY:

DES R DIEHL

ITEM: DISCONNECT, QUICK FILL

HELIUM WITH SPRING LOADED POPPET AND STRUCTURAL END CAP (1/4").

FUNCTION:

PROVIDES HELIUM TANK FILL POINT FOR GROUND OPERATIONS AND LOADING SERVICING.

FAILURE MODE: FALLS OPEN, CAP (S)

LEAKS IN EXCESS OF ACCEPTABLE RATE.

CAUSE(S):

VIBRATION, AND LOOSENING OF THE RETAINER NUT, IMPROPER HANDLING, MECHANICAL SHOCK.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:

(A) LOSS OF REDUNDANCY. (B) NONE. (C) POTENTIAL LAUNCH DELAY

(MISSION LOSS) IF DETECTED. (D) POSSIBLE LOSS OF CREW/VEHICLE IF FAILURE OCCURS PRIOR TO ET SEPARATION.

CORRECTING ACTION:

REPLACE OR TIGHTEN END CAP ON GROUND. NONE AVAILABLE IN FLIGHT.

REMARKS/HAZARDS:

BECAUSE STRUCTURAL CAP IS LOADED OVER THE DISCONNECT, THIS FAILURE MODE IS VERY REMOTE IN FLIGHT.
SUBSYSTEM: FWD – REACTION CONTROL  
ASSEMBLY: PRESSURIZATION  
P/N R: MCZ 76-0017-0402/0403  
P/N VENDOR: 75372000-0402/0403  
MISSION: HF VF X FF OF SM  
PHASE(S): PL X LO X DD X DO X LS X  
QUANTITY: 2  
REDUNDANCY SCREEN: A-N/A B-N/A C-N/A  
PREPARED BY: DES C SCARLETT  
APPROVED BY: REL R DIEHL  
APPROVED BY: NASA  
DES C SCARLETT  
REL R DIEHL  
APPROVED WITH CHANGES  
See Section 13.0  

ITEM: DISCONNECT, QUICK FILL  
* HELIUM WITH SPRING LOADED POPPET AND STRUCTURAL END CAP (1/4"). (MD 105/106)  
* FUNCTION: PROVIDES HELIUM TANK FILL POINT FOR GROUND OPERATIONS AND LOADING SERVICING.  
* FAILURE MODE: FAILS OPEN, CAP (S) LEAKS IN EXCESS OF ACCEPTABLE RATE.  
* CAUSE(S): VIBRATION, AND LOOSENING OF THE RETAINER NUT, IMPROPER HANDLING, MECHANICAL SHOCK.  
* EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE: (A) LOSS OF REDUNDANCY. (B) NONE. (C) POTENTIAL LAUNCH DELAY (MISSION LCSS) IF DETECTED. (D) POSSIBLE LOSS OF CREW/VEHICLE IF FAILURE OCCURS PRIOR TO ET SEPARATION.  
* DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY: (A) CAP SEAL DESIGN DETERMINED TO BE ADEQUATE TO PRECLUDE LEAKAGE. DESIGN FACTOR OF SAFETY IS 2.0 X 4000 PSIG MAX WORKING PRESSURE. CAP PLUS COUPLING CONSTITUTES DUAL SEALING. ALL RETAINER NUTS ARE PROPERLY TORQUED TO PRECLUDE LOOSENING. (B) SEALS ARE EXPOSED TO OVER 600 CYCLES DURING DEVELOPMENT. COUPLINGS ARE SUBJECTED TO 600 OPERATIONAL CYCLES IN QUAL TEST. ALL CAPS AND COUPLING LEAK TESTED FOR 3 MIN. AT PRESSURES UP TO 1.25 MAX WORKING PRESSURE DURING ACCEPTANCE TEST. TURNAROUND LEAK CHECKS PERFORMED BEFORE EACH FLIGHT. RANDOM VIBRATION PERFORMED DURING QUAL PROGRAM. 68 MINUTES IN TWO AXES AT ANTICIPATED MISSION LEVELS. (C) TURNAROUND INSPECTION INCLUDES VISUAL INSPECTION ALL COUPLINGS THAT HAVE BEEN USED DURING TURNAROUND FOR DAMAGE PLUS INSPECTING FOR LEAKS DURING LEAK CHECKS. ALSO, PROPER BLEED SCREW TORQUE IS VERIFIED PRIOR TO REINSTALLATION OF ANY CAPS THAT HAVE BEEN REMOVED. SUPPLIER AUDIT CONDUCTED 4-5-77 VERIFIED THAT SUPPLIER INSPECTION CONTROLS RAW MATERIAL PARTS IDENTIFICATION, MFG PROCESSES, CONTAMINATION CONTROL, AND STORAGE ENVIRONMENTS. (D) NEW DESIGN FOR SHUTTLE APPLICATION. NO FLIGHT FAILURE HISTORY
1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY
   ANNUNCIATE OR TAKE ACTION IN RESPONSE)?
   YES ☐ NO ☐

1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD
    USE TO DETECT THE FAILURE?
   *YES ☐ NO ☐

2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF
   IN-FLIGHT DETECTABILITY?
   YES ☐ *NO ☐

3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE
   (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
   YES ☐ NO ☐

3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS
    FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE
    PROGRAM LOGIC)?
   *YES ☐ NO ☐

4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR
   INDUCE ANOTHER FAILURE?
   *YES ☐ NO ☐

5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT
   OTHER FUNCTIONS?
   *YES ☐ NO ☐

6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW
   ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.
   *0 ☐ 1 ☐ 2 ☐

7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED
   TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?
   N/A ☐ YES ☐ NO ☐

8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:
   A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?
      YES ☐ *NO ☐
   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?
      YES ☐ *NO ☐

*EXPLANATION REQUIRED (SEE BELOW)

CHANGE/RETENTION RATIONALE SUMMARY
1. ☐ NO H/S ISSUES  3. ☐ NO SOFTWARE DETECTION  5. ☐ ACCEPTANCE RATIONALE BELOW
2. ☐ HARDWARE ACCEPTS RISK  4. ☐ DETECTION DURING CHECKOUT  6. ☐ RECOMMENDED CHANGES BELOW

EXPLANATION/COMMENTS:

1. Out of Scope. Ground operations only.
SUBSYSTEM: FWO - REACTION CONTROL

ASSEMBLY: PRESSURIZATION

P/N: MC276-0017-042/043

P/N VENDOR: 75372000-042/043

QUANTITY: 2

P/N: MC276-0017-042/043

MISSION: HF VF X PP UF SM

PHASE(S): PL X LG DD DU LS

NUMBER OF SUCCESS PATHS REMAINING:

AFTER FIRST FAILURE:

REDUNDANCY SCREEN:

FAILURES DETECTABLE IN FLIGHT?: N/A

GROUND TURNAROUND?: YES

FUEL FILL RATE AND HELIUM PRESSURE

PREPARED BY:

DEP C SCARLETT

APPROVED BY:

DEP R DIEHL

ITEM: DISCONNECT, QUICK FILL

HELIUM WITH SPRING LOADED POPPET AND STRUCTURAL END CAP (1/4"") (MU 105/106)

FUNCTION:

PROVIDES HELIUM TANK FILL POINT FOR GROUND OPERATIONS AND LOADING SERVICING.

FAILURE MODE: RESTRICTED FLOW - (F)

FAIILS CLOSED DURING GROUND FILL OPERATIONS

CAUSE(S):

VIBRATION/IMPROPER HANDLING WHICH CAUSES FILTER/POPPET DAMAGE IN DISCONNECT.

EFFECT(S): UN (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:

(A) LOSS OF OR REDUCED HELIUM FILL CAPABILITY. (B) NONE. (C) LAUNCH DELAY. (D) NONE.

CORRECTING ACTION:

REMOVE/REPLACE FILL VALVE OR ATTEMPT TO RECOUPLE.

REMARKS/HAZARDS:

NONE. NO REDUNDANCY PROVIDED FOR THIS ITEM IN THIS MODE.
**HARDWARE/SOFTWARE ANALYSIS CHECKLIST** 03-2F-101080-1

**SUBSYSTEM** Fwd. Reaction Control

**ITEM** Purge Quick Disconnect, Propellant

**FMEA NUMBER** SD75-SH-0016A

**FAILURE MODE** External Leakage During Flight

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the flight software detect this failure mode (i.e., automatically</td>
<td></td>
<td></td>
</tr>
<tr>
<td>announce or take action in response)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1a. If not, does the hardware provide information that the flight software could use to detect the failure?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Are the answers to questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3a. If not, does the capability exist for the software to compensate for this failure mode (either by commanding hardware action or implementing alternate program logic)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. As a result of this failure mode, can the software overstress the hardware or induce another failure?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Can this failure mode, in combination with software logic, adversely affect other functions?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)? Note change to FMEA Criticality.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?</td>
<td>N/A</td>
<td>YES</td>
</tr>
<tr>
<td>8. If the answer to either 1 or 3 is Yes:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Can the BFS be engaged after occurrence?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. Will BFS tolerate failure without loss of crew/vehicle?</td>
<td>YES</td>
<td></td>
</tr>
</tbody>
</table>

*Explanation required (see below)*

**CHANGE/RETENTION RATIONALE SUMMARY**

1. [ ] No H/S Issues
2. [X] Hardware accepts risk
3. [ ] No software detection
4. [ ] Detection during checkout
5. [ ] Acceptance rationale below
6. [ ] Recommended changes below

**EXPLANATION/COMMENTS:**

1. Per backup flight system program requirements document MG038103, once a pre-set delta between the propellant quantities is reached a class 2 caution and warning light and tone will be annunciated. Also primary flight control requirements FSSR 0026A except OPS 1,6.

2. The above statement indicates in-flight detection.

6. Capped quick disconnect provides one redundant success path.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N RI: KC276-0018
P/N VENDOR: 7b30600
QUANTITY: 14

ITEM: DISCONNECT, QCK, PURGE, VENT, PROPELLANT WITH STRUCTURAL END CAP AND SPRING LOADED POPPET (1/2")

FUNCTION:
- TO ALLOW GROUND PURGE OF PROPELLANT TANKS AND ASSOCIATED MANIFOLDS/LINES/THUSTERS AFTER LANDING & PROPELLANT TANKS FILL, MAIN & VENT

FAILURE MODE: EXTERNAL LEAKAGE

CAUSE(S):
- VIBRATION AND LOOSENING OF THE RETAINER NUT, STRUCTURAL FAILURE, PIECE PART FAILURE MECHANICAL SHOCK, IMPROPER GROUND HANDLING.

EFFECT(S):
- (A) LOSS OF PROPELLANT FIRST ORDER FAILURE FOR LOOSE RETAINER NUT. (b) POSSIBLE FIRE/EXPLOSION IF FUEL REACTS WITH COMPLEMENTARY OXIDIZER (OR EXTREME HEAT DURING RE-ENTRY). (C) POSSIBLE LOSS OF MISSION DUE TO FLUID SEPARATION. (D) POSSIBLE LOSS OF CREW/VEHICLE IF FAILURE OCCURS PRIOR TO ET SEPARATION.

CORRECTING ACTION:
- NONE AVAILABLE - IN FORWARD MODULE, CRITICALITY IS LESS SEVERE IF AFT MODULES OPERATIVE

REMARKS/HAZARDS:
- POTENTIAL CORROSION OF SURROUNDING COMPONENTS. STRUCTURAL CAP CONSIDERED AS STRUCTURE.
SUBSYSTEM: Fwd - Reaction Control
ASSEMBLY: Pressurization
P/N: WC276-0018
P/N Vendor: 76306000
QUANTITY: 14

ABORT: CRIT. FUNC: 1
MISSIONS: HF, VF, X, FF, OF, SM
PHASE(S): PL, LO, X, DO, X, LS

REDUNDANCY SCREEN: A-N/A, B-N/A, C-N/A

PREPARED BY: C. Scarlet
APPROVED BY: HJ/CP

FUNCTION:
TO ALLOW GROUND PURGE OF PROPELLANT TANKS AND ASSOCIATED MANIFOLDS/LINES/THRUSTERS AFTER LANDING & PROPELLANT TANKS FILL, DRAIN & VENT

FAILURE MODE: EXTERNAL LEAKAGE

CAUSE(S):
VIBRATION AND LOOSENING OF THE RETAINER NUT, STRUCTURAL FAILURE, PIECE PART FAILURE MECHANICAL SHOCK, IMPROPER GROUND HANDLING.

EFFECT(S):
(A) LOSS OF PROPELLANT FIRST ORDER FAILURE FOR LOOSE RETAINER NUT. (B) POSSIBLE FIRE/EXPLOSION IF FUEL REACTS WITH COMPLEMENTARY OXIDIZER (OR EXTREME HEAT DURING RE-ENTRY). (C) POSSIBLE LOSS OF MISSION DUE TO FLUID SEPARATION. (D) POSSIBLE LOSS OF CREW/VEHICLE IF FAILURE OCCURS PRIOR TO ET SEPARATION.

DISPOSITION & RATIONALE:
(A) DESIGN
DESIGN FACTOR OF SAFETY IS 3.0 X 710 PSIG MAX WORKING PRESSURE. CAP PLUS COUPLING CONSTITUTES DUAL SEALING. ALL RETAINER NUTS ARE PROPERLY TORQUED TO PRECLUDE LOOSENING. (B) SEALS ARE EXPOSED TO OVER 500 CYCLES DURING DEVELOPMENT. COUPLINGS ARE SUBJECTED TO 600 OPERATIONAL CYCLES IN QUAL TEST. ALL CAPS AND COUPLINGS LEAK TESTED FOR 3 MINUTES AT PRESSURES UP TO MAX WORKING PRESSURE DURING ACCEPTANCE TEST. TURNAROUND LEAK CHECKS PERFORMED BEFORE EACH FLIGHT. RANDOM VIBRATION PERFORMED DURING QUAL PROGRAM. 68 MINUTES IN TWO AXES AT ANTICIPATED MISSION LEVELS. (C) TURNAROUND INSPECTION INCLUDES VISUAL INSPECTING ALL COUPLINGS USED DURING TURNAROUND FOR DAMAGE PLUS INSPECTING FOR LEAKS DURING LEAK CHECKS. ALSO, PROPER BLEED SCREW TORQUE IS VERIFIED PRIOR TO REINSTALLATION OF ANY CAPS THAT HAVE BEEN REMOVED. SUPPLIER AUDIT CONDUCTED 4-5-77 VERIFIED THAT SUPPLIER INSPECTION CONTROLS RAW MATERIAL PARTS IDENTIFICATION, MFG PROCESSES, CONTAMINATION CONTROL, AND STORAGE ENVIRONMENTS. (D) NEW DESIGN FOR SHUTTLE APPLICATION. NO FLIGHT FAILURE HISTORY.

ORIGINAL PAGE IS OF POOR QUALITY
### HARDWARE/SOFTWARE ANALYSIS CHECKLIST

**SUBSYSTEM**: Fwd. Reaction Control  
**FMEA NUMBER**: SD75-SH-0016A  
**ITEM**: Purge Quick Disconnect, Propellant  
**FAILURE MODE**: Fails Closed/Ground Ops.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. **DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?**  
   - **YES** □  **NO** □  
   - **1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?**  
     - **YES** □  **NO** □  

2. **DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**  
   - **YES** □  **NO** □  

3. **IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**  
   - **YES** □  **NO** □  

4. **AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?**  
   - **YES** □  **NO** □  

5. **CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?**  
   - **YES** □  **NO** □  

6. **HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)?**  
   - **NO** □  **1** □  **2** □  

7. **IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?**  
   - **N/A** □  **YES** □  **NO** □  

8. **IF THE ANSWER TO EITHER 1 OR 3 IS YES: **  
   - **A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?**  
     - **YES** □  **NO** □  
   - **B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?**  
     - **YES** □  **NO** □  

**EXPLANATION/COMMENTS:**

1. Out of scope/ground operations only.
SUBSYSTEM : FWD - REACTION CONTROL
ASSEMBLY : PRESSURIZATION
P/N RI : MC276-0018
P/N VENDOR : 76306000
QUANTITY : 14

MISSIONS : HF VF X FF CF SM
PHASE(S) : PL X LG OD DO LS

FAILSAFE DETECTABLE IN FLIGHT? : N/A
TIME TO EFFECT:
REFERENCE DOCUMENTS:
MJC70-4001-01
SB72-SH-0103-2
VSTC-421001

GSE EQUIPMENT FLOW RATE AND TANK OUTPUT
PRESSURE V42F-121OC, 1310C

ITEM : DISCONNECT, QUICK, PURGE,
VENT, PROPELLANT WITH STRUCTURAL END CAP AND SPRING LOADED POPPET
(1/2"), (MD 117, 116, 123, 124, 127, 137, 138, 147, 161, 162, 163, 164).
FUNCTION:
TO ALLOW GROUND PURGE OF PROPELLANT TANKS AND ASSOCIATED
MANIFOLDS/LINES/THRUSTERS AFTER LANDING & PROPELLANT TANKS FILL, OR IN
VENT
FAILURE MODE: FAILS CLOSED (F)

CORRECTING ACTION:
ATTEMPT TO REMOVE BLOCKAGE (BACK-FLOW) OR REMOVE COUPLING AND REPLACE

COMMENTS/HAZARDS:
NONE. NO REDUNDANCY PROVIDED FOR THIS ITEM.
<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY</td>
<td>YES</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1a.</td>
<td>IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?</td>
<td></td>
<td>YES</td>
<td>NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?</td>
<td>YES</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?</td>
<td>YES</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3a.</td>
<td>IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?</td>
<td>YES</td>
<td>NO</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?</td>
<td>YES</td>
<td>NO</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?</td>
<td>YES</td>
<td>NO</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.</td>
<td>0</td>
<td>1</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?</td>
<td>N/A</td>
<td>YES</td>
<td>NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>IF THE ANSWER TO EITHER 1 OR 3 IS YES:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?</td>
<td>YES</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?</td>
<td>YES</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*EXPLANATION REQUIRED (SEE BELOW)*

---

**EXPLANATION/COMMENTS:**

1 & 2. V42P1110C, V42P1112C and V42P1113C will detect the failure and issue class 3 alarm (system management blue light on crew-cockpit glare shield) at <500 psia. Gross leak indication is quicker (class 2).

6. Capped quick disconnect provides one redundant success path.
SUBSYSTEM : FW - REACTION CONTROL
ASSEMBLY : PRESSURIZATION
P/N : ME276-0632
P/N VENDOR: XR42670-567, R64290C-163
QUANTITY : 14
SEVEN REQ'D FOR EACH
PROPELLANT

ABORT: CRITICAL FUCN: IM
MISSIONS: HF, VP, FF, GF, SH
PHASE(S): PL, LU, DU, X, DO, X, LS

FAILURE DETECTABLE IN FLIGHT? YES
HELIUM TANK PRESSURE: V42P-1110C, 1112C, 1113C,
1114C
GROUND TURNAROUND?.............N/A

PREPARED BY: DES C SCARLETT
APPROVED BY: DES R DIEHL

ITEM: DISCONNECT, QUICK, TEST
FUNCTION:
TO PROVIDE ACCESS TO THE HELIUM SUPPLY SYSTEM AT VARIOUS POINTS IN THE SYSTEM: (1) RELIEF VALVES/BURST DISCS (2) REGULATORS (3) CHECK VALVES. PROVIDES FOR C/O OF PRESSURIZATION SUB-SYS COMPONENTS. COMPONENT INPUTS & OUTPUTS ARE ACCESSIBLE AT HE SERVICE PANEL.

FAILURE MODE: EXTERNAL LEAKAGE (S)
FUNCTIONAL CRITICAL EFFECTS - POSSIBLE LOSS OF HELIUM SUPPLY WHICH COULD RESULT IN LOSS OF VEHICLE IF THE LOSS OCCURRED BEFORE ET SEPARATION.

CORRECTING ACTION:
UTILIZE AFT MODULES TO ORIENT VEHICLE FOR ENTRY AND COMPLETE ABDK1.
SUBSYSTEM: FWD - REACTION CONTROL  
ASSEMBLY: PRESSURIZATION  
P/N NI: ME276-0032  
P/N VENDOR: RR42670-567, R642900-163  
QUANTITY: 14  
MISSIONS: HF, VF, FF OF SM  
PHASE(S): PL, LO X CO X DO X LS  
P/N: RI ME276-0032  
REV: II/SUBSYSTEM: FWD - REACTION CONTROL  
PREPARED BY:  
DEP: G SCARLETT  
REL: R DIEHL  
APPROVED BY:  
DEP: G SCARLETT  
REL: R DIEHL  
MISSION: HF, VF, FF OF SM  
PHASE: PL, LO X CO X DO X LS  
REDUNDANCY SCREEN: A-PASS B-FAIL C-PASS  
ITEM: DISCONNECT, QUICK, TEST  
FUNCTION:  
TO PROVIDE ACCESS TO THE HELIUM SUPPLY SYSTEM AT VARIOUS POINTS IN THE SYSTEM: (1) RELIEF VALVES/BURST DISCS (2) REGULATORS (3) CHECK VALVES.  
PROVIDES FOR C/O OF PRESSURIZATION SUB-SYS COMPONENTS. COMPONENT INPUTS & OUTPUTS ARE ACCESSABLE AT THE SERVICE PANEL.  
FAILURE MODE: EXTERNAL LEAKAGE  
DURING FLIGHT  
CAUSE(S):  
VIBRATION, PIECE PART STRUCTURAL FAILURE (POPPET, SEAL), MECHANICAL SHOCK.  
EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:  
(A) LOSS OF HELIUM PRESSURANT. (SECOND ORDER FAILURE). (B) LOSS OF PROPellant FEED CAPABILITY. (C) POTENTIAL LOSS OF MISSION DUE TO FLUID LOSS. (D) NONE. (E) FUNCTIONAL CRITICALITY EFFECTS - POTENTIAL LOSS OF HELIUM SUPPLY WHICH COULD RESULT IN LOSS OF VEHICLE IF THE LOSS OCCURRED BEFORE ET SEPARATION.  
DISPOSITION & RATIONALE:  
(A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:  
(A) DUAL SEALING SURFACES ON CAP WILL PRECLUDE FAILURE. EACH SEALING SURFACE INDEPENDENT OF THE DESIGN BURST PRESSURE IS TWO TIMES OPER PRESSURE. (B) EACH COUPLING PROOF TESTED TO AT LEAST 1.5 OPER PRESSURE & LEAK TESTED FOR 15 MIN DURING ACCEPTANCE TESTING. (C) AUDIT CONDUCTED ON 11-3-76 VERIFY THAT SUPPLIER INSPECT INCLUDES VERIFY OF RAW MTL. PARTS MFG. IDENTIFICATION, AND PROTECTION, ASSY OPERATIONS, MTL EXAM OF WELDS, BRAZES, AND MTL AND EQUIP CONFORMANCE. TURNAROUND INSPECTION INCLUDES VISUALLY INSPECTING ALL COUPLINGS THAT HAVE BEEN USED FOR DAMAGE AND LEAKAGE. ALSO, PROPER AHC CAP TORQUE IS VERIFIED UPON REINSTALLATION OF ANY CAPS THAT HAVE BEEN REMOVED. (D) 14 NON-FLIGHT EXTERNAL LEAKAGE FAILURES EXPERIENCED ON LM/SM RCS DUE TO PROCESS DEFICIENCIES.
HARDWARE/SOFTWARE ANALYSIS CHECKLIST 03-2F-101090-2

SUBSYSTEM Fwd. Reaction Control

ITEM Test Quick Disconnect, Propellant

FMEA NUMBER SD75-SH-0016A

FAILURE MODE Fails Closed/Ground Ops

---

1. Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?
   - YES [ ] NO [ ]

1a. If not, does the hardware provide information that the flight software could use to detect the failure?
   - *YES [ ] NO [ ]

2. Are the answers to questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?
   - YES [ ] *NO [ ]

3. Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?
   - YES [ ] NO [ ]

3a. If not, does the capability exist for the software to compensate for this failure mode (either by commanding hardware action or implementing alternate program logic)?
   - *YES [ ] NO [ ]

4. As a result of this failure mode, can the software overstress the hardware or induce another failure?
   - YES [ ] NO [ ]

5. Can this failure mode, in combination with software logic, adversely affect other functions?
   - *YES [ ] NO [ ]

6. How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)? Note change to FMEA criticality.
   - N/A [ ] *YES [ ] *NO [ ]

7. If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?
   - YES [ ] *NO [ ]

8. If the answer to either 1 or 3 is YES:
   A. Can the BFS be engaged after occurrence?
      - YES [ ] *NO [ ]
   B. Will BFS tolerate failure without loss of crew/vehicle?
      - YES [ ] *NO [ ]

*Explanation required (see below)

---

CHANGE/RETENTION RATIONALE SUMMARY

1. [ ] NO H/S ISSUES
2. [ ] HARDWARE ACCEPTS RISK
3. [ ] NO SOFTWARE DETECTION
4. [ ] DETECTION DURING CHECKOUT
5. [ ] ACCEPTANCE RATIONALE BELOW
6. [ ] RECOMMENDED CHANGES BELOW

---

FMEA CHANGE RECOMMENDED

EXPLANATION/COMMENTS:

1. Out of scope - ground operations only.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: ME276-0032
P/N VENDOR: RR42670-5&7, R64290-1&3
QUANTITY: 14
MISSIONS: HF, VF, X, FF, UF, SM
PHASE(S): PL, X, LG, GO, DD, LS
SEVEN REQ'D FOR EACH
NUMBER OF SUCCESS PATHS REMAINING
PROPELLANT
AFTER FIRST FAILURE: 1
REDUNDANCY SCREEN: A-PASS, 8-N/A, C-PASS!

FAILURE DETECTABLE IN FLIGHT? N/A
TIME TO EFFECT: SECONDS TO HOURS
REFERENCE DOCUMENTS: MJ70-O101EB

GROUND TURNAROUND? YES
PRESSURE READ-OUT
V42P-1110C, 1112C, 1113C, VS70-4210C

PREPARED BY: LES C SCARLETT
APPROVED BY: DES R DIEHL

ITEM: DISCONNECT, QUICK, TEST

FUNCTION:
TG PROVIDE ACCESS TO THE HELIUM SUPPLY SYSTEM AT VARIOUS POINTS IN THE SYSTEM: (1) RELIEF VALVES/BURST DISCS (2) REGULATORS (3) CHECK VALVES. PROVIDES FOR C/O OF PRESSURIZATION SUB-SYS COMPONENTS. COMPONENT INPUTS & OUTPUTS ARE ACCESSIBLE AT HE SERVICE PANEL.

FAILURE MODE: FAILS CLOSED (F)
DURING TURN-AROUND/GROUND OPERATIONS
CAUSE(S):
CONTAMINATION, PIECE PART STRUCTURAL FAILURE (POPPET, SEAL).

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
LOSS OF TEST/CHECKOUT DATA. (A) INCREASED GROUND EQUIPMENT REQUIREMENTS. (C) POTENTIAL MISSION LAUNCH DELAY. (D) NONE.

CORRECTING ACTION:
TEST AT ALTERNATE POINT (IF AVAILABLE) OR REMOVE AND REPLACE COUPLING.

REMARKS/HAZARDS:
NONE.
### HARDWARE/SOFTWARE ANALYSIS CHECKLIST

**SUBSYSTEM**: Fwd. Reaction Control  
**FMEA NUMBER**: SD75-SH-0016A  
**ITEM**: Helium Quad Check Valve  
**FAILURE MODE**: Fails Open

<table>
<thead>
<tr>
<th>Question</th>
<th>YES</th>
<th>NO</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?</td>
<td>☒</td>
<td>☐</td>
<td>☑</td>
</tr>
<tr>
<td>1a. If not, does the hardware provide information that the flight software could use to detect the failure?</td>
<td>☐</td>
<td>☑</td>
<td>☐</td>
</tr>
<tr>
<td>2. Are the answers to Questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>3. Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?</td>
<td>☑</td>
<td>☐</td>
<td>☑</td>
</tr>
<tr>
<td>3a. If not, does the capability exist for the software to compensate for this failure mode (either by commanding hardware action or implementing alternate program logic)?</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>4. As a result of this failure mode, can the software overstress the hardware or induce another failure?</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>5. Can this failure mode, in combination with software logic, adversely affect other functions?</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>6. How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)? Note change to FMEA criticality.</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>7. If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?</td>
<td>☐</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>
| 8. If the answer to either 1 or 3 is yes:  
A. Can the BFS be engaged after occurrence?  
B. Will BFS tolerate failure without loss of crew/vehicle? | ☒ | ☐ | ☐ | ☑ | ☐ |

*Explanation required (see below)*

#### CHANGE/RETENTION RATIONALE SUMMARY

- [ ] NO H/S ISSUES
- [ ] HARDWARE ACCEPTS RISK
- [ ] NO SOFTWARE DETECTION
- [ ] DETECTION DURING CHECKOUT
- [ ] ACCEPTANCE RATIONALE BELOW
- [ ] RECOMMENDED CHANGES BELOW

#### EXPLANATION/COMMENTS:

1. Series redundant.
2. Series redundant.

---

57
SUBSYSTEM: FPD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: MC284-0481-C01/-0602
P/N VENDOR: RSC105-00-001/-011
QUANTITY: 2
: ONE PER HELIUM SUPPLY

FAILURE DETECTABLE IN FLIGHT? NO

GROUND TURNAROUND? YES

PREPARED BY: DES R BURKHART APPROVED BY: DES

ITEM: VALVE, QUAD, CHECK, HE (CV 101/102)

FUNCTION:
TO PRECLUDE PROPELLANT VAPORS FROM MIGRATING TO REGULATORS FROM THE PROPELLANT TANK.

FAILURE MODE: FAILS OPEN (F) OR FAILS TO REMAIN CLOSED (INTERNAL LEAKAGE).

CAUSE(S):
CONTAMINATION, VIBRATION, PIECE PART STRUCTURAL FAILURE, MECHANICAL SHOCK, VIBRATION.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF REDUNDANCY-SERIES VALVE WILL PROTECT REGULATORS FROM VAPORS. (B,C,D) NO EFFECT UNLESS MULTIPLE FAILURES OCCUR. (E) FUNCTIONAL CRITICALITY EFFECT - POSSIBLE CONTAMINATION OF REGULATORS WITH PROPELLANT VAPORS IF BOTH CHECK VALVES ARE OPEN.

CORRECTING ACTION:
NONE AVAILABLE.

REMARKS/HAZARDS:
NO HAZARDS ACTION OF PROPELLANT VAPORS AND CONTAMINATION.

ORIGINAL PAGE IS OF POOR QUALITY.
### HARDWARE/SOFTWARE ANALYSIS CHECKLIST

**SUBSYSTEM:** Fwd Reaction Control  
**FMEA NUMBER:** SD75-SH-0016A  
**ITEM:** Helium Quad Check Valve  
**FAILURE MODE:** Fails Closed

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>1a. If not, does the hardware provide information that the flight software could use to detect the failure?</td>
<td>YES</td>
<td>No</td>
</tr>
<tr>
<td>2. Are the answers to questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?</td>
<td>YES</td>
<td>X</td>
</tr>
<tr>
<td>3. Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>3a. If not, does the capability exist for the software to compensate for this failure mode (either by commanding hardware action or implementing alternate program logic)?</td>
<td>YES</td>
<td>No</td>
</tr>
<tr>
<td>4. As a result of this failure mode, can the software overstress the hardware or induce another failure?</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>5. Can this failure mode, in combination with software logic, adversely affect other functions?</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>6. How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)?</td>
<td>0</td>
<td><em>1</em></td>
</tr>
<tr>
<td>7. If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?</td>
<td>N/A</td>
<td>YES</td>
</tr>
<tr>
<td>8. If the answer to either 1 or 3 is yes:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Can the BFS be engaged after occurrence?</td>
<td>YES</td>
<td><em>No</em></td>
</tr>
<tr>
<td>B. Will BFS tolerate failure without loss of crew/vehicle?</td>
<td>YES</td>
<td><em>No</em></td>
</tr>
</tbody>
</table>

*Explanation required (see below)*

### CHANGE/RETENTION RATIONALE SUMMARY

1. **No H/S issues**  
2. *Hardware accepts risk*  
3. **No software detection**  
4. Detection during checkout  
5. Acceptance rationale below  
6. Recommended changes below

**FMEA CHANGE RECOMMENDED**

**EXPLANATION/COMMENTS:**

1 & 2. Upon using the thrusters, tank ullage pressure will decay until <200 psi which will give a class 2 caution and warning alarm.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 1C2

SUBSYSTEM: FWD - REACTION CONTROL  
ASSEMBLY: PRESSURIZATION  
P/N: MG264-0481-0001/-0002  
P/N VENDOR: KSO1C500-001-011  
QUANTITY: 2  
UNIT: ONE PER HELIUM SUPPLY  
MISSIONS: HF VF X FF OF SM  
PHASE(S): PL LO X IO X 03 X LS  
NUMBER OF SUCCESS PATHS REMAINING:  
AFTER FIRST FAILURE: 1  
REDUNDANCY SCREEN: A-PASS B-FAIL C-FAIL  
FAILURE DETECTABLE IN FLIGHT? NO  
TIME TO EFFECT:  
DUE TO SMALL P THE LEAKAGE IS NOT DETECTABLE  
REFERENCE DOCUMENTS:  
MJC70-0001-012  
VS70-421401  
GROUND TURNAROUND? YES  
SAME AS FLIGHT INSTRUMENTATION  
PREPARED BY: APPROVED BY:  
DES R BURKHART DES  
REL R DIEHL REL  
ITEM: VALVE, QUAD, CHECK, HE  
FUNCTION:  
TO PRECLUDE PROPELLANT VAPORS FROM MIGRATING TO REGULATORS (FROM THE PROPELLANT TANK).  
FAIL MODE: FAILS CLOSED  
RESTRICTED FLOW.  
CAUSE(S):  
PIECE PART STRUCTURAL FAILURE, MECHANICAL SHOCK, ACCELERATION.  
EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:  
(A) LOSS OF REDUNDANCY - PARALLEL PATH PROVIDES PRESSURANT FEED.  
(B, C, D) NO EFFECT UNLESS MULTIPLE FAILURES OCCUR.  
(E) FUNCTIONAL CRITICAL EFFECTS - IF FAILURE OCCURS BEFORE ET SEPARATION, LOSS OF DOWN FIRING THRUSTERS WILL PREVENT ET SEPARATION AND RESULT IN LOSS OF CREW/VEHICLE.  
CORRECTING ACTION:  
NONE (BLOWDOWN MAY BE USED AFTER SECOND FAILURE).  
REMARKS/HAZARDS:  
MINIMUM DELTA CRACKING PRESSURE FOR CRACKING IS NECESSARY REQUIREMENT TO MINIMIZE SYSTEM PRESSURE DROP TO TANKS.

ORIGINAL PAGE IS OF POOR QUALITY
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N RI: MCZ84-0481-0001/-0002
P/N VENDOR: RS010500-001/-011
QUANTITY: =2
ABORT: CRIT. FUNC: 1R
MISSIONS: HF VF X FF OF SM
PHASE(S): PL LC X DO X DO X LS

REACTOR CONTROL FMEA NO: 03-2F -101095-2 REV:11/10/78
CRIT. HOW
ASSEMBLY: PRESSURIZATION
P/N VENDOR: RS010500-001/-011
QUANTITY: =2
ONE PER HELIUM SUPPLY

PREPARED BY: DES R BURKHART DES RIEHL
REL R DIELH REL

ITEM: VALVE, QUAD, CHECK, HE
(CY 101/102)
FUNCTION:
TO PRECLUDE PROPELLANT VAPORS FROM MIGRATING TO REGULATORS (FROM THE PROPELLANT TANK).
FAILURE MODE: FAILS CLOSED (F)
RESTRICTED FLOW.

CAUSE(S):
PIECE PART STRUCTURAL FAILURE, MECHANICAL SHOCK, ACCELERATION.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF REDUNDANCY - PARALLEL PATH PROVIDES PRESSURANT FEED.
(B,C) NO EFFECT UNLESS MULTIPLE FAILURES OCCUR.
(D) NO EFFECT.

FUNCTIONAL CRITICAL EFFECTS - IF FAILURE OCCURS BEFORE SEPARATION, LOSS OF DOWNFIRE THRUSTERS WILL PREVENT SEPARATION AND RESULT IN LOSS OF CREW/VEHICLE.

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
(A) VALVE SEAT MATERIAL WILL NOT STICK, CAUSING A FAILURE TO OPEN AND SPECIFIED MAXIMUM CRACKING PRESSURE IS ONLY 5 PSI. (B) CHECK VALVE TO BE CERTIFIED FOR 100,000 CYCLES WITHOUT CHANGE IN PERFORMANCE CHARACTERISTICS/ALSO, WILL CHECK OUT EACH VALVE ELEMENT (PARALLEL - SERIES) AFTER EACH FLIGHT. VALVE SUBJECT TO 48 MIN OF 10-6 GRMS RANDOM VIBRATION PER AXIS DURING QUAL PROGRAM. (C) AN AUDIT CONDUCTED ON 1-16-78 INDICATED THAT SUPPLIER QC VERIFIED RAW MATER. CERTIFICATION TO SATISFY SHUTTLE DESIGN REQUIREMENTS, VERIFIED PROTECTION OF DETAIL PARTS FROM DAMAGE DURING MFG AND TEST, IN-PROCESS INSPECTION VERIFIED MFG TRAVELER SEQUENCES. TURNAROUND INSPECTION TO INCLUDE MONITORING FUNCTIONAL TESTS TO VERIFY FLOW AND CHECK FOR LEAKAGE. (D) NO FAILURE HISTORY. THIS IS A NEW DESIGN FOR SHUTTLE USE.
<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1a. If not, does the hardware provide information that the flight software could use to detect the failure?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Are the answers to questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3a. If not, does the capability exist for the software to compensate for this failure mode (either by commanding hardware action or implementing alternate program logic)?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. As a result of this failure mode, can the software overstress the hardware or induce another failure?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Can this failure mode, in combination with software logic, adversely affect other functions?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)? Note change to FMEA criticality.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. If the answer to either 1 or 3 is yes: A. Can the BFS be engaged after occurrence? B. Will BFS tolerate failure without loss of crew/vehicle?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Explanation Required (see below)**

**Change/Retention Rationale Summary**

1. [ ] No H/S issues
2. [x] Hardware accepts risk
3. [ ] No software detection
4. [ ] Detection during checkout
5. [ ] Acceptance rationale below
6. [ ] Recommended changes below

**Explanation/Comments:**

1. V42P1115C, 1116C will give a class 2 alert once pressure drops to a pre-determined low. Gross leak indication occurs first.

6. No redundancy available.

7. V42P1116C and V42P1115C goes to shared meter M2 and will show a large pressure drop for worst case (large leak).

FMEA Change - add V42P1116C to "failure detectable in flight".

---

42
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 102

**SUBSYSTEM**: FWD - REACTION CONTROL  
**ASSM**: PROPELLANT FEED  
**P/N**: 03-2F -102166-1  
**P/N VENDOR**: MC271-CD95  
**QUANTITY**: 2  
**MISSIONS**: HF VF FF CF SM  
**MISSING**: 2  
**PHASE(S)**: PL LO X OX X LO X LS  
**CONE PER PROPELLANT NUMBER OF SUCCESS PATHS REMAINING**:  
**AFTER FIRST FAILURE**:  

**FAILURE DETECTABLE IN FLIGHT?**: YES  
**TIME TO EFFECT**: SECONDS TO DAYS  
**PROPELLANT TANK PRESSURE V42P-131CC AND MANIFOLD**:  
**PRESSURE 1312C61312C**:  
**GROUND TURBOWRND?**: YES  
**SAME AS FLIGHT INSTRUMENTATION**:  

**PREPARED BY**: DES J. TAGGART  
**APPROVED BY**: DES  
**REL R. DIEHL**  

**ITEM**: PROP LINE FLEX ASSY  
**FUNCTION**: TO PROVIDE PROPELLANT FEED TO APPROPRIATE PROPELLANT FEEDLINES.  
**FAILRE MODE**: EXTERNAL LEAKAGE (S)  
**CAUSE(S)**: MECHANICAL SHOCK, VIBRATION, FLOW, FATIGUE, IMPROPER INSTALLATION (WELD)  
**EFFECT(S)**: ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:  
(A) LOSS OF PROPELLANTS.  
(B) POTENTIAL CORROSION FROM FREE PROPELLANTS IN MODULE.  
(C) POTENTIAL MISSION LOSS OR ABORT DECISION.  
(D) POTENTIAL LOSS OF CREW/VEHICLE IF FAILURE RESULTS IN LOSS OF RCS FUNCTION BEFORE ET SEPARATION.  
**CORRECTING ACTION**: ATTEMPT TO ISOLATE AND INITIATE ABORT IF REQ'D.  
**REMARKS/HAZARDS**: POTENTIAL HAZARD OF FIRE/EXPLOSION FROM FREE PROPELLANTS. SOME LEAK POINTS MAY NOT BE ISOLATABLE (I.E. BEFORE/UPSTREAM OF TANK ISOLATION VALVES) NO REDUNDANCY PROVIDED FOR LINES. SEE HAZARD NO. 1YXX-0302-64.
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM : FWD - REACTION CONTROL
ASSEMBLY : PROPELLANT FEED
P/N RI : CRIT. FEA NO 03-2F -102106-1
P/N VENDOR: MC271-0095
QUANTITY : 2

ASSEMBLY : PROPELLANT FEED ABORT: CRIT. FUNC: 1
P/N VENDOR: MC271-0095 MISSIONS: HF VF XF FF OF SM
PHASE(S): PL LO 00 X DO X LS

PREPARED BY: J. TAGGART
APPROVED BY: R DIEHL

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
(a) STRUCTURAL MARGIN OF 2.0 WILL MINIMIZE FAILURE MODE POTENTIAL. (B) PROOF TESTED TO 1.5 TIMES WORKING PRESSURE AND 65 MINUTES OF RANDOM VIBRATION AT ANTICIPATED MISSION LEVELS. (C) IN PROCESS INSPECTIONS X-RAY OF WELDS & PENETRANT INSPECT. TURN AROUND INSPECTION INCLUDES MONITORING FUNCTIONAL TESTS DURING PRESSURIZATION CYCLE FOR EVIDENCE OF LEAKS AND DAMAGE. SUPPLIER INSPECTION DEEMED TO BE SATISFACTORY BASED ON SURVEY CONDUCTED ON 4-20-77. (D) NO FAILURE HISTORY FOR THIS SPECIFIC DESIGN.

See Section 13.0

ITEM: PROP LINE FLEX ASSY

FUNCTION: TO PROVIDE PROPELLANT FEED TO APPROPRIATE PROPELLANT FEEDLINES.
FAILURE MODE: EXTERNAL LEAKAGE (S)

CAUSE(S): MECHANICAL SHOCK, VIBRATION, FLOW, FATIGUE, IMPROPER INSTALLATION (WELD)

EFFECT(S): (A) LOSS OF PROPELLANTS. (B) POTENTIAL CORROSION FROM FREE PROPELLANTS IN MODULE. (C) POTENTIAL MISSION LOSS OR ABORT DECISION. (D) POTENTIAL LOSS OF CREW/VEHICLE IF FAILURE RESULTS IN LOSS OF RCS FUNCTION BEFORE ET SEPARATION.

REduDANCY SCREEN: A-N/A B-N/A C-N/A

APPROVED WITH CHANGES
HARDWARE/SOFTWARE ANALYSIS CHECKLIST 03-2F-102108-1

SUBSYSTEM Fwd Reaction Control
ITEM Feedline and Fittings

<table>
<thead>
<tr>
<th>Failure Mode</th>
<th>External Leakage</th>
</tr>
</thead>
</table>

1. **Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?**
   - Yes [X] No [ ]

1a. If not, does the hardware provide information that the flight software could use to detect the failure?
   - Yes [ ] No [X] *

2. **Are the answers to questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?**
   - Yes [X] No [ ] *

3. **Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?**
   - Yes [ ] No [X] *

3a. If not, does the capability exist for the software to compensate for this failure mode (either by commanding hardware action or implementing alternate program logic)?
   - Yes [ ] No [X] *

4. **As a result of this failure mode, can the software overstress the hardware or induce another failure?**
   - Yes [ ] No [X] *

5. **Can this failure mode, in combination with software logic, adversely affect other functions?**
   - Yes [ ] No [X] *

6. **How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)? Note change to FMEA criticality.**
   - Yes [X] No [ ] *

7. **If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?**
   - Yes [X] No [ ] *

8. **If the answer to either 1 or 3 is yes:**
   - A. Can the BFS be engaged after occurrence? Yes [X] No [ ] *
   - B. Will BFS tolerate failure without loss of crew/vehicle? Yes [X] No [ ] *

*Explanation required (see below)

---

**Change/Retention Rationale Summary**

1. No H/S Issues
2. Hardware accepts risk
3. No software detection
4. Detection during checkout
5. Acceptance rationale below
6. Recommended changes below

---

**Explanation/Comments:**

1. V42P1115C, 1116C will give a class 2 alert once pressure drops to a pre-determined low. Gross leak indication occurs first.

5. No redundancy available.

7. V42P1115C and V42P1116C goes to shared meter M2 and will show a large pressure drop for worst case (large leak).
SUBSYSTEM: FWC - REACTION CONTROL  
ASSEMBLY: PROPellant FEED.  
P/N: V070-42101  
P/N VENDOR:  
QUANTITY: 1  

critical FUNCTION: 1  

Missions: HF Vl X FF OF SM  
Phase(s): PL LO X 00 X 00 X LS  

ONE SET PER PROPELLANT  

NUMBER OF SUCCESS PATHS REMAINING  

AFTER FIRST FAILURE: 0  

REDUNDANCY SCREEN: A-N/A B-N/A C-N/A  

FAILURE DETECTABLE IN FLIGHT? YES  
PROPELLANT TANK PRESSURE V42P-1310C AND MANIFOLD  
PRESSURE 1312C & 1315C  

GROUND TURNAROUND?..............YES  
SAME AS FLIGHT INSTRUMENTATION  

PREPARED BY: A SIEGELIN  
APPROVED BY: R DIEHL  

ITEM: FEEDLINE AND FITTINGS  
FROM TANK TO 1) TANK VALVES TO 2) MANIFOLD VALVES, TO 3) THRUSTERS.  
FUNCTION:  
TO PROVIDE FEED TO APPROPRIATE PROPELLANT COMPONENTS FOR THRUSTER OPERATION - 3 AXIS ACCELERATION CONTROL AND ROTATIONAL CONTROL.  

FAILURE MODE: EXTERNAL LEAKAGE  

CAUSE(S): MECHANICAL SHOCK, VIBRATION/FATIGUE, STRUCTURAL FAILURE, IMPROPER INSTALLATION (WELD), FLUID FITTING SEAL FAILURE.  

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:  
(A) POTENTIAL LOSS OF PROPELLANTS. (B) POTENTIAL CORROSION FROM FREE PROPELLANTS IN MODULE. (C) POTENTIAL MISSION LOSS OR ABORT DECISION. (D) POTENTIAL LOSS OF CREW/VEHICLE IF LEAKING PROPELLANT EXPLODES DUE TO CONTACT WITH CATALYTIC AGENT OR HEAT SOURCE WITH SUBSEQUENT LOSS OF FORWARD MODULE OR IF LOSS OF PROPELLANT PROHIBITS SEPARATION.  
CORRECTING ACTION:  
ATTEMPT TO ISOLATE AND INITIATE ABORT IF REQUIRED.  

REMARKS/HAZARDS:  
POTENTIAL HAZARD OF FIRE/EXPLOSION FROM FREE PROPELLANTS. SOME LEAK POINTS MAY NOT BE ISOLATABLE (I.E. BEFORE/UPSTREAM OF TANK ISOLATION VALVES) NO REDUNDANCY PROVIDED FOR LINES. SEE HAZARD NO. LYXX-0302-04.
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM : FWD - REACTION CONTROL  
ASSEMBLY : PROPELLANT FEED - ORBITER 102  
P/N RI : V070-421001  
P/N VENDOR:  
QUANTITY : 1  

SUBSYSTEM FWD - REACTION CONTROL  
ASSEMBLY PROPELLANT FEED - ORBITER 102  
P/N RI V070-421001  
P/N VENDOR:  
QUANTITY 1  

MISSIONS: HF VF X FF OF SM  
PHASE(S): PL LO X CO X DO X LS  

REdundancy Screen: A-N/A B-N/A C-N/  

PREPARED BY: A SIEGELIN R DIEHL  
APPROVED BY:  

ITEM: FEEDLINE AND FITTINGS  
FROM TANK TO 1) TANK VALVES TO 2) MANIFOLD VALVES, TO 3) THRUSTERS.  

FUNCTION:  
TO PROVIDE FEED TO APPOPRIATE PROPELLANT COMPONENTS FOR THRUSTER OPERATION - 3 AXIS ACCELERATION CONTROL AND ROTATIONAL CONTROL.  

FAILURE MODE: EXTERNAL LEAKAGE  

CAUSE(S):  
MECHANICAL SHOCK, VIBRATION/FATIGUE, STRUCTURAL FAILURE, IMPROPER INSTALLATION (WELD), FLUID FITTING SEAL FAILURE.  

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:  
(A) POTENTIAL LOSS OF PROPELLANTS. (B) POTENTIAL CORROSION FROM FREE PROPELLANTS IN MODULE. (C) POTENTIAL MISSION LOSS OR ABORT DECISION. (D) POTENTIAL LOSS OF CREW/VEHICLE IF LEAKING PROPELLANT EXPOLDES DUE TO CONTACT WITH CATALYTIC AGENT OR HEAT SOURCE WITH SUBSEQUENT LOSS OF FORWARD MODULE OR IF LOSS OF PROPELLANT PROHIBITS SEPARATIONS.  

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY  
(A) FACTOR OF SAFETY OF 4.0 WILL MINIMIZE FAILURE POTENTIAL. DYNATUBE FITTINGS HAVE DUAL SEALS. WELD CONSTRUCTION REDUCES JOINTS & POSSIBLE LEAK PATHS. FASTENING CLAMPS AND TUBE BEND DESIGN ALLOWS DEGREE OF MOVEMENT WHICH HELPS PREVENTING LEAKS. (B) POST INSTALLATION TEST AND OPERATIONAL CHECKOUTS WILL VERIFY SYSTEM INTEGRITY. ALL LINES SUBJECTED TO PROOF TEST OF 1.25 X MAX OPERATING PRESSURE OR 1.1 X SURGE (TRANSIT) PRESSURE WHICHEREVER IS GREATER. PERFORMED TUBING CERTIFICATION PER "ORBITER TUBING VERIFICATION PLAN SD75-SH-0205". (C) IN-PROCESS INSPECT INCLUDES NDT & CHECKS DURING INSTALLATION. TURNAROUND INSPECTION INCLUDES MONITORING FUNCTIONAL TESTS DURING PRESSURIZATION CYCLE FOR EVIDENCE OF LEAKS. VISUALLY INSPECT FOR DAMAGE WHERE ACCESSIBLE. HARDWARE INSPECTION IN ACCORDANCE WITH PLANNING ROUTINES APPROVED BY NASA. (D) MINOR FAILURE HISTORY-CORROSION AND FAB PROBLEMS REPORTED DURING APOLLO PROGRAM AND CORRECTED WITH APPLICABLE TMO/TPC REQUIREMENT.
**SUBSYSTEM**: Fwd Reaction Control  
**FMEA NUMBER**: SD75-SH-00016A  
**ITEM**: AC Motor Operated Valve (Tank)  
**FAIL MODE**: Fails Closed

| Q1. | DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)? | YES [X] NO |
| Q1a. | IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE? | *YES [X] NO |
| Q2. | ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY? | YES [X] *NO |
| Q3. | DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)? | YES [X] NO |
| Q3a. | IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)? | YES [X] NO |
| Q4. | AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE? | YES [X] NO |
| Q5. | CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS? | YES [X] NO |
| Q6. | HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY. | *0 [X] 1 [X] 2 |
| Q7. | IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION? | N/A [X] YES [X] NO |
| Q8. | IF THE ANSWER TO EITHER 1 OR 3 IS YES: | |
| Q8a. | CAN THE BFS BE ENGAGED AFTER OCCURRENCE? | YES [X] *NO |
| Q8b. | WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE? | YES [X] *NO |

*EXPLANATION REQUIRED (SEE BELOW)*

**CHANGE/RETENTION RATIONALE SUMMARY**:  
1. [X] NO H/S ISSUES  
2. [X] HARDWARE ACCEPTS RISK  
3. [X] NO SOFTWARE DETECTION  
4. [X] DETECTION DURING CHECKOUT  
5. [X] ACCEPTANCE RATIONALE BELOW  
6. [X] RECOMMENDED CHANGES BELOW

**EXPLANATION/COMMENTS**:  
1. "RCS JETS" light on caution and warning panel.  
6. The manifolds are in parallel (2 legs) giving one redundant path.

[FMEA CHANGE RECOMMENDED]
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS: ORBITER 161

SU2 SYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PROPELLANT FEED
P/N: KC204-C430-0007/0008
P/N VENDOR: 5750025/5750026
QUANTITY: 4

FAILURE DETECTABLE IN FLIGHT?: YES
MISSIONS: HF VF X FF OF SM
COMMENTS:

PREPARED BY: DES R GONZALEZ
APPROVED BY: DES K DIEHL

ITEM: VLV, AC MOTOR OPERATED - TANK (1 1/2"), (LV 161-164)

FUNCTION:
1) PROVIDES ISOLATION OF TANKS FROM MANIFOLDS.
2) PROVIDES BACK-UP SHUT-OFF/ISOLATION OF PROP MANIFOLDS AND ASSOCIATED THRUSTERS.

COMPONENTS: BI-STABLE, (TANK PRESSURE=245 PSI). AC MOTOR DRIVEN 3 PHASE (2 OF 3 WILL ACTUATE VALVE) 115 TO 200 VOLTS 400 HZ.

FAILURE MODE: FAILS CLOSED (F)
POSITION - INCLUDES RESTRICTED FLOW TO LEVEL THAT DOES NOT ALLOW PROPER MIXTURE RATIO.

CAUSE(S):
VIBRATION, STRUCTURAL FAILURE, PREMATURE POWER TO MUTUK, ELECTRICAL SHORT.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF PROPELLANT FLOW IN TWO MANIFOLDS AND SUBSEQUENT LOSS OF THRUSTER FUNCTION (THRUSTER BURN-THRU DUE TO OXID RICH MIXTURE). (B) POSSIBLE BURN-THRU PROPAGATION. (C) LOSS OF MISSION. ABORT DECISION.
(D) POTENTIAL VEHICLE DAMAGE FROM COLLISION WITH KENNEDY TARGET, AFTER SECOND FAILURE. CRIT 1 FOR RTLS ABORT.

CORRECTING ACTION:
UTILIZE REMAINING FORWARD THRUSTERS IN COUPLE WITH APPROPRIATE AFT THRUSTERS FOR BRAKING. DE-ORBIT WITH AFT MODULES.

REMARKS/HAZARDS:
POTENTIAL HAZARD OF EXPLOSION IF OX VALVE FAILS. SEE PARKER FMEA + RKM 5750025.
SUBSYSTEM : FWO - REACTION CONTROL
ASSEMBLY : PROPELLANT FEED
P/N RI : MC284-0430-0007/-0008
P/N VENDOR: 5750025/5750026
QUANTITY : 4

SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

ITEM: VLV, AC MOTOR OPERATED - TANK [1 1/2"] - (LV161-164).

FUNCTION:
1) PROVIDES ISOLATION OF TANKS FROM MANIFOLDS.
2) PROVIDES BACK-UP SHUT-OFF/ISOLATION OF PROP MANIFOLDS AND ASSOCIATED THRUSTERS' COMPONENTS.
3) STABLE, (TANK PRESSURE=245 PSI). AC MOTOR DRIVEN.
4) PHASE (2 OF 3 WILL ACTUATE VALVE) 115 TO 200 VOLTS 400 HZ.

FAILURE MODE: FAILS CLOSED (F) POSITION - INCLUDES RESTRICTED FLOW TO LEVEL THAT DOES NOT ALLOW PROPER MIXTURE RATIO.

CAUSE(S):
- VIBRATION, STRUCTURAL FAILURE, PREMATURE POWER TO MOTOR, ELECTRICAL SHORT.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF PROPELLANT FLOW IN TWO MANIFOLDS AND SUBSEQUENT LOSS OF THRUSTER FUNCTION (THRUSTER BURN-THRU DUE TO OXID RICH MIXTURE).
(B) POSSIBLE BURN-THRU PROPAGATION.
(C) LOSS OF MISSION, ABORT DECISION.
(D) POTENTIAL VEHICLE DAMAGE FROM COLLISION WITH RENDEVOUS TARGET, AFTER SECOND FAILURE, CRIT III FOR RTLS ABORT.

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
(A) VALVES ARE ALWAYS OPEN. DUAL SERIES SWITCHES WILL PRECLUDE SINGLE FAILURE PREMATURE ACTUATION. SHORTED RPC WILL NOT CLOSE VALVE.
(B) EACH VALVE IS SUBJECT TO ACCEPT TEST VIBRATION. VALVE IS SUBJECT TO 48 MIN OR RANDOM VIB IN EACH AXIS AT ANTICIPATED MISSION LEVELS AND AN ENDURANCE TEST EQUIV. TO 100 MISSIONS DURING THE QUAL TEST PROGRAM. EACH VALVE SUBJECTED TO PROOF PRESSURE OF 1500 PSI, MORE THAN 4 X WORKING PRESSURE.
(C) AUDIT CONDUCTED 7-1-76 VERIFY SUPPLIER INSPECTION CONTROL OF PARTS ID AND PROTECTION, MFG PROCESSES, ELECT TERRMINATIONS.
(D) NO FLIGHT FAILURE EXPERIENCE.
**HARDWARE/SOFTWARE ANALYSIS CHECKLIST 03-2F-102150-I**

**SUBSYSTEM** Fwd. Reaction Control  
**FMEA NUMBER** SD75-SH-0016A  
**ITEM** Quick Disconnect  
**FAILURE MODE** External Leakage

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>Unchecked</th>
</tr>
</thead>
</table>
| 1. **DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE** (i.e., automatically\ 
  ANNUNCIATE OR TAKE ACTION IN RESPONSE)? | ☑   |    |           |
| 1a. **IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?** | ☑   |    |           |
| 2. **ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?** | ☑   |    |           |
| 3. **DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?** | ☑   |    |           |
| 3a. **IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?** | ☑   |    |           |
| 4. **AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?** | ☑   |    |           |
| 5. **CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?** | ☑   |    |           |
| 6. **HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)?** Note Change to FMEA Criticality. | ☑   |    |           |
| 7. **IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?** | ☑   |    |           |
| 8. **IF THE ANSWER TO EITHER 1 OR 3 IS YES:** | ☑   |    |           |
| A. **CAN THE BFS BE ENGAGED AFTER OCCURRENCE?** | ☑   |    |           |
| B. **WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?** | ☑   |    |           |

*EXPLANATION REQUIRED (SEE BELOW)*

**CHANGE/RETENTION RATIONALE SUMMARY**

1. ☑ NO H/S ISSUES  
2. ☑ HARDWARE ACCEPTS RISK  
3. ☑ NO SOFTWARE DETECTION  
4. ☑ DETECTION DURING CHECKOUT  
5. ☑ ACCEPTANCE RATIONALE BELOW  
6. ☑ RECOMMENDED CHANGES BELOW:

**EXPLANATION/COMMENTS:**

1. The tank pressure drop (worst case/full open) will be detected by V42P1115C, 1116C; unless regulated the gross leak indication will detect it. Also measurements 1313C, and 1314C appear obsolete and should be removed from the FMEA.

---

[X] FMEA CHANGE RECOMMENDED

71
FAILURE DETECTABLE IN FLIGHT? YES

LOSS OF TANK PRESSURE

1312C, 1313C, 1314C, 1315C TANK TEMP 1300 AND 1400

GROUND TURNAROUND? N/A

PREPARED BY: DES C SCARLETT

APPROVED BY: DES R DIEHL

ITEM: DISCONNECT, QUICK, FILL

FUNCTION:

TO PROVIDE FOR DRAINING, VENTING, AND BLEEDING PROPELLANT TANKS. IN BOTH HORIZONTAL AND VERTICAL VEHICLE ORIENTATION.

FAILURE MODE: EXTERNAL LEAKAGE

DURING FLIGHT

CAUSE(S):

VIBRATION, AND LOOSENING OF RETAINER NUT, PIECE PART STRUCTURAL FAILURE, MECHANICAL SHOCK.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:

(A) LOSS OF PROPELLANT OVERBOARD (1ST ORDER FAILURE FOR LOOSE RETAINING NUT). (B) POSSIBLE FIRE/EXPLOSION IF FUEL REACTS WITH OXIDIZER (2ND ORDER) OR EXTREME HEAT DURING RE-ENTRY. (C) POSSIBLE LOSS OF MISSION DUE TO FLUID LOSS. (C) POSSIBLE LOSS OF CREW/VEHICLE IF FAILURE OCCURS PRIOR TO ET SEPARATION.

CORRECTING ACTION:

INITIATE ABORT OR RESCUE OPERATIONS.

REMARKS/HAZARDS:

POTENTIAL HAZARD FROM FIRE, EXPLOSION, AND FREE PROPELLANTS. SEE HAZARD 1YXX-0302-05.
SUBSYSTEM : FWD - REACTION CONTROL
ASSEMBLY : PROPELLANT
P/N RI : MC276-001A
P/N VENDOR : 76301000
QUANTITY : 6
MISSIONS : HF VF X FF DF SM
PHASE(S) : PL LO X OC X DO X LS

ASSEMBLY : PROPELLANT Abort: CRIT. P/N : MC276-0018
CRIT. FUNC : 1
CRIT. HDW : 1
P/N VENDOR : 76301000
MISSIONS : HF VF X FF DF SM
QUANTITY : 6
PHASE(S) : PL LO X OC X DO X LS

THREE REQ PER PROPELLANT
REduNDANCY SCREEN: A-N/A B-N/A C-N/A

ITEM: DISCONNECT, QUICK, FILL
PROPELLANT, SPRING LOADED POPPET & STRUCTURAL CAP (MD119-126)
FUNCTION: TO PROVIDE FOR DRAINING, VENTING, AND BLEEDING PROPELLANT TANKS. IN BOTH HORIZONTAL AND VERTICAL VEHICLE ORIENTATION.
FAILURE MODE: EXTERNAL LEAKAGE
DURING FLIGHT
CAUSE(S): VIBRATION, AND LOOSENING OF RETAINER NUT, PIECE PART STRUCTURAL FAILURE, MECHANICAL SHOCK.
EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF PROPELLANT OVERBOARD (1ST ORDER FAILURE FOR LOOSE RETAINING NUT). (B) POSSIBLE FIRE/EXPLOSION IF FUEL REACTS WITH OXIDIZER (2ND ORDER) OR EXTREME HEAT DURING RE-ENTRY. (C) POSSIBLE LOSS OF MISSION DUE TO FLUID LOSS. (D) POSSIBLE LOSS OF CREW/VEHICLE IF FAILURE OCCURS PRIOR TO ET SEPARATION.
DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
(A) CAP SEAL DESIGN DETERMINED TO BE ADEQUATE TO PRECLUDE LEAKAGE. DESIGN FACTOR OF SAFETY IS 3.0 X 710 PSIG MAX WORKING PRESSURE. CAP PLUS COUPLING CONSTITUTES DUAL SEALING. ALL RETAINER NUTS ARE PROPERLY TORQUED TO PRECLUDE LOOSENING. (B) SEALS ARE EXPOSED TO OVER 500 CYCLES DURING DEVELOPMENT. COUPLINGS ARE SUBJECTED TO 600 OPERATIONAL CYCLES IN QUAL TEST. ALL CAPS & COUPLINGS LEAK TESTED FOR 3 MIN. AT PRESSURES UP TO 1.25 X MAX WORKING PRESSURE DURING ACCEPTANCE TEST. TURNAROUND LEAK CHECKS PERFORMED BEFORE EACH FLIGHT. RANDOM VIBRATION PERFORMED DURING QUAL PROGRAM. 68 MINUTES IN TWO EXES AT ANTICIPATED MISSION LEVELS. (C) TURNAROUND INSPECTION INCLUDES VISUAL INSPECTING ALL COUPLINGS THAT HAVE BEEN USED DURING TURNAROUND FOR DAMAGE PLUS INSPECTING FOR LEAKS DURING LEAK CHECKS. ALSO, PROPER BLEED SCREW TORQUE IS VERIFIED PRIOR TO REINSTALLATION OF ANY CAPS THAT HAVE BEEN REMOVED. SUPPLIER AUDIT CONDUCTED 4-5-77 VERIFIED THAT SUPPLIER INSPECTION CONTROLS RAW MATERIAL PARTS IDENTIFICATION, MFG PROCESSES, CONTAMINATION CONTROL, AND STORAGE ENVIRONMENTS. (D) NEW DESIGN FOR SHUTTLE APPLICATION. NO FLIGHT FAILURE HISTORY.
HARDWARE/SOFTWARE ANALYSIS CHECKLIST 03-2F-102150-2

SUBSYSTEM: Fwd. Reaction Control
FMEA NUMBER: SD75-SH-0016A
FAILURE MODE: Fails Closed/Ground Ops

ITEM: Quick Disconnect

1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?
   - YES [ ]
   - NO [ ]
   - N/A [ ]

1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?
   - YES [ ]
   - NO [ ]
   - N/A [ ]

2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?
   - YES [ ]
   - NO [ ]

3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
   - YES [ ]
   - NO [ ]
   - N/A [ ]

3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
   - YES [ ]
   - NO [ ]
   - N/A [ ]

4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?
   - YES [ ]
   - NO [ ]
   - N/A [ ]

5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?
   - YES [ ]
   - NO [ ]
   - N/A [ ]

6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.
   - 0 [ ]
   - 1 [ ]
   - 2 [ ]
   - N/A [ ]

7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?
   - YES [ ]
   - NO [ ]
   - N/A [ ]

8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:
   A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?
      - YES [ ]
      - NO [ ]
      - N/A [ ]
   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?
      - YES [ ]
      - NO [ ]
      - N/A [ ]

*EXPLANATION REQUIRED (SEE BELOW)

CHANGE/RETENTION RATIONALE SUMMARY

1. [ ] NO H/S ISSUES
2. [ ] HARDWARE ACCEPTS RISK
3. [ ] NO SOFTWARE DETECTION
4. [ ] DETECTION DURING CHECKOUT
5. [ ] ACCEPTANCE RATIONALE BELOW
6. [ ] RECOMMENDED CHANGES BELOW

EXPLANATION/COMMENTS:

Out of scope - ground operations only.
**SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 101**

<table>
<thead>
<tr>
<th>SUBSYSTEM</th>
<th>FWD - REACTION CONTROL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASSEMBLY</td>
<td>PROPELLANT</td>
</tr>
<tr>
<td>P/N #1</td>
<td>MC276-0018</td>
</tr>
<tr>
<td>P/N VENDOR</td>
<td>7610100</td>
</tr>
<tr>
<td>QUANTITY</td>
<td>6</td>
</tr>
</tbody>
</table>

- **AEROT**: CRIT. FUNC: 3
- **MISSIONS**: HF VF X FF UF SM
- **PHASE(S)**: PL X LO 00 DO LS
- **NUMBER OF SUCCESS PATHS REMAINING**: THREE REQ PER PROPELLANT AFTER FIRST FAILURE: 0
- **REDUNDANCY SCREEN**: A-PASS B-N/A C-PASS
- **FAI LURE DETECTABLE IN FLIGHT?**: NA
- **TIME TO EFFECT**: SECONDS TO HOURS
- **REFERENCE DOCUMENTS**: MJ070-C081-21b
- **GROUND TURNAROUND?**: YES
- **GROUND EQUIPMENT FLOW RATE READ OUT**: VS70-421061

**PREPARED BY:** DES C SCARLETT REL R DIEHL

**APPROVED BY:**

**ITEM**: DISCONNECT, QUICK, FILL

**FUNCTION**: PROPELLANT, SPRING LOADED POPPET & STRUCTURAL CAP (MD119-12x).

**CAUSE(S)**: CONTAMINATION, PIECE PART STRUCTURAL FAILURE IMPROPER HANDLING.

**EFFECT(S)**: ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:

- (A) LOSS OF FILL CAPABILITY, (B) INCREASED GROUND OPERATIONS REQUIREMENTS, (C) LAUNCH DELAY, (D) NONE.

**CORRECTING ACTION**: REMOVE AND REPLACE FILL VALVE OR ATTEMPT RECONNECTION.

**REMARKS/HAZARDS**: NONE.
1. **DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNOUNCE OR TAKE ACTION IN RESPONSE)?**
   - **YES** [X] **NO**

1a. **IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?**
   - **YES** [☐] **NO** [☐]

2. **ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?**
   - **NO** [X]

3. **DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**
   - **NO** [X]

3a. **IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**
   - **YES** [☐] **NO** [☐]

4. **AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?**
   - **NO** [X]

5. **CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?**
   - **NO** [X]

6. **HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION) NOTE CHANGE TO FMEA CRITICALITY?**
   - **O** [☐]  **1** [X]  **2** [☐]

7. **IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?**
   - **N/A** [☐]  **YES** [X]  **NO** [☐]

8. **IF THE ANSWER TO EITHER 1 OR 3 IS YES:**
   - **A.** CAN THE BFS BE ENGAGED AFTER OCCURRENCE?
     - **YES** [X]  **NO** [☐]
   - **B.** WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?
     - **YES** [X]  **NO** [☐]

*EXPLANATION REQUIRED (SEE BELOW)*

**EXPLANATION/COMMENTS:**

1. Manifold status on CRT and panel talk back is available.

6. One failure is all that can occur since there is no redundancy. The Shuttle can tolerate this failure since it is a criticality 3.

7. The measurements V42X1332X and V42X1232X are downlisted and available for CRT callup.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 1G2

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PROPELLANT FEED
P/N: MG284-0420-0011/-0012
P/N VENDOR: 7395-0011/-0012
QUANTITY: 2

MISSIONS: HF VF X FF OF SM

FAILURE MODE: FAILS CLOSED-PREMATURE (F)

OPERATION
CAUSE(S):
- IMPROPER ELECTRICAL SIGNAL (CONTINUOUS SHORT), PIECE PART FAILURE, CONTAMINATION, VIBRATION.

EFFECT(S):
- (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:

- (A) LOSS OF VERNIER THRUSTER FUNCTION.
- (B) NONE.
- (C) POSSIBLE EARLY MISSION TERMINATION. BECAUSE LARGE THRUSTERS INADEQUATE FOR SMALL RATE ATTITUDE HOLD.
- (D) NONE.

CORRECTING ACTION:
- ATTEMPT TO UTILIZE LARGE THRUSTER IN AFFECTED AXIS TO MAINTAIN SMALL DEADBAND.

REMARKS/HAZARDS:
- POTENTIAL FOR COLLISION WITH OR LOSS OF PAYLOAD/SATELLITE. SEE CONSOLIDATED CONTROLS FMEA # 73895 FMEA 1.

PREPARED BY: DES R BURKHART
APPROVED BY: DES R DIEHL

ITEM:
- VALVE, DC SOLENOID OPERATED -
  - VERNIER THRUSTER MANIFOLD, (1/4") 51-STABLE, SOLENOID DRIVEN 26VDC. (LV 157-159)

FUNCTION:
- TO PROVIDE ISOLATION OF PROPELLANT MANIFOLD AND ASSOCIATED VERNIER THRUSTERS 1) SUBSEQUENT TO DOWNSTREAM FAILURE(S) 2) PRIOR TO SYSTEM ACTIVATION.

FAILURE DETECTABLE IN FLIGHT?: YES
MANIFOLD POSITON INDICATOR V42X1232E
V42X1332E

GROUND TURNAROUND?: YES
SAME AS FLIGHT

FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 1G2
FMEA NO 03-2F -1G217C-1 REV: 12/08/77

KCV:
12/vCt/7.

A$SMFLY:
PROPELLANT FEED ABORT: CRIT. FUNC: 2

P/N MFR:
CRIT. MKUS: 2

REFERENCE DOCUMENTS:
MJC70-C001-01E
SD72-SM-01C3-2
VS70-421501

TIME TO EFFECT:
SECONDS

REMARKS/HAZARDS:
POTENTIAL FOR COLLISION WITH OR LOSS OF PAYLOAD/SATELLITE. SEE CONSOLIDATED CONTROLS FMEA # 73895 FMEA 1.
**SUBSYSTEM:** FWO - REACTION CONTROL  
**ASSEMBLY:** PROPELLANT FEED  
**P/N:** MC284-0420-0011/0012  
**P/N VENDOR:** 73895-0011/-0012  
**QUANTITY:** 2  
**P/N VENDOR:** 73895-O011/-O012  
**MISSIONS:** HF VF X FF OF SM  
**QUANTITY:** 2  
**ONE REQ'D PER PROPELLANT MANIFOLD**  
**ASSEMBLY:** PROPELLANT FEED  
**P/N:** MC284-0420-0011/0012  
**P/N VENDOR:** 73895-0011/-0012  
**MISSIONS:** HF VF X FF OF SM  
**QUANTITY:** 2  
**ONE REQ'D PER PROPELLANT MANIFOLD**  

**ITEM:** VALVE, DC SOLENOID OPERATED -  
**VERNIER THRUSTER MANIFOLD, (1/4") BI-STABLE, SOLENOID DRIVEN 28VDC.**  
**FUNCTION:**  
1) TO PROVIDE ISOLATION OF PROPELLANT MANIFOLD AND ASSOCIATED VERNIER THRUSTERS 2) PRIOR TO SYSTEM ACTIVATION.  
**FAILURE MODE:** FAIL CLOSED - PREMATURE  
**OPERATION:**  
**CAUSE(S):**  
- IMPROPER ELECTRICAL SIGNAL (CONTINUOUS SHORT), PIECE PART FAILURE, CONTAMINATION, VIBRATION.  
**EFFECT(S):** ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:  
- (A) LOSS OF VERNIER THRUSTER FUNCTION. (B) NONE. (C) POSSIBLE EARLY MISSION TERMINATION, BECAUSE LARGE THRUSTERS INADEQUATE FOR SMALL RATE ATTITUDE CONTROL. (D) NONE.  

**DISPOSITION & RATIONALE:** (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:  
- (A) SERIES CONTROL CIRCUITRY PROVIDED TO MINIMIZE FAILURE MODE. 100 MICRON FILTER IS PROVIDED. MEDIA HAS BEEN FILTERED TO 25 MICRON PRIOR TO ENTERING TANK. SPECIAL EMPHASIS PLACED ON THE DESIGN AND LAYOUT OF SOLENOID WIRING TO PRECLUDE SHORTS. (B) QUAL TEST INCLUDES 48 MINUTES PER AXIS OF RANDOM VIBRATION AT ANTICIPATED MISSION LEVELS AND LIFE TESTING CONSISTING OF 2000 OPERATING CYCLES. ITEM IS USED DURING SYSTEM EVALUATION AT WHITE SANDS TESTING. (C) TURNAROUND INSPECTION INCLUDES MonITORING TESTS TO VERIFY ELECTRICAL POWER TO SOLENOID VALVE FOR EVIDENCE OF SHORT CIRCUIT, SUPPLIER AUDIT CONDUCTED 8-31-77 VERIFIED SUPPLIER INSPECTION EXERCISED CONTROL OF PARTS ID, PARTS PROTECTION, MFG PROCESSES, CONTAMINATION CONTROL, AND CORROSION PROTECTION VERIFICATION. (D) FAILURES ON APOLLO WERE MOSTLY DUE TO CONTAMINATION RESULTING FROM IN-HOUSE PROCESSING.
1. **DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?**
   - **YES**  
   - **NO**

1a. **IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?**
   - **YES**  
   - **NO**

2. **ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?**
   - **YES**  
   - **NO**

3. **DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**
   - **YES**  
   - **NO**

3a. **IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**
   - **YES**  
   - **NO**

4. **AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?**
   - **YES**  
   - **NO**

5. **CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?**
   - **YES**  
   - **NO**

6. **HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)?**
   - **0**
   - **1**
   - **2**

7. **IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?**
   - **YES**  
   - **NO**

8. **IF THE ANSWER TO EITHER 1 OR 3 IS YES:**
   - **A.** WILL BFS BE ENGAGED AFTER OCCURRENCE?  
     - **YES**  
     - **NO**
   - **B.** WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?  
     - **YES**  
     - **NO**

**EXPLANATION REQUIRED (SEE BELOW)**

**CHANGE/RETENTION RATIONALE SUMMARY**

1. **NO H/S ISSUES**
2. **HARDWARE ACCEPTS RISK**
3. **NO SOFTWARE DETECTION**
4. **DETECTION DURING CHECKOUT**
5. **ACCEPTANCE RATIONALE BELOW**
6. **RECOMMENDED CHANGES BELOW**

**EXPLANATION/COMMENTS:**

1. **V42P1115C, 1116C will give a class 2 caution and warning alert.** Gross leak indication will detect failure.

If an internal rupture occurs and helium reaches the thrusters you will get a "fail off" light from redundancy management.

6. **There are no redundant tanks.**

8b. **Backup flight system same as primary.**
SUBSYSTEM : FWD - REACTION CONTROL
ASSEMBLY : PROPELLANT FEED
P/N : MG282-0001-0001/0002
P/N VENDOR : 855320000-009/010
QUANTITY : 2
MISSIONS: HF VF X FF OF SH
FAILURE DETECTABLE IN FLIGHT?: YES
MONITOR TANK PRESSURES: V42P1310C, 1312C, 1316C,
GROUND TURNAROUND?..............YES
PREPARED BY: DES R BEMIS
APPROVED BY: DES ____________________
REL R DIEHL
REL ____________________

ITEM: TANK ASSY, PROPELLANT
INCLUDING PROPELLANT ACQUISITION DEVICE AND COMPARTMENT ENCASER. (TK 102)
FUNCTION:
TO STORE/SUPPLY PROPELLANT TO REACTION CONTROL ENGINE MANIFOLDS.
NOMINAL STORAGE PRESSURE 245 PSIG + OR -15 (1.5 SAFETY FACTOR).
FAILURE MODE: STRUCTURAL FAILURE - (S)
TANK WALL CRACK OR RUPTURE WHICH PROPOGATES AROUND TANK
CAUSE(S): VIBRATION, OVERPRESSURIZATION, MECHANICAL SHOCK, STRESS CORROSION, FATIGUE.
EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF PROPELLANT SUPPLY FOR MODULE THRUSTERS. (B) POTENTIAL FIRE/EXPLOSION AND CERTAIN CONTAMINATION OF SUBSYSTEMS IN RCS COMPARTMENT. (C) LOSS OF MISSION. (D) POTENTIAL LOSS OF CREW/VEHICLE FROM EXPLOSION AND/OR LACK OF PROPELLANT.
CORRECTING ACTION:
NONE AVAILABLE
REMARKS/HAZARDS:
POTENTIAL HAZARUD FROM FIRE, EXPLOSION DUE TO FREE FUEL IN MODULE.
REFERENCE HAZARDS 1YXX-0302-02 AND 1YXX-0302-04.
SUBSYSTEM: FWD - REACTION CONTROL

ASSEMBLY: PROPELLANT FEED

P/N VENDOR: 855C3320000-009/010

MISSIONS: HF, VF, XP, PP, NF, SM

QUANTITY: 2

PHASE(S): PL, LO, X, ON, X, DO, X, LS

PREPARED BY: PREPARED BY:

APPROVED BY: NASA:

DES R BENIS OES

REL R DIEHL REL

APPROVED WITH CHANGES
See Section 13.0

ITEM: TANK ASSY, PROPELLANT

INCLUDING PROPELLANT ACQUISITION DEVICE AND COMPARTMENT BARRIER. (TK 103).

FUNCTION:

TO STORE/SUPPLY PROPELLANT TO REACTION CONTROL ENGINE MANIFOLDS. NOMINAL STORAGE PRESSURE 245 PSIG +/−15 (1.5 SAFETY FACTOR).

FAILURE MODE: STRUCTURAL FAILURE - (S)

TANK WALL CRACK OR RUPTURE WHICH PROPAGATES AROUND TANK

CAUSE(S): VIBRATION, OVERPRESSURIZATION, MECHANICAL SHOCK, STRESS CORROSION, FATIGUE.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:

(A) LOSS OF PROPELLANT SUPPLY FOR MODULE THRUSTERS. (B) POTENTIAL FIRE/EXPLOSION AND CERTAIN CONTAMINATION OF SUBSYSTEMS IN RCS COMPARTMENT. (C) LOSS OF MISSION. (D) POTENTIAL LOSS OF CREW/VEHICLE FROM EXPLOSION AND/OR LACK OF PROPELLANT.

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:

(A) DESIGN FACTR OF SAFETY IS 1.5 MIN. DEVELOPMENT TESTS INCLUDE WELD CYCLE LIFE (800 CYCLES), FRACTURE MECHANICS, FORGING EVALUATION, AND TUBE SHADING. (B) TANKS SUBJECTED TO RADIOGRAPHIC, FLUORESCENT PENETRANT, PROOF PRESSURE (1.33 MAX OPER PRESSURE), AND EXTERNAL LEAK TESTS DURING ACCEPTANCE TESTING. TANKS SUBJECTED TO 90 DAY PROPELLANT EXPOSURE, 800 PRESSURE CYCLES, 48 MINUTES PER AXIS OF 3.9 GRMS RANDOM VIBRATION AND BURST PRESSURE DURING QUAL PROGRAM. (C) TURNAVUD INSPECTION INCLUDES MONITORING FUNCTIONAL TEST DURING PRESSURIZATION CYCLE FOR EVIDENCE OF LEAKS. VISUAL INSPECT WHERE ACCESSIBLE FOR DAMAGE. AUDIT CONDUCTED 11-1-76 VERIFIED SUPPLIER INSPECTION CONTROL OF MTL IDENTIFICATION PARTS PROTECTION AE7 PROCESSES, CORROSION PROTECTION PROVISIONS, NDE EXAM OF WELDS AND STORAGE ENVIRONMENTS. (D) NONE [NEW DEVELOPMENT ITEM].
**SUBSYSTEM**  Fwd Reaction Control  
**FMEA NUMBER**  SD75-SH-0016A

## ITEM: Tank Assembly and Propellant Acquisition  
**FAILURE MODE:** Small Crack - External Leakage Device

1. **DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?**  
   - Yes [✓]  
   - No [ ]

1a. **IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?**  
   - Yes [ ]  
   - No [✓]

2. **ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?**  
   - Yes [✓]  
   - No [ ]

3. **DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**  
   - Yes [ ]  
   - No [✓]

3a. **IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**  
   - Yes [✓]  
   - No [ ]

4. **AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?**  
   - Yes [ ]  
   - No [✓]

5. **CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?**  
   - Yes [ ]  
   - No [✓]

6. **HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.**  
   - Yes [✓]  
   - No [ ]  
   - 2 [ ]

7. **IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?**  
   - Yes [✓]  
   - No [ ]

8. **IF THE ANSWER TO EITHER 1 OR 3 IS YES:**  
   A. **CAN THE BFS BE ENGAGED AFTER OCCURRENCE?**  
      - Yes [✓]  
      - No [ ]
   B. **WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?**  
      - Yes [✓]  
      - No [ ]

*EXPLANATION REQUIRED (SEE BELOW)*

---

**CHANGE/RETENTION RATIONALE SUMMARY**

1. [ ] No H/S issues  
2. [✓] Hardware accepts risk  
3. [ ] No software detection  
4. [ ] Detection during checkout  
5. [ ] Acceptance rationale below  
6. [ ] Recommended changes below

---

**EXPLANATION/COMMENTS:**

1. V42pl1115C, 1116C will give a class 2 caution and warning alert.  
   Gross leak indication will detect failure.  
   If an internal rupture occurs and helium reaches the thrusters you will get a "fail off" light from redundancy management.

6. There are no redundant tanks.

8b. Backup flight system same as primary.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PROPELLANT FEED
P/N VENDOR: 255C332000-009/C1C
P/N: WC282-0061-001/002
P/N VENDOR: 255C332000-009/C1C
QTY: 2

MISSIONS: HF VF X FF OF SM
PHASE(S): PL X LO X CO X OM X LS

NUMBER OF SUCCESS PATHS REMAINING
AFTER FIRST FAILURE:
0

REDUNDANCY SCREEN: A=N/A B=N/A C=N/A

FAILURE DETECTABLE IN FLIGHT?: YES
MONITOR TANK PRESSURE
V42P-1310C,1312C,1316C,
1116C

GROUND TURNAROUND?: YES
SAME AS FLIGHT AND VISUAL OBSERVATION

PREPARED BY: DES R BEMIS
APPROVED BY: DES R DIEHL

ITEM: TANKassy, PROPELLANT
INCCLUDING PROPELLANT ACQUISITION DEVICE AND COMPARTMENT CARRIER. (IN 103).

FUNCTION:
TO STORE/SUPPLY PROPELLANT TO REACTION CONTROL ENGINE MANIFOLDS.

FAILURE MODE: EXTERNAL LEAKAGE - (S)
TANK CRACK OR FLAW WHICH ALLOWS A LIMITED AMOUNT OF PROPELLANT TO LEAVE THE TANK.

CAUSE(S):
VIBRATION, STRESS CORROSION, PRESSURE CYCLES, FATIGUE OR FLANGE SEAL FAILURE.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF A QUANTITY OF PROPELLANT AND HELIUM TO AN EXTENT DEPENDENT ON SIZE AND LOCATION OF LEAK. (B) CONTAMINATION OF SURROUNDING AREA AND SUBSYSTEMS. (C) LOSS OF MISSION. (D) POTENTIAL EXPLOSION AND LOSS OF CREW/VEHICLE IF IGNITION SOURCE PRESENT (SECOND FAILURE).

CORRECTING ACTION:
CLOSE HELIUM PRESSURIZATION ISOLATION VALVE TO MINIMIZE AMOUNT OF PROPELLANT/HELIOUM LOST.

REMARKS/HAZARDS:
POTENTIAL HAZARD FROM FREE PROPELLANT IN MODULE. NO REDUNDANCY PROVIDED FOR THIS ITEM. REFERENCE HAZARD 1YXX-0302-05.
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM : FWD - REACTION CONTROL
ASSEMBLY : PROPELLANT FEED
P/N RI: MCZ06-0661-0002
P/N VENDOR: 855E3120000-009/010
QUANTITY: 2
ONE REQ'D PER PROPELLANT

PREPARED BY: DES: R. BEHIS
REL: R. DIEHL
APPROVED BY: DES: S. SMITH
REL: C. BUSH

ITEM: TANK ASSY, PROPELLANT
INCLUDING PROPELLANT ACQUISITION DEVICE AND COMPARTMENT BARRIER. (TK 103).

FUNCTION:
TO STORE/SUPPLY PROPELLANT TO REACTION CONTROL ENGINE MANIFOLDS. NOMINAL STORAGE PRESSURE 245 PSIG + OR -15 (1.5 SAFETY FACTOR).

FAILURE MODE: EXTERNAL LEAKAGE - (S)
TANK CRACK OR FLAW WHICH ALLOWS A LIMITED AMOUNT OF PROPELLANT TO LEAVE THE TANK.

CAUSE(S):
VIBRATION, STRESS CORROSION, PRESSURE CYCLES, FATIGUE OR FLANGE SEAL FAILURE.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF A QUANTITY OF PROPELLANT AND HELIUM TO AN EXTENT DEPENDENT ON SIZE AND LOCATION OF LEAK. (B) CONTAMINATION OF SURROUNDING AREA AND SUBSYSTEMS. (C) LOSS OF MISSION. (D) POTENTIAL EXPLOSION AND LOSS OF CREW/VEHICLE IFignition SOURCE PRESENT (SECOND FAILURE).

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
(A) DESIGN FACTOR OF SAFETY IS 1.5 MIN. DEVELOPMENT TESTS INCLUDE WELD CYCLE LIFE (800 CYCLES), FRACTURE MECHANICS, FORGING EVALUATION, AND TUBE SWAGING. (B) TANKS SUBJECTED TO RADIOGRAPHIC; FLUORESCENT PENETRANT, PROOF PRESSURE (1.33 MAX OPER PRESSURE), AND EXTERNAL LEAK TESTS DURING ACCEPTANCE TESTING. TANKS SUBJECTED TO 90 DAY PROPELLANT EXPOSURE, 800 PRESSURE CYCLES, 48 MINUTES PER AXIS OF 3.9 GMS RANDOK VIBRATION; AND BURST PRESSURE DURING QUAL PROGRAM. (C) TURNAROUND INSPECTION INCLUDES MONITORING FUNCTIONAL TEST DURING PRESSURIZATION CYCLE FOR EVIDENCE OF LEAKS; VISUAL INSPECT WHERE ACCESSIBLE FOR DAMAGE. AUDIT CONDUCTED 11-1-76 VERIFIED SUPPLIER INSPECTION CONTROL OF MATL IDENTIFICATION PARTS PROTECTION MFG PROCESSES, CORROSION PROTECTION PROVISIONS, NDE EXAM OF WELDS AND STORAGE ENVIRONMENTS. (D) NONE (NEW DEVELOPMENT ITEM).
1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?  
   YES ☑ NO ☐

1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?  
   *YES ☑ NO ☑

2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?  
   YES ☑ *NO ☑

3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?  
   YES ☑ *NO ☑

3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?  
   *YES ☑ NO ☑

4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?  
   *YES ☑ NO ☑

5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?  
   *YES ☑ NO ☑

6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.  
   0 ☑ 1 ☐ 2 ☐

7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?  
   N/A ☑ YES ☑ NO ☐

8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:  
   A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?  
      YES ☑ *NO ☑

   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?  
      YES ☑ *NO ☑

*EXPLANATION REQUIRED (SEE BELOW)

CHANGE/RETENTION RATIONALE SUMMARY:

1. ☐ NO H/S ISSUES  3. ☐ NO SOFTWARE DETECTION  5. ☐ ACCEPTANCE RATIONALE BELOW
2. ☑ HARDWARE ACCEPTS RISK  4. ☐ DETECTION DURING CHECKOUT  6. ☐ RECOMMENDED CHANGES BELOW

EXPLANATION/COMMENTS:

1. "Fail Off" detection in RCS RM.

6. No redundant tanks.

7. No correcting action... abort...

8b. Same as primary.
### SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER IC2

**SUBSYSTEM**: FWD - REACTION CONTROL  
**ASSEMBLY**: PROPELLANT FEED  
**P/N**: MC282-0061-0001/0002  
**P/N VENDOR**: 550C33200GC-009/010  
**QUANTITY**: 2  
**ONE REQ'D**: NO  
**PER PROPELLANT**: NO  

**MISSIONS**: HF, VF, X, FF, UF, SM  
**PHASE(S)**: PL, LC, X, CO, X, LC, X, LS  

**FAILURE DETECTABLE IN FLIGHT?**: YES  
**ENGINE PERFORMANCE**: SECONDS TO DAYS  
**GROUND TURNAROUND?**: NO  

**PREPARED BY**:  
**APPROVED BY**:  

---

**ITEM**: TANK ASSY, PROPELLANT  
**INCLUDING**: PROPELLANT ACQUISITION DEVICE AND COMPARTMENT EARRIER. (TK 103).  
**FUNCTION**:  
**TO STORE/SUPPLY PROPELLANT TO REACTION CONTROL ENGINE MANIFOLDS. NOMINAL STORAGE PRESSURE 245 PSIG + OR -15 (1.5 SAFETY FACTOR).**  
**FAILURE MODE**: RESTRICTED FLOW - (S)  
**STRUCTURAL FAILURE OF PROPELLANT ACQUISITION DEVICE WHICH BLOCKS OR RETARDS RATE OF FLOW OF PROPELLANT INTO TANK OUTLET.**  
**CAUSE(S)**:  
VIBRATION, MECHANICAL SHOCK, EXCESSIVE FLOW RATES DUE TO EXCESSIVE GAS IN THRUSTER MANIFOLD. (SEE FAILURE MODE NO. 4 ON NEXT PAGE).  
**EFFECT(S)**: ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:  
(A) LOSS OF FULL PROPELLANT FLOW CAPABILITY/HELLEUM INGESTION. (B) NONE.  
(C) LOSS OF MISSION DUE TO LOSS OF PROPELLANT. (D) NOSE UNLESS FAILURE OCCURS WHEN MODULE REQUIRED FOR ET SEPARATION.  
**CORRECTING ACTION**:  
NONE AVAILABLE - CLOSE DOWN FRCS AND ABORT MISSION.  
**REMARKS/HAZARDS**:  
COMPLETE LOSS OF FRCS USAGE THEREFORE ALL ATTITUDE CONTROL MUST BE ACCOMPLISHED BY ARCS.

---

**ORIGINAL PAGE IS OF POOR QUALITY**
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

- SUBSYSTEM: FWD - REACTION CONTROL
- ASSEMBLY: PROPELLANT FEED ABORT:
- P/N RI: MC282-0061-0001/0002
- P/N VENDOR: 855C332 0000-009/O10
- QUANTITY: 2
  - ONE REQ'D
  - PER PROPELLANT REEDUNDANCY SCREEN: A-N/A B-N/A C-N/A
- PREPARED BY: DES R. BEMIS DES
  REL R. DIEHL REL
  APPROVED BY: SSM
  APPROVED WITH CHANGES
  11-1-76
- VENDOR: 855C332 0000-009/O10 MISSIONS: HF VFX FF OF SH.
- PHASE(S): PL LO X NO X DO X LS
- FMEA NO 03-2F -111110-3 REV: 11/10/76
- CRIT. FUNC: 1
  CRIT. HDW: 1
- MISSIONS: HF VFX FF OF SH.
- REDUNDANCY SCREEN: A-N/A B-N/A C-N/A
- APPROVED BY NASA
  11-1-76
- ITEM: TANK ASSY, PROPELLANT
  INCLUDING PROPELLANT ACQUISITION DEVICE AND COMPARTMENT BARRIER (TK 103).
- FUNCTION:
  TO STORE/SUPPLY PROPELLANT TO REACTION CONTROL ENGINE MANIFOLDS. NOMINAL
  STORAGE PRESSURE 245 PSIG ± 15 (1.5 SAFETY FACTOR).
- FAILURE MODE: RESTRICTED FLOW - (S)
  STRUCTURAL FAILURE OF PROPELLANT ACQUISITION DEVICE WHICH BLOCKS OR
  RETARDS RATE OF FLOW OF PROPELLANT INTO TANK OUTLET.
- CAUSE(S):
  VIBRATION, MECHANICAL SHOCK, EXCESSIVE FLOW RATES DUE TO EXCESSIVE GAS
  IN THRUSTER MANIFOLD. (SEE FAILURE MODE NO. 4 ON NEXT PAGE).
- EFFECT(S): ON (A) SUBSYSTEMS (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
  (A) LOSS OF FULL PROPELLANT FLOW CAPABILITY/HELIUM INGESTION. (B) NONE.
  (C) LOSS OF MISSION DUE TO LOSS OF PROPELLANT. (D).NONE UNLESS FAILURE
  OCCURS WHEN MODULE REQUIRED FOR ET SEPARATION.
- DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
  (A) 1.5 DESIGN SAFETY FACTOR. DEVELOPMENT TESTS VERIFY WELD CYCLE LIFE,
  SCREEN REPAIR METHOD, SCREEN CYCLE LIFE AND SCREEN FLOW. (B) PROPELLANT
  ACQUISITION DEVICE COMPONENTS, SUBASSEMBLIES AND TANK ASSY INTEGRITY
  VERIFIED BY PERFORMING BUBBLE POINT TEST. TANKS SUBJECTED TO PROPELLANT
  EXPOSURE, 200 EXPULSION CYCLES, 48 MINUTES PER AXIS OF 3.9 G'S RANDOM
  VIBRATION AND BURST PRESSURE DURING QUAL PROGRAM. (C) TURNAROUND
  INSPECT INCLUDES MONITOR FLOW DURING FUNCTIONAL TESTS. AUDIT CONDUCTOR
  11-1-76 VERIFIED SUPPLIER INSPECTION CONTROL OF MATL IDENTIFICATION
  PARTS PROTECTION MFG PROCESSES, CORROSION PROTECTION PROVISIONS, NDE
  EXAM OF WELDS AND STORAGE ENVIRONMENTS. (D) NONE (NEW DEVELOPMENT ITEM).
HARDWARE/SOFTWARE ANALYSIS CHECKLIST
SUBSYSTEM: Fwd Reaction Control
FMEA NUMBER: SD75-SH-D016A

ITEM: Tank Assembly and Propellant Acquisition Failure Mode: Loss of Gas in Propellant Device

1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?

YES ☒ NO ☐

1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?

*YES ☐ NO ☒

2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?

*YES ☐ NO ☒

3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?

*YES ☒ NO ☐

3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?

*YES ☒ NO ☐

4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?

*YES ☒ NO ☐

5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?

*YES ☒ NO ☐

6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.

*0 ☒ 1 ☐ 2 ☐

7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?

N/A ☐ YES ☒ NO ☒

8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:

A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?

YES ☒ *NO ☐

B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?

YES ☒ *NO ☐

*EXPLANATION REQUIRED (SEE BELOW)

CHANGE/RETENTION RATIONALE SUMMARY

1. ☐ NO H/S ISSUES 3. ☐ NO SOFTWARE DETECTION 5. ☐ ACCEPTANCE RATIONALE BELOW
2. ☒ HARDWARE ACCEPTS RISK 4. ☐ DETECTION DURING CHECKOUT 6. ☐ RECOMMENDED CHANGES BELOW

EXPLANATION/COMMENTS:

1. "Fail Off" detection in RCS RM.
6. No redundant tanks.
7. No correcting action - abort.
8. Same as primary.
SUBSYSTEM : FWD - REACTION CONTROL  
ASSEMBLY : PROPELLANT FEED  
P/N/RI : MC282-C661-001/002  
P/N VENDOR : 655632000C-004/016  
MISSIONS : HF, VF, X, FF of SM  
QUANTITY : 2  
PHASE(S) : PL, X, LC, X, DW, X, DW, X, LS  
REDUNDANCY SCREEN : A-N/A, B-N/A, C-N/A  
FAILRE DETECTABLE IN FLIGHT? YES  
ENGINE PERFORMANCE AND COMPARTMENT PRESSURE : V42P1541  
GROUND TURNAROUND? NO  
PREPARED BY: DES, R, BEMIS, DES  
APPROVED BY: REL, R, DIEHL, REL

ITEM: TANK ASSY, PROPELLANT  
INCLUDING PROPELLANT ACQUISITION DEVICE AND COMPARTMENT BARRIER (TK 103).  
FUNCTION:  
TO STORE/SUPPLY PROPELLANT TO REACTION CONTROL ENGINE MANIFOLDS.  
NOMINAL STORAGE PRESSURE 245 PSIG + OR -15 (1.5 SAFETY FACTOR).  
FAILRE MODE: LOSS OF GAS RETENTION IN (S)  
PROPELLANT ACQUISITION DEVICE (PAC).  
CAUSE(S):  
VIBRATION, SHOCK, PROPELLANT CONTAMINATION (CHEMICAL OR DIRT).  
EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (L) CTRX/VEHICLE:  
(A) EXCESSIVE GAS FLOW TO THRUSTERS COULD CAUSE TANK BARRIER FAILURE.  
(B) POTENTIAL DAMAGE TO THRUSTERS IF UNDETECTED.  
(C) ADEQUATE DECISION.  
(D) POSSIBLE LOSS OF CREW/VEHICLE IF FAILURE OCCURS PRIOR TO LT SEPARATION.  
CORRECTING ACTION:  
SHUT DOWN FRCS AND ABORT MISSION.  
REMARKS/HAZARDS:  
IF UNDETECTED, THE THRUSTERS COULD BE DAMAGED WHICH COULD CAUSE ENTRY UNCERTAINTY.
**SUBSYSTEM**: FWD - REACTION CONTROL  
**ASSEMBLY**: PROPELLANT FEED ABORT: CPIT. FUNC: 2  
**P/N RI**: YCG202-0061-0001/0002  
**P/N VENDOR**: 855C3320000-009/010  
**MISSIONS**: HF VF X FF DF SM  
**FUNCTION**: TO STORE/SUPPLY PROPELLANT TO REACTION CONTROL ENGINE MANIFOLDS. NCHIA STORAGE PRESSURE 245 PSIG + OR -15 (1.5 SAFETY FACTOR).  
**FAILURE MODE**: LOSS OF GAS RETENTION IN (S)  
**PROPELLANT ACQUISITION DEVICE (PAD)**.  
**CAUSE(S)**: VIBRATION, SHOCK, PROPELLANT CONTAMINATION (CHEMICAL OR DIRT).  
**EFFECT(S)**: ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:  
(A) EXCESSIVE GAS FLOW TO THRUSTERS COULD CAUSE TANK BARRIER FAILURE.  
(B) POTENTIAL DAMAGE TO THRUSTERS IF UNDETECTED.  
(C) ABORT DECISION.  
(D) POSSIBLE LOSS OF CREW/VEHICLE IF FAILURE OCCURS PRIOR TO ET SEPARATION.  
**DISPOSITION & RATIONALE**:  
(A) DESIGN FACTOR OF SAFETY IS 1.5. DEVELOPMENT TESTS INCLUDE WELD CYCLE LI FE (800 CYCLES), FRACTURE MECHANICS, FORGING EVALUATION, AND TUBE SWAGING.  
(B) PROPELLANT ACQUISITION DEVICE COMPONENTS, SUBASSEMBLIES AND TANK ASSY INTEGRITY VERIFIED BY PERFORMING BUBBLE POINT TESTS. TANKS SUBJECTED TO PROPellant EXPOSURE, 200 EXPULSION CYCLES, 45 MINUTES PER AXIS OF 3.9 GRMS RANDOM VIBRATION AND BURST PRESSURE DURING QUAL PROGRAM.  
(C) TURNOVER INSPECTION INCLUDES PERIODIC BUBBLE POINT CHECKS OF THE PAD. AUDIT CONDUCTED 11-1-76 VERIFIED SUPPLIER INSPECTION CONTROL OF MATE IDENTIFICATION PARTS PROTECTION MFG PROCESSES, CORROSION PROTECTION PROVISIONS, NDE EXAM OF WELDS AND STORAGE ENVIRONMENTS.  
(D) NONE (NEW DEVELOPMENT ITEM).
**HARDWARE/SOFTWARE ANALYSIS CHECKLIST**

**SUSSYSTEM**: Fwd Reaction Control  
**FMEA NUMBER**: SD75-SH-0016A  
**ITEM**: Flex Line and Fittings  
**FAILURE MODE**: External Leakage

<table>
<thead>
<tr>
<th>Quesiton</th>
<th>Yes</th>
<th>No</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?</strong></td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>1a. <strong>IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?</strong></td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>2. <strong>ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?</strong></td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>3. <strong>DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?</strong></td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>3a. <strong>IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?</strong></td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>4. <strong>AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?</strong></td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>5. <strong>CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, AVERSELY AFFECT OTHER FUNCTIONS?</strong></td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>6. <strong>HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)?</strong></td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>7. <strong>IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?</strong></td>
<td>N/A</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>8. <strong>IF THE ANSWER TO EITHER 1 OR 3 IS YES:</strong> A. <strong>CAN THE BFS BE ENGAGED AFTER OCCURRENCE?</strong></td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>8. <strong>WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?</strong></td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
</tbody>
</table>

*EXPLANATION REQUIRED (SEE BELOW)*

---

**CHANGE/RETENTION RATIONALE SUMMARY**

1. NO H/S ISSUES  
2. HARDWARE ACCEPTS RISK  
3. NO SOFTWARE DETECTION  
4. DETECTION DURING CHECKOUT  
5. ACCEPTANCE RATIONALE BELOW  
6. RECOMMENDED CHANGES BELOW

---

**EXPLANATION/COMMENTS:**

1. V42P1115C, 1116C will give class 2 alarm.

Gross leak detection applies.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: THRUSTER
P/N: MC271-0084
P/N VENDOR: 74713-Thru 74717
VENDOR: 74713-TRU 74717
QUANTITY: 3
FUNCTION: TO PROVIDE COUPLING BETWEEN PROPELLANT SUBSYSTEM AND FORWARD RCS PRIMARY AND VERNIER THRUSTER.

FAILURE MODE: EXTERNAL LEAKAGE - (S)

CAUSE(S): FATIGUE, SHOCK, VIBRATION, HANDLING.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CARGO/VEHICLE:
(A) LOSS OF PROPELLANTS TO EXTENT OF LEAK SIZE. (B) INCREASED GROWTH.
CONTROL & USE OF ALTERNATE THRUSTERS. (C) POTENTIAL MISSION TERMINATION PRIOR TO PLANNED TIME. (D) NO EFFECT AFTER ASCENT UNLESS LEAK IS EXCESSIVE & RESULTS IN IGNITION WITH REACTANT (SECOND ORDER FAILURE) THE RITS ABORT THE LOSS OF A MANIFOLD RESULTS IN THE LOSS OF TWO DOWN FIRING THRUSTERS WHICH RESULTS IN A CRITICAL MISSION TERMINATION PRIOR TO PLANNED TIME. (D) NO EFFECT AFTER ASCENT UNLESS LEAK IS EXCESSIVE & RESULTS IN IGNITION WITH REACTANT (SECOND ORDER FAILURE) DURING ASCENT THE FAILURE CANNOT BE DETECTED AND ISOLATED WHICH RESULTS IN POSSIBLE LOSS OF VEHICLE.

CORRECTING ACTION:
ISOLATE THRUSTER AT MANIFOLD.

REMARKS/HAZARDS:
POTENTIAL HAZARD FROM FREE FUEL IN MODULE.

ORIGINAL PAGE IS OF POOR QUALITY

92
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM: FWD - REACTION CONTROL  FMEA NO 03-ZF -121303-1 REV:11/10/
ASSEMBLY: THRUSTER
P/N: MC271-0084
P/N VENDOR: 74713-THRU 74717
MISSIONS: HF VF X FF JF X SM
QUANTITY : 30
PHASE(S): PL x LO X OQ X CO X LS X

* ONE FUEL AND ONE OXIDIZER PER THRUSTER

PREPARED BY: J. TAGGART
APPROVED BY: SSM
DES REL
R DIEHL

ITEM: LINE ASSEMBLY FLEXIBLE AND FITTINGS
FUNCTION:
TO PROVIDE COUPLING BETWEEN PROPELLANT SUBSYSTEM AND FORWARD RCS PRIMARY AND VERNIER THRUSTER.

FAILURE MODE: EXTERNAL LEAKAGE - Rupture of line or coupling.

CAUSE(S):
Fatigue, shock, vibration, handling.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF PROPELLANTS TO EXTENT OF LEAK SIZE. (B) INCREASED GN&C CONTROL & USE OF ALTERNATE THRUSTERS. (C) POTENTIAL MISSION TERMINATION PRIOR TO PLANNED TIME. (D) NO EFFECT AFTER ASCENT UNLESS LEAK IS EXCESSIVE & RESULTS IN IGNITION OF REACTANT (2ND ORDER FAILURE) DURING A RTLS ABDOT THE LOSS OF A MANIFOLD RESULTS IN THE LOSS OF TWO DCN FIRING THRUSTERS WHICH RESULTS IN CRIT 1. DURING ASCENT THE FAILURE CANNOT BE DETECTED AND ISOLATED WHICH RESULTS IN POSSIBLE LOSS OF VEHICLE.

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
(A) DESIGN BURST PRESSURE IS UP TO 3 TIMES THE MAX OPER PRESSURE OF 700 PSIG. PROOF PRESSURE IS UP TO 1.5 TIMES THE MAX OPER PRESSURE. THE DESIGN ALLOWS SUFFICIENT MOVEMENT TO PRECLUDE EXCESSIVE STRESSES DURING INSTALLATION AND OPERATION. LINES CAN BE ISOLATED AT THE MANIFOLD IN CASE OF LEAKAGE. (B) POST INSTALLATION TEST AND OPERATIONAL CHECKOUTS WILL VERIFY SYSTEM INTEGRITY. ALL LINES SUBJECTED TO PROOF PRESSURE DURING ATP AND RANDOM VIBRATION AT ANTICIPATED MISSION LEVELS DURING QUAL TESTING. LINES ARE ALSO TESTED DURING SYSTEM EVALUATION AT WHITE SANDS TEST FACILITY. (C) SEE FMEA/CIL 102126-1. (D) NO HISTORY OF FAILURE IN FLIGHT. (NEW DEVELOPMENT ITEM FOR MANNED FLIGHT APPLICATION.)

C-2

93-034  SD75-SH-0003
## HARDWARE/SOFTWARE ANALYSIS CHECKLIST

**SUBSYSTEM**  
Fwd. Reaction Control

**ITEM**  
Injector Plate

**FAILURE MODE**  
Improper Mixture Ratio

**FMEA NUMBER**  
SD75-SH-0016A

---

### 1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?

- **YES** [X]  
- **NO** [ ]

### 1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?

- **YES** [ ]  
- **NO** [X]

### 2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?

- **YES** [X]  
- **NO** [ ]

### 3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?

- **YES** [ ]  
- **NO** [X]

### 3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?

- **YES** [ ]  
- **NO** [X]

### 4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?

- **YES** [ ]  
- **NO** [X]

### 5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?

- **YES** [ ]  
- **NO** [X]

### 6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)?  
**NOTE CHANGE TO FMEA CRITICALITY.**

- **YES** [X]  
- **NO** [ ]

### 7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?

- **YES** [ ]  
- **NO** [X]

### 8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:

- **A.** CAN THE BFS BE ENGAGED AFTER OCCURRENCE?  
  - **YES** [ ]  
  - **NO** [X]

- **B.** WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?  
  - **YES** [X]  
  - **NO** [ ]

*EXPLANATION REQUIRED (SEE BELOW)*

---

### CHANGE/RETENTION RATIONALE SUPPLEMENT:

1. **[ ] NO H/S ISSUES**  
2. **[X] HARDWARE ACCEPTS RISK**  
3. **[ ] NO SOFTWARE DETECTION**  
4. **[ ] DETECTION DURING CHECKOUT**  
5. **[ ] ACCEPTANCE RATIONALE BELOW**
6. **[ ] RECOMMENDED CHANGES BELOW**

---

**EXPLANATION/COMMENTS:**

1. "Fail Off" in RCS RM if sufficiently blocked.

---

94
SUBSYSTEM: FW - REACTION CONTROL

ASSEMBLY: THRUSTER, PRIMARY

P/N: MC467-0028

P/N VENDOR: X3C668

QUANTITY: 14

PLANNED MISSIONS: HFVFX EF CF SM

FAILURE DETECTABLE IN FLIGHT?: NO

GROUND TURNAROUND?: NO

PREPARED BY: W. Searcy

APPROVED BY: R. Diehl

ITEM: INJECTOR, PLATE

FUNCTION:

TO RECEIVE FUEL AND OXIDIZER FROM THRUSTER INLET VALVES AND PROVIDE DOUBLET MIXING AT 1:60 OX TO FUEL (WEIGHT) RATIO FOR A HYPERGULIC REACTION WHICH PRODUCES 825 POUNDS OF THRUST AT 76,000 FEET. ALSO CONTROL CHAMBER WALL COOLING.

FAILURE MODE: FAILS TO DELIVER PROPS (F) AT PROPER MIXTURE RATIO AND FAILS TO PROVIDE ADEQUATE COOLING OF THE COMBUSTOR WALL.

CAUSE(S):

- CONTAMINATION, BLOCKED ORIFICES.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:

- (A) LOSS OF ONE THRUSTER IN A GIVEN AXIS. (D) GNC CONTROL SWITCHING REQUIRED. (C,G) NO EFFECT. (E) POSSIBLE LOSS OF VEHICLE IF FAILURE OCCURS BEFORE ET SEPARATION. DOWN FIRING THRUSTERS REQUIRED FOR ET SEPARATION.

CORRECTING ACTION:

- SWITCH TO REDUNDANT THRUSTER IN AFFECTED AXIS. ISOLATE MANIFOLD CONTAINING FAILED THRUSTER.

REMARKS/HAZARDS:

- POSSIBLE LOCAL HOT SPOT RESULTING IN COATING DAMAGE OR COMBUSTOR BURN THROUGH.
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: THRUSTER, PRIMARY
P/N: MC467-0028
P/N VENDOR: X30888
QUANTITY: 14

DESCRIPTION:
- ONE INJECTOR PROVIDED FOR EACH PRIMARY THRUSTER
- REACTANTS: FUEL AND OXIDIZER FROM THRUSTER INLET VALVES
- MIXING: DOUBLET MIXING AT 1.60 OX TO FUEL (WEIGHT) RATIO
- REACTION: HYPERGOLIC REACTION PRODUCES 825 POUNDS OF THRUST AT 70,000 FEET
- CONTROL: CHAMBER WALL COOLING

FAILURE MODE:
- FAILS TO DELIVER PROPS AT PROPER MIXTURE RATIO
- FAILS TO PROVIDE ADEQUATE COOLING OF THE COMBUSTOR WALL

CAUSE(S):
- CONTAMINATION, BLOCKED ORIFICES

EFFECT(S):
- (A) LOSS OF ONE THRUSTER IN A GIVEN AXIS
- (B) GNC CONTROL SWITCHING REQUIRED
- (C) NO EFFECT
- (D) POSSIBLE LOSS OF VEHICLE IF FAILURE OCCURS BEFORE ET SEPARATION. DOWN FIRING THRUSTERS REQUIRED FOR ET SEPARATION

DISPOSITION & RATIONALE:
- (A) DESIGN
- (B) TEST
- (C) INSPECTION
- (D) FAILURE HISTORY

- 75 MICRON FILTER PROVIDED UPSTREAM TO PRECLUDE CONTAMINATION
- FUEL HAS BEEN FILTERED TO 25 MICRONS PRIOR TO ENTERING TANK
- ACOUSTIC CAVITIES PRECLUDE OCCURRENCE OF COMBUSTION INSTABILITY IN THE EVENT OF POOR DISTRIBUTION
- TOTAL FLOW & FLOW DISTRIBUTION CHECKED BY WATER FLOW TEST AND VERIFIED BY BURN TEST DURING THRUSTER ACCEPTANCE TESTS
- FIBER OPTICS USED TO VISUALLY INSPECT INJECTOR HOLES FOR EVIDENCE OF BURRS AND CONTAMINATION PRIOR TO ASSEMBLY
- SUPPLIER INSPECTION CONTROLS RAW MATERIAL VERIFICATION, PARTS PROTECTION, MFG FAB AND ASSY OPERATIONS, CONTAMINATION CONTROL, CORROSION CONTROL PROVISIONS AND STORAGE ENVIRONMENTS
- TURN AROUND INSPECTION TO INCLUDE USE OF OPTICS INSPECTION WHERE ACCESSIBLE FOR EVIDENCE OF DAMAGE & SYSTEM FLUID SAMPLINGS FOR DETECTION OF CONTAMINATION

PREPARED BY: W. SEARCY
APPROVED BY: J. DEAN
APPROVED ON: (NASA):
REL R. DIEHL

See Section 13.0

DELTA

SD75-SH-0003
<table>
<thead>
<tr>
<th>Item: Thrust Chamber</th>
<th>Failure Mode: Burn Through</th>
</tr>
</thead>
</table>

1. **Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?**
   - Yes [x] No [ ]

1a. **If not, does the hardware provide information that the flight software could use to detect the failure?**
   - Yes [ ] No [x] *

2. **Are the answers to questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?**
   - Yes [x] No [ ] *

3. **Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?**
   - Yes [x] No [ ] *

3a. **If not, does the capability exist for the software to compensate for this failure mode (either by commanding hardware action or implementing alternate program logic)?**
   - Yes [x] No [ ] *

4. **As a result of this failure mode, can the software overstress the hardware or induce another failure?**
   - Yes [x] No [ ] *

5. **Can this failure mode, in combination with software logic, adversely affect other functions?**
   - Yes [x] No [ ] *

6. **How many of these hardware failures can the Shuttle tolerate (consider crew action and Hardware/Software operation)? Note change to FMEA criticality.**
   - 0 [ ] 1 [x] 2 [x]

7. **If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?**
   - N/A [ ] Yes [x] No [ ] *

8. **If the answer to either 1 or 3 is Yes:**
   - A. Can the BFS be engaged after occurrence? Yes [x] No [ ] *
   - B. Will BFS tolerate failure without loss of crew/vehicle? Yes [x] No [ ] *

*Explanation required (see below)*

**Change/Retention Rationale Summary**

1. [ ] No H/S issues
2. [x] Hardware accepts risk
3. [ ] No software detection
4. [ ] Detection during Checkout
5. [ ] Acceptance Rationale Below
6. [ ] Recommended Changes Below

**Explanation/Comments:**

FMEA change - Measurement numbers V42X1541X through V42X1556X should be listed as V42P1541A through V42P1556A.

1. RM uses thrust chamber pressure transducers to sense the low pressure in question and give a "fail off" in RCS RM.

7. The thrust chamber measurements are downlinked.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 1C2

SUBSYSTEM : Fwd - REACTION CONTROL
ASSEMBLY : THRUSTER, PRIMARY
P/N VENDOR: MC467-0028
P/N: X50958
QUANTITY: 14
P/N: MC6T-0028 CRITICAL

MISSIONS: HF VF X FF OF SM
PHASE(S): PL LO X DD X CD X LS
QUANTITY: 14 PER THRUSTER

NUMBER OF SUCCESS PATHS REMAINING:
AFTER FIRST FAILURE:

FAILURE DETECTABLE IN FLIGHT?: YES
INCIPIENT BURN-THRU DETECTORS V42X1541X THROUGH SECONDS
V42X1556X PC TRANS DUCER IF LEAKAGE
GROUND TURNAROUND?: YES
VISUAL EXAMINATION

* : ON " PER THRUSTER NUMBER OF SUCCESS PATHS REMAINING

REduNDANCY SCREEN: A-N/A B-N/A C-N/A

PREPARED BY: DES W SEARCY
APPROVED BY: DES R DIEHL

ITEM: THRUST CHAMBER FROM INJECTOR TO NOZZLE EXTENSION (COATED COLUMBIUM).
FUNCTION:
TO CONTAIN HYPERGOLIC REACTION OF PROPELLANTS AND TO EXPAND COMBUSTION PRODUCTS TO PRODUCE THRUST THROUGH NOZZLE EXTENSION TO PROVIDE IMPULSE TO VEHICLE.

FAILURE MODE: OVERHEAT/BURNTHROUGH (S)
DUE TO INADEQUATE COOLING.

CAUSE(S):
BLOCKED (CONTAMINATED) COOLANT (FUEL) INJECTOR HOLES, POOR BOUNDARY FLOW CONDITIONS COMBUSTION INSTABILITY, SEPARATION OR FRACTURE OF PROTECTIVE DILSICIDE COATING.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES, (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF A PRIMARY THRUSTER IN A GIVEN AXIS. (B) INCREASED GNCC CONTROL AUTHORITY REQUIRED. (C) POTENTIAL LOSS OF MISSION ABORT DECISION. (D) POTENTIAL LOSS OF VEHICLE. CRITICAL DAMAGE COULD OCCUR BEFORE FAILURE IS DETECTED.

CORRECTING ACTION:
ISOLATE THRUSTER AND UTILIZE REDUNDANT THRUSTER IN AFFECTED AXIS. (AUTOMATIC FUNCTION).

REMARKS/HAZARDS:
POTENTIAL HAZARD FROM ESCAPING HOT GASES IN MODULE AND POTENTIAL PROPAGATION OF FAILURE IF NOT ISOLATED IN A TIMELY MANNER.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: THRUSTER, PRIMARY
P/N: 4C467-0029
P/N VENDOR: X30958
QUANTITY: 14
ONE PER THRUSTER

MISSION: HF V6 X FF OF SM
PHASE(S): PL LO X DO X DD X LS

REduNDANCY SCREEN: A-N/A B-N/A C-N/A

PREPARED BY: W. SEARCY
APPROVED BY: DES
APPROVED: NASA
REL: R. DIEHL

ITEM: THRUST CHAMBER
FROM INJECTOR TO NOZZLE EXTENSION (COATED COLUMBIA)

FUNCTION:
TO CONTAIN HYPERGOLIC REACTION OF PROPELLANTS AND TO EXPAND COMBUSTION PRODUCTS TO PRODUCE THRUST THROUGH NOZZLE EXTENSION TO PROVIDE IMPULSE TO VEHICLE.

FAILURE MODE: OVERHEAT/BURNTHROUGH (S)
DUE TO INADEQUATE COOLING.

CAUSE(S):
BLOCKED (CONTAMINATED) COOLANT (FUEL) INJECTOR HOLES, POOR BOUNDARY FLOW CONDITIONS COMBUSTION INSTABILITY, SEPARATION OR FRACTURE OF PROTECTIVE DISILICIDE COATING.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF A PRIMARY THRUSTER IN A GIVEN AXIS. (B) INCREASED GN&C CONTROL AUTHORITY REQUIRED. (C) POTENTIAL LOSS OF MISSION ABORT DECISION. (D) POTENTIAL LOSS OF VEHICLE. CRITICAL DAMAGE COULD OCCUR BEFORE FAILURE IS DETECTED.

DISPOSITION & RATIONALE:
(A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
INTERMETALLIC DIFFUSION LAYER FORMS AN INTEGRAL BOND BETWEEN THE DISILICIDE COATING AND THE PARENT COLUMBIA MATERIAL AND TENDS TO RESIST SHOCK LOADING. 75 MICRON FILTER IN VALVE INLET UPSTREAM OF INJECTOR HOLES WILL PRECLUDE ENTRY OF CONTAMINANTS. ACOUSTIC CAVITIES DAMPEN THE FREQUENCIES THAT EXCITE INSTABILITY. (B) SIMULATED THRUSTERS AND THRUSTER NO. 5 VIBRATION TESTS HAVE DEMONSTRATED THE ABILITY OF THE DISILICIDE COATING TO WITHSTAND 2.0 G SQUARED PER Hertz RANDOM VIBRATION STRESSES. THRUSTER IS SUBJECTED TO RANDOM VIBRATION AT ANTICIPATED MISSION LEVELS DURING THE QUAL. PROGRAM. (C) COATING THICKNESS AND QUALITY WILL BE CONTROLLED BY SUPPLIER INSPECTION PROCEDURE MPS 525 WHICH REQUIRES CERTIFICATION THAT COATING PROCESS CONFORMS TO THE PROCESS SPEC. VISUAL INSPECTION, VERIFICATION OF COATING THICKNESS AND A SMOKE TEST THAT VERIFIES COAT INTEGRITY. TURNAROUND INSPECTION TO INCLUDE VISUAL INSPECTION FOR EVIDENCE OF BURN THRU. (D) NO FLIGHT FAILURE HISTORY. (2) DEVELOPMENT FAILURES HAVE OCCURRED ON SHUTTLE PROGRAM. ONE FAILURE DUE TO DOUBLET DESIGN WHICH HAS BEEN CHANGED AND ONE FAILURE DUE TO THIN COAT OF DISILICIDE COATING. THIN COAT STILL WITHSTOOD MORE FIRING TIME THAN IS NORMALLY SEEN BY THE THRUSTER IN NORMAL 100 MISSION LIFE.
1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNOUNCE OR TAKE ACTION IN RESPONSE)?  
   YES ☐ NO ☑ 

1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?  
   ΡYES ☐ NO ☐ 

2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?  
   YES ☑ NO ☐ 

3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?  
   YES ☑ NO ☐ 

3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?  
   ΡYES ☑ NO ☐ 

4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?  
   YES ☐ NO ☑ 

5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?  
   YES ☐ NO ☑ 

6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.  
   N/A ☐ YES ☑ NO ☐ 

7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?  
   YES ☑ NO ☐ 

8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:  
   A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?  
      YES ☑ NO ☑ 
   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?  
      YES ☑ NO ☑ 

*EXPLANATION REQUIRED (SEE BELOW)

---

CHANGE/RETENTION RATIONALE SUMMARY

1. ☑ NO H/S ISSUES  
2. ☑ HARDWARE ACCEPTS RISK  
3. ☑ NO SOFTWARE DETECTION  
4. ☑ DETECTION DURING CHECKOUT  
5. ☑ ACCEPTANCE RATIONALE BELOW  
6. ☑ RECOMMENDED CHANGES BELOW

---

EXPLANATION/COMMENTS:

3a. Instrumentation is available for software redesign.
ITEM: NOZZLE EXTENSION, COATED COLUMBIUM (WITH INSULATION BLANKET).

FUNCTION:
TO PROVIDE FOR EXPANSION OF COMBUSTION GASES TO M>1 SUCH THAT THE REQUIRED THRUST IS PRODUCED.

FAILURE MODE: STRUCTURAL FAILURE, (S)

CAUSE(S): HIGH TEMPERATURE IN LOCAL SPOT DUE TO FILM COOLING FAILURE (CONTAMINATED INJECTOR COOLANT HOLES) VIBRATION, SHOCK, WELD OR MATERIAL DEPOL. EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF A THRUSTER IN A GIVEN AXIS. (B) INCREASED GN&C CONTROL AUTHORITY REQUIRED. (C) NO EFFECT. (D) NO EFFECT UNLESS FAILURE PROPAGATES—CRIT1 FOR RTLS ABORT IF THRUSTER IS ISOLATED AT MANIFOLD LEVEL.

CORRECTING ACTION:
ISOLATE THRUSTER AT INLET VALVE OR MANIFOLD AND UTILIZE ALTERNATE IN AFFECTED AXIS.

REMARKS/HAZARDS:
POTENTIAL FOR FAILURE PROPAGATION TO ADJACENT THRUSTERS IF INSULATION BLANKET DOES NOT PRECLUDE GAS/LIQUID ESCAPING. REFERENCE: HAZAIX-0302-01.
SUBSYSTEM : FWD - REACTION CONTROL

ASSEMBLY : THRUSTER PRIMARY

P/N RN : MC467-0028

P/N VENDOR : X30872

QUANTITY : 14

PREPARED BY : Searcy

APPROVED BY : SSM

SUBJECT : NOZZLE EXTENSION

FUNCTION :

TO PROVIDE FOR EXPANSION OF COMBUSTION GASES TO \( \frac{\Delta V}{\Delta t} > 1 \) SUCH THAT THE REQUIRED THRUST IS PRODUCED.

FAILURE MODE : STRUCTURAL FAILURE

(a) LOSS OF A THRUSTER IN A GIVEN AXIS

(b) INCREASED GUIDED CONTROL AUTHORITY REQUIRED

(c) NO EFFECT

(d) NO EFFECT UNLESS FAILURE PROPAGATES - CRITICAL FOR RTLS ABORT IF THRUSTER IS ISOLATED AT MANIFOLD LEVEL

DISPOSITION & RATIONALE

(a) DESIGN

(b) TEST

(c) INSPECTION

(d) FAILURE HISTORY

(a) INTERMETALLIC DIFFUSION LAYER FORMS INTEGRAL BOND TO RESIST SHOCK - COATING PROCESS CONTROLLED. INJECTOR DESIGN INCORPORATES ACOUSTIC CAVITIES WHICH REDUCE POSSIBILITY OF INSTABILITY. DUCTILE PROPERTIES OF C-103 COLUMBIUM PRECLUDES FRAGMENTATION OR CATASTROPHIC MODE OF FAILURE.

(b) VIBRATION TESTS DEMONSTRATE ABILITY OF DISILIYDE COATING TO WITHSTAND 2.0 G SQUARED/HZ RANDOM VIBRATION. TEMP TESTS DEMONSTRATE EXCELLENT DUCTILE/BRITTLE QUALITIES FOR COATED C-103 COLUMBIUM.

(c) TURNAROUND INSPECTION TO INCLUDE VISUAL INSPECTION FOR EVIDENCE OF BURN THROUGH & WHERE ACCESSIBLE, USE OF FIBER-OPTICS TO INSPECT FOR SURFACE FLAWS. SUPPLIER INSPECTION INCLUDES FLOUORESCENT PENETRATE INSPECTION PRIOR TO COATING TO DETECT SURFACE DEFECTS AND X-RAY INSPECTION IS REQUIRED FOR DETECTION OF INTERNAL DEFECTS. AUDIT CONDUCTED 9-2-76 VERIFIED THAT SUPPLIER INSPECTION CONTROLS OF MATEL, IDENTIFICATION OF PARTS, MFG PROCESSES, CORROSION PROTECTION, CONTAMINATION CONTROL AND ENVIRONMENTS. (d) 4 OCCURANCES OF BELL FAILURES CAUSED BY BRITTLE HETEROGENEOUS GRAIN STRUCTURE DUE TO VIBRATION FATIGUE ON APOLLO LM/SM RCS ENGINES.
1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNOUNCE OR TAKE ACTION IN RESPONSE)?
   YES X NO

1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?
   *YES ☑ NO ☐

2. ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?
   YES X *NO ☑

3. DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
   YES ☑ NO ☒

3a. IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?
   *YES ☑ NO ☒

4. AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?
   *YES ☑ NO ☒

5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?
   *YES ☑ NO ☒

6. HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)? NOTE CHANGE TO FMEA CRITICALITY.
   *0 ☐ *1 [X] 2 ☑

7. IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?
   H/A [X] YES ☒ NO ☐

8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:
   A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?
      YES X *NO ☐
   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?
      YES X *NO ☐

*EXPLANATION REQUIRED (SEE BELOW)

CHANGE/RETENTION: RATIONALE SUMMARY
1. ☐ NO H/S ISSUES 3. ☐ NO SOFTWARE DETECTION 5. ☐ ACCEPTANCE RATIONALE BELOW
2. [X] HARDWARE ACCEPTS RISK 4. ☐ DETECTION DURING CHECKOUT 6. ☐ RECOMMENDED CHANGES BELOW

EXPLANATION/COMMENTS:
1. RM uses thrust chamber pressure transducers to sense the low pressure in question and give a "fail.off" in RCS.RM.

3. The GN&C RM program will automatically deselect a failed jet under certain conditions (provided it is not inhibited). See FSSR "10" paragraph 4.1.7.1.6.3 for the conditions.

6. This failure can be tolerated since it is criticality 2.

7. The thrust chamber pressures can be downlinked.
SUBSYSTEM: FWC - REACTION CONTROL
ASSEMBLY: THRUSTER ASSY
P/N R1: MC467-0029
P/N VENDOR: MISSIONS: HFFVFXH FOFM
QUANTITY: 2 PHASE(S): PL LU ODXDO LS
ONE REQ'D PER SIDE NUMBER OF SUCCESS PATHS REMAINING
(DOWN FIRING) AFTER FIRST FAILURE:
FAILURE DETECTABLE IN FLIGHT? YES
THRUSTER CHAMBER PRESSURE V42P-1555A, 1556A
GROUND TURNAROUND? YES
POSITION INDICATION

PREPARED BY: DES J TAGGART
APPROVED BY: DES R DIEHL

ITEM: THRUSTER, VERNIER
(FN 157/15b).
FUNCTION:
TO PROVIDE THRUST FOR LOW LEVEL ACCELERATIONS ASSOCIATED WITH POINTING MANEUVERS AND THREE AXIS ATTITUDE HOLD. THRUSTER FIRES IN +Z DIRECTION FOR +PITCH AND -Z ACCELERATION. INCLUDES INLET VALVE, INJECTOR, THRUST CHAMBER, NOZZLE EXTENSION, HEATER, INSULATION, PRESS/TEMP XSDUCERS.
FAILURE MODE: LOSS OF OUTPUT (F)
INLET VALVES/BLOCKED INJECTOR/STAND-OFF'S.
CAUSE(S):
CONTAMINATION, PIECE PART STRUCTURAL FAILURE, IMPROPER SOLVENT ACTUATION, VIBRATION
EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF VERNIER FUNCTION. (B) NO EFFECT. (C) POTENTIAL WARNING. MISSION TERMINATION. LOSS OF TIGHT DEADBAND ATTITUDE CONTROL. (D) NO EFFECT.
CORRECTING ACTION:
UTILIZE LARGE THRUSTERS FOR ATTITUDE CONTROL IN AFFECTED AXIS (INCREASED PROPELLANT QUANTITY DEPLETION)
REMARKS/HAZARDS:
POTENTIAL HAZARD IF FAILURE OCCURS DURING CRITICAL MANEUVERS - TIME CRITICAL. NO REDUNDANCY IS PROVIDED FOR THIS COMPONENT.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: THRUSTER ASSY
P/N: MC467-0029
P/N VENDOR:

MISSIONS: HF VF X FF OF SM

QUANTITY: 2
ONE REQ'D PER SIDE
(DOWN FIRING)

REDUNDANCY SCREEN: A-N/A B-N/A C-N/A

PREPARED BY: J TAGGART DES R DIEHL REL

APPROVED BY: SSM

ITEM: THRUSTER, VERNIER
(EN 157/158)

FUNCTION:
- TO PROVIDE THRUST FOR LOW LEVEL ACCELERATIONS ASSOCIATED WITH POINTING MANEUVERS AND THREE AXIS ATTITUDE HOLD. THRUST IS APPLIED IN +Z DIRECTION FOR + PITCH AND -Z ACCELERATION. INCLUDES INLET VALVE, INJECTOR, THRUST CHAMBER, NOZZLE EXTENSION, HEATER, INSULATION, PRESS/TEMP XSOUCERS.

FAILURE MODE: LOSS OF OUTPUT
- INLET VALVES/BLOCKED INJECTOR/STAND-OFF'S.

CAUSE(S):
- CONTAMINATION, PIECE PART STRUCTURAL FAILURE, IMPROPER SCLENCID ACTUATION, VIBRATION

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
- (A) LOSS OF VERNIER FUNCTION. (B) NO EFFECT. (C) POTENTIAL EARLY MISSION TERMINATION. LOSS OF TIGHT DEADBAND ATTITUDE CONTROL. (D) NO EFFECT.

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
- (A) VALVE INCORPORATES A 25 MICRON FILTER TO PRECLUDE CONTAMINATION. VALVE HAS BEEN DESIGNED TO PRECLUDE SELF GENERATED CONTAMINATES. SPECIAL EMPHASIS PLACED ON SOLENOID AND WIRING TO PRECLUDE SHORTS. (B) PRE/POST FLIGHT CHECKOUT AND VALVE SIGNATURE TESTS WHEN MODULE REMOVED. VALVE SUBJECTED TO RANDOM VIBRATION AT ANTICIPATED MISSION LEVELS DURING QUAL PROGRAM. LENGTH OF TIME FOR VIBRATION TO EQUAL 100 MISSION LIFE EXPECTANCY. (C) AUDIT CONDUCTED 9-2-76 VERIFIED THAT SUPPLIER INSPECTION CONTROLS RAW MAT'L, IDENTIFICATION OF PARTS, MFG PROCESSES, CORROSION PROTECTION, CONTAMINATION CONTROL, AND ELECTRICAL TERMINATIONS. TURNAROUND INSPECTION INCLUDES MONITORING FUNCTIONAL TEST DURING PRESSURIZATION CYCLE FOR EVIDENCE OF ERRATIC OPERATION. (D) NO FAILURE HISTORY APPLICABLE TO THIS FAILURE MODE.
**SUBSYSTEM**  Fwd Reaction Control  
**FMEA NUMBER**  SD75-SH-0016A  
**ITEM**  Vernier Thruster  
**FAILURE MODE**  Erratic Operation

1. **DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUCIAITE OR TAKE ACTION IN RESPONSE)?**:  
   - **YES**  
   - **NO**  
   *YES*  

1a. **IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?**  
   - **YES**  
   - **NO**  
   - **X**  

2. **ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?**  
   - **YES**  
   - **NO**  
   *YES*  

3. **DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**  
   - **YES**  
   - **NO**  
   *NO*  

3a. **IF NOT, DOES THE CAPABILITY EXIST FOR THE SOFTWARE TO COMPENSATE FOR THIS FAILURE MODE (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?**  
   - **YES**  
   - **NO**  
   - **X**  

4. **AS A RESULT OF THIS FAILURE MODE, CAN THE SOFTWARE OVERSTRESS THE HARDWARE OR INDUCE ANOTHER FAILURE?**  
   - **YES**  
   - **NO**  
   *NO*  

5. **CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?**  
   - **YES**  
   - **NO**  
   *NO*  

6. **HOW MANY OF THESE HARDWARE FAILURES CAN THE SHUTTLE TOLERATE (CONSIDER CREW ACTION AND HARDWARE/SOFTWARE OPERATION)?**  
   - **YES**  
   - **NO**  
   - **X**  

7. **IF CREW ACTION IS REQUIRED TO RESPOND TO THIS FAILURE MODE, ARE CUES PROVIDED TO SIGNAL THE NEED FOR INTERVENTION AND THE REQUIRED CORRECTIVE ACTION?**  
   - **YES**  
   - **NO**  
   *NO*  

8. **IF THE ANSWER TO EITHER 1 OR 3 IS YES:**  
   A. **CAN THE BFS BE ENGAGED AFTER OCCURRENCE?**  
      - **YES**  
      - **NO**  
      *NO*  
   B. **WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?**  
      - **YES**  
      - **NO**  
      *NO*  

*EXPLANATION REQUIRED (SEE BELOW)*

---

**CHANGE/RETENTION RATIONALE SUMMARY**

1. **NO H/S ISSUES**  
2. **X** **HARDWARE ACCEPTS RISK**  
3. **NO SOFTWARE DETECTION**  
4. **DETECTION DURING CHECKOUT**  
5. **ACCEPTANCE RATIONALE BELOW**  
6. **RECOMMENDED CHANGES BELOW**

**EXPLANATION/COMMENTS:**

1. May not be detected unless 3 consecutive low pressures.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 102

SUBSYSTEM: FWL - REACTION CONTROL
ASSEMBLY: THRUSTER ASSY
P/N RI: MC467-0029
P/N VENDOR: MC467-0029
QUANTITY: 2

P/N VENDOR: MC467-0029
MISSION: HF VF X FF OF SM

FAILURE DETECTABLE IN FLIGHT? YES
THRUSTER CHAMBER PRESS. INDICATION V4ZP-1555A
1556A

GROUND TURNAROUND? NO

REFERENCE DOCUMENTS:
MJ070-0061-016
SD72-5H-0153-2
VS70-421CC1

PREPARED BY: DES J. TAGGART
APPROVED BY: DES R. DIEHL

ITEM: THRUSTER, VERNIER
FUNCTION:
- TO PROVIDE THRUST FOR LOW LEVEL ACCELERATIONS ASSOCIATED WITH POINTING MANEUVERS AND THREE AXIS ATTITUDE HOLD. THRUSTER FIRES IN +Z DIRECTION FOR +PITCH AND -Z ACCELERATION. INCLUDES INLET VALVE, INJECTOR, THRUST CHAMBER, NOZZLE EXTENSION, HEATER, INSULATION, PRESS/TEMP XSDUCERS.

FAILURE MODE: ERRATIC OPERATION (F)
- LOW/HIGH THRUST OR INTERMITTENT OPERATION

CAUSE(S):
- CONTAMINATION, IMPROPER SOLENOID ACTUATION.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACE (C) MISSION (D) CREW/VEHICLE:
- (A) LOSS OF VERNIER CONTROL (B) INTERFACE SWITCHING OF POWER AND GNC CONTROL TO LARGE THRUSTERS, (C) POSSIBLE EARLY MISSION TERMINATION BOTH VERNIER THRUSTERS WOULD HAVE TO BE ISOLATED SUCH THAT TIGHT DEADBAND ATTITUDE CONTROL WOULD BE LOST, (D) NONE.

CORRECTING ACTION:
- SHUT DOWN/ISOLATE FAILED THRUSTER AND UTILIZE LARGE THRUSTER IN AFFECTED AXIS

REMARKS/HAZARDS:
- POTENTIAL HAZARD FROM COLLISION. NO REDUNDANCY IS PROVIDED FOR THIS COMPONENT.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: THRUSTER ASSY
P/N: 46467-0029
VENDOR: MISSION: HF VF X FF
P/N: 0029
VENDOR: MISSION: HF VF X FF
QUANTITY: 2
PREPARED BY:
APPROVED BY:
FMEA NO 03-2F - 131310-3 REV: 11/13
CRITICAL ITEMS LIST
ITEM: THRUSTER, VERNIER
FUNCTION:
* TO PROVIDE THRUST FOR LOW LEVEL ACCELERATIONS ASSOCIATED WITH POINTING MANEUVERS AND THREE AXIS ATTITUDE HOLD. THRUSTER FIRES IN +Z DIRECTION FOR +PITCH AND -Z ACCELERATION. INCLUDES INLET VALVE, INJECTOR, THRUST CHAMBER, NOZZLE EXTENSION, HEATER, INSULATION, PRESS/TEMP SENSORS.
FAILURE MODE: ERRATIC OPERATION (F)
* LOW/HIGH THRUST OR INTERMITTENT OPERATION
CAUSE(S):
* CONTAMINATION, IMPROPER SOLENOID ACTUATION.
EFFECT(S):
* (A) LOSS OF VERNIER CONTROL (B) INTERFACE SWITCHING OF POWER AND GN&C CONTROL TO LARGE THRUSTERS. (C) POSSIBLE EARLY MISSION TERMINATION IF BOTH VERNIER THRUSTERS WOULD HAVE TO BE ISOLATED SUCH THAT TIGHT DEADBAND ATTITUDE CONTROL WOULD BE LOST. (D) NONE.
DISPOSITION & RATIONALE
* (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
* (A) VALVE INCORPORATES A 75 MICRON FILTER TO PRECLUDE CONTAMINATION. VALVE HAS BEEN DESIGNED TO PRECLUDE SELF GENERATED CONTAMINATES. SPECIAL EMPHASIS PLACED ON SOLENOID AND WIRING TO PRECLUDE SHORTS. (B) PRE/POST FLIGHT CHECKOUT AND VALVE SIGNATURES TESTS WHEN MODULE REMOVED. VALVE SUBJECT TO RANDOM VIBRATION AT ANTICIPATED MISSION LEVELS DURING QUAL PROGRAM. LENGTH OF TIME FOR VIBRATION TO EQUAL 100 MISSION LIFE EXPECTANCY. (C) AUDIT CONDUCTED 9-2-75 VERIFIED THAT SUPPLIER INSPECTION CONTROLS RAW MATEL. IDENTIFICATION OF PARTS, MFG PROCESSES, CORROSION PROTECTION, CONTAMINATION CONTROL, AND ELECTRICAL TERMINATIONS. TURNAROUND INSPECTION INCLUDES MONITORING FUNCTIONAL TEST DURING PRESSURIZATION CYCLE FOR EVIDENCE OF ERRATIC OPERATION. (D) NO FAILURE HISTORY CONCERNING THIS FAILURE MODE.

PREPARED BY:
APPROVED BY:
FMEA NO 03-2F - 131310-3 REV: 11/13
CRITICAL ITEMS LIST
ITEM: THRUSTER, VERNIER
FUNCTION:
* TO PROVIDE THRUST FOR LOW LEVEL ACCELERATIONS ASSOCIATED WITH POINTING MANEUVERS AND THREE AXIS ATTITUDE HOLD. THRUSTER FIRES IN +Z DIRECTION FOR +PITCH AND -Z ACCELERATION. INCLUDES INLET VALVE, INJECTOR, THRUST CHAMBER, NOZZLE EXTENSION, HEATER, INSULATION, PRESS/TEMP SENSORS.
FAILURE MODE: ERRATIC OPERATION (F)
* LOW/HIGH THRUST OR INTERMITTENT OPERATION
CAUSE(S):
* CONTAMINATION, IMPROPER SOLENOID ACTUATION.
EFFECT(S):
* (A) LOSS OF VERNIER CONTROL (B) INTERFACE SWITCHING OF POWER AND GN&C CONTROL TO LARGE THRUSTERS. (C) POSSIBLE EARLY MISSION TERMINATION IF BOTH VERNIER THRUSTERS WOULD HAVE TO BE ISOLATED SUCH THAT TIGHT DEADBAND ATTITUDE CONTROL WOULD BE LOST. (D) NONE.
DISPOSITION & RATIONALE
* (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
* (A) VALVE INCORPORATES A 75 MICRON FILTER TO PRECLUDE CONTAMINATION. VALVE HAS BEEN DESIGNED TO PRECLUDE SELF GENERATED CONTAMINATES. SPECIAL EMPHASIS PLACED ON SOLENOID AND WIRING TO PRECLUDE SHORTS. (B) PRE/POST FLIGHT CHECKOUT AND VALVE SIGNATURES TESTS WHEN MODULE REMOVED. VALVE SUBJECT TO RANDOM VIBRATION AT ANTICIPATED MISSION LEVELS DURING QUAL PROGRAM. LENGTH OF TIME FOR VIBRATION TO EQUAL 100 MISSION LIFE EXPECTANCY. (C) AUDIT CONDUCTED 9-2-75 VERIFIED THAT SUPPLIER INSPECTION CONTROLS RAW MATEL. IDENTIFICATION OF PARTS, MFG PROCESSES, CORROSION PROTECTION, CONTAMINATION CONTROL, AND ELECTRICAL TERMINATIONS. TURNAROUND INSPECTION INCLUDES MONITORING FUNCTIONAL TEST DURING PRESSURIZATION CYCLE FOR EVIDENCE OF ERRATIC OPERATION. (D) NO FAILURE HISTORY CONCERNING THIS FAILURE MODE.
1. **Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?**
   - Yes [X] No [ ]

1a. If not, does the hardware provide information that the flight software could use to detect the failure?
   - Yes [ ] No [X] *Yes [ ] No [ ]

2. Are the answers to questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?
   - Yes [X] *No [ ]

3. **Does the flight software take action to negate the effects of the failure (either by commanding hardware action or implementing alternate program logic)?**
   - Yes [X] No [ ]

3a. If not, does the capability exist for the software to compensate for this failure mode (either by commanding hardware action or implementing alternate program logic)?
   - Yes [X] No [ ]

4. As a result of this failure mode, can the software overstress the hardware or induce another failure?
   - Yes [X] No [ ]

5. **Can this failure mode, in combination with software logic, adversely affect other functions?**
   - Yes [X] No [ ]

6. How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)? Note change to FMEA criticality.
   - Yes [X] No [X] *1 [ ] 2 [ ]

7. If crew action is required to respond to this failure mode, are cues provided to signal the need for intervention and the required corrective action?
   - N/A [ ] Yes [X] No [ ]

8. If the answer to either 1 or 3 is Yes:
   - A. Can the BFS be engaged after occurrence? Yes [X] No [ ]
   - B. Will BFS tolerate failure without loss of crew/vehicle? Yes [X] No [ ]

*Explanation required (see below!)

**Change/Retention Rationale Summary:**

1. [ ] No H/S Issues
2. [X] Hardware Accepts Risk
3. [ ] No Software Detection
4. [ ] Detection During Checkout
5. [ ] Acceptance Rationale Below
6. [ ] Recommended Changes Below

**Explanation/Comments:**

1. The GN&C RM Program will automatically deselect a failed jet and issue an alert. Detectable in thrust chamber but not in nozzle.
2. [ ]
3. 6. This is a criticality 1 failure and cannot be tolerated.
4. 7. The thrust chamber pressures can be downlinked.
5. 8B. Same as primary.
SUBSYSTEM : FWD - REACTION CONTROL
ASSEMBLY : THRUSTER ASSY
P/N R1 : MC467-0029
P/N VENDOR: MISSIONS: HF VF X FF OF SM
QUANTITY : 2
ONE REQ'D PER SIDE
PHASE(S): PL LO DO DU LS
FAILURE DETECTABLE IN FLIGHT?: YES
MINOR LEAKAGE OR INCipient FAILURE
GROUND TURNAROUND?.............YES
VISUAL EXAMINATION

PREPARED BY: DES J TAGGART
APPROVED BY: DES R DIEHL

ITEM: THRUSTER, VERNIER
FUNCTION:
TO PROVIDE THRUST FOR LOW LEVEL ACCELERATIONS ASSOCIATED WITH POINTING MANEUVERS AND THREE AXIS ATTITUDE HOLD. THRUSTER FIRES IN +Z DIRECTION FOR + PITCH AND -Z ACCELERATION. INCLUDES INLET VALVE, INJECTOR, THRUST CHAMBER, NOZZLE EXTENSION, HEATER, INSULATION, PRESS/TEMP SOURCEs.

FAILURE MODE: OVERHEAT/BURNTHROUGH (F)

CAUSE(S):
MAX PRESSURE SPIKES, SURFACE DEFECTS IN THE PROTECTIVE DISILICIUM COATING FOR CHAMBER WALL AND VIBRATION.

EFFECT(S): (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF VERNIER THRUSTER. (B) POTENTIAL DAMAGE. (C) POTENTIAL EARLY MISSION TERMINATION. (D) POTENTIAL LOSS OF VEHICLE. CRITICAL DAMAGE COULD OCCUR BEFORE FAILURE IS DETECTED.

CORRECTING ACTION:
ISOLATE FAILED THRUSTER AND USE OTHER THRUSTERS.

REMARKS/HAZARDS:
POTENTIAL HAZARD FROM ESCAPING HOT GASES IN THE MODULE AND POTENTIAL PROPAGATION OF FAILURE IF NOT ISOLATED IN A TIMELY MANNER.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: THRUSTER ASSY
P/N RI: MC467-0029
P/N VENDOR:
QUANTITY: 2

PREPARED BY: DES J TAGGART DES
APPROVED BY: NASA

ITEM: THRUSTER, VERNIER
FUNCTION:
TO PROVIDE THRUST FOR LOW LEVEL ACCELERATIONS ASSOCIATED WITH POINTING MANEUVERS AND THREE AXIS ATTITUDE HOLD. THRUSTER FIRES IN +Z DIRECTION FOR + PITCH AND -Z ACCELERATION. INCLUDES INLET VALVE, INJECTOR, THRUST CHAMBER, NOZZLE EXTENSION, HEATER, INSULATION, PRESS/TEMP XSDUCERS.

FAILURE MODE: OVERHEAT/BURNTHROUGH (F)

CAUSE(S):
MAX PRESSURE SPIKES, SURFACE DEFECTS IN THE PROTECTIVE DISILICIDE COATING FOR CHAMBER WALL AND VIBRATION.

EFFECT(S): (A) LOSS OF VERNIER THRUSTER, (B) POTENTIAL DAMAGE, (C) POTENTIAL EARLY MISSION TERMINATION, (D) POTENTIAL LOSS OF VEHICLE. CRITICAL DAMAGE COULD OCCUR BEFORE FAILURE IS DETECTED.

DISPOSITION & RATIONALE: (A) DESIGN, (B) TEST, (C) INSPECTION, (D) FAILURE HISTORY:
(A) INTERMETALIC DIFFUSION LAYER FORMS AN INTEGRAL BOND BETWEEN THE DISILICIDE COATING AND THE PARENT COLUMBIA MATERIAL (C-103) AND TENDS TO RESIST SHOCK LOADING. (B) PRIOR TESTS CONDUCTED ON THE R1-1 THRUSTER HAVE DEMONSTRATED THE ABILITY OF THE DISILICIDE COATING TO WITHSTAND IMPACT LEVELS AND THERMAL STRESSES PRODUCED BY TEMPERATURES IN EXCESS OF 2900 DEGREES F. TORCH TESTS HAVE DEMONSTRATED THE INSENSITIVITY OF THE R512A COATING TO THERMAL SHOCK. (C) AUDIT CONDUCTED 9-2-76 VERIFIED THAT THE SUPPLIER INSPECTION CONTROLS RAW MATERIAL, IDENTIFICATION OF PARTS MFG. PROCESSES, CORROSION PROTECTION, CONTAMINATION CONTROL, AND FLOURESCENT PENETRANT INSPECTION PRIOR TO COATING TO DETECT SURFACE FLAWS AND X-RAY INSPECTION IS REQUIRED FOR DETECTION OF INTERNAL DEFECTS. COATING THICKNESS AND QUALITY IS CONTROLLED BY MPS 525 WHICH WILL REQUIRE CERTIFICATION THAT COATING PROCESS CONFORMS TO THE PROCESS SPECIFICATION, VISUAL INSPECTION, VERIFICATION OF COATING THICKNESS & TEST TO VERIFY COATING INTEGRITY. TURNAROUND INSPECTION TO INCLUDE VISUAL INSPECTION FOR EVIDENCE OF BURN THROUGH AND WHERE ACCESSIBLE, USE OF FIBER OPTICS NDE TO INSPECT FOR SURFACE FLAWS.
(D) NO FLIGHT FAILURE HISTORY.
Meeting Minutes


1. Meeting held at Rockwell International, Downey, 1:00PM to 2:30PM, 9/24/79.

2. Attendees
   - Edward Vonusa NASA X-1470
   - Dave Latham JSC Reliability (Boeing) 527-0323
   - Rudy Kubica RI Propulsion/RCS X-4720
   - Larry Gladu RI System Engineering X-1189
   - Bill Meyers RI System Engineering X-1726
   - Bob Diehl RI Reliability X-2098

3. The following changes were discussed and will be incorporated in the final release of Forward Reaction Control System Hardware/Software Interaction Analysis and will be reflected in next update of Fwd RCS FMEA:

   03-2F-101010-1: Change "SMU" to "SM". Insert "SM Alert" before "blue light."

   03-2F-101013-1: Same as 03-2F-101010-1.

   03-2F-101020-3: Same as 03-2F-101010-1.

   03-2F-101020-4: Same as 03-2F-101010-1.

   03-2F-101030-1: Add "X" in No. Block, question la.

   03-2F-101030-2: Add V42P1116C to Explanation 1. and 2.

   03-2F-101060-1: Show class 3 alarm with blue light and class 2 alarm with red light. Add V421116C. (Explanation 1.)

   03-2F-101060-2: Add "X", No Block, question la.

   03-2F-101060-3: Same as 03-2F-101060-1.

   03-2F-101060-4: Same as 03-2F-101060-1.

   03-2F-101060-5: Same as 03-2F-101060-1.

   03-2F-101070-1: Under 1 & 2 Explanation, add V421113C, 1114C. Change class 2 to 3.

   03-2F-101080-1: Change FMEA to show detectability method.

   03-2F-101090-1: Under 1 & 2 Explanation, change V42P1110C, 1112C to 1113C, 1114C. Change class 2 to 3. Add gross leakage detectability (see 03-2F-101080-1).
03-2F-101095-2: Change "X" from Yes Block to No Block, question 1. Under Explanation, delete 1 & 2 (failure is one leg only - requires failure of both legs to actuate C & W).

03-2F-102106-1: Under 1 Explanation, add gross leakage detectability (see 03-2F-101080-1). Under 7 Explanation and FMEA change add V42P1115C. Change FMEA to show detectability.

03-2F-102108-1: Under 1 Explanation, add gross leakage detectability (see 03-2F-101080-1) Under 7 Explanation add V42P1115C.

03-2F-102120-1: Under 1 Explanation, add oxidizer measurement numbers, and add "failed off thruster will give "failed jet on C & W".

03-2F-102150-1: Same as 03-2F-102120-1 plus retain V42P1312C and delete 1313C and 1314C.

03-2F-102170-1: Under 1 Explanation, add measurements V42X1333X, 1233X. Change class 2 to 3.

03-2F-111110-1: Under 1 Explanation, add V42P1210C, 1212C, 1216C and add to FMEA detectability. Add X in FMEA change recommended block.

03-2F-111110-2: Same as 03-2F-111110-1.

03-2F-111110-3: Under 1 Explanation, add gross leakage detectability (see 03-2F-101080-1).

03-2F-111110-4: Change X from No Block to Yes block for question 1. Under Explanation, delete 1st paragraph and 1. (White Sands Test on vernier showed complete loss chamber pressure which is detectable. Similar gas bubbles in propellant tests are planned for primary thrusters).

03-2F-121308-1: Under 1 Explanation, the class 3 alarm is doubtful. Check and verify findings with Bill Meyers RI Systems Engineering. Also add gross leakage detectability (see 03-2F-101080-1).

03-2F-121311-1: Change Failure Mode to agree with failure mode in FMEA.

03-2F-121312-1: Under 1 Explanation, add "If failure is upstream of throat it will be detected by PC; if failure is downstream of throat it will not be detected."

03-2F-121313-1: Change X from Yes Block to No Block, question 1. Delete 1. under Explanation (failure is downstream of throat and will not be detected by PC).

03-2F-131310-3: Change X from Yes Block to No Block, question 1. Add X to FMEA change recommended block. Under 1. Explanation, delete entire sentence (the pressure transducers are snubbed by an orifice and will not detect the erratic operation). Change FMEA to indicate no detectability.
Approved by:

Larry Gladw, RI
System Engineering

Dave Latham
JSC Reliability (Boeing)

Edward Vonusa
NASA QARSO