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 11/4/80  
Chief, Reliability Division
VERIFICATION PLAN
- VERIFICATION ROADMAP
- REQUIREMENTS VERIFICATION

IMPLEMENTING DOCUMENTATION
- TRD
- TRSD
- TCP

ANALYSIS

TEST

VCN

FLIGHT READINESS STATEMENT

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.

SEAM TEAMS
- SYSTEM ENGINEERING
- RELIABILITY
- DESIGN

FMEA/CFI
HARDWARE/SOFTWARE INTERACTION ANALYSIS
PRACA
CERTIFICATION

SYSTEM ENGINEERING
FSSR
CPDS
INT, SCHEMATIC
OMRSD/TRSD

VERIFICATION PLANNING AND MANAGEMENT
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.
## HARDWARE/SOFTWARE ANALYSIS CHECKLIST

<table>
<thead>
<tr>
<th>Item</th>
<th>Failure Mode</th>
<th>FMEA Number</th>
<th>Subsystem</th>
<th>Hardware/Software Analysis Checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Does the flight software detect this failure mode (i.e., automatically announce or take action in response)?</td>
<td>YES □ NO □</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>*YES □ 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 □ *NO □</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 □ NO □</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 □ NO □</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>As a result of this failure mode, can the software over-stress the hardware or induce another failure?</td>
<td>YES □ NO □</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 □ NO □</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 □ 1 □ 2 □</td>
<td></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 □ YES □ 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>
</tr>
<tr>
<td></td>
<td>A. Can the BFS be engaged after occurrence?</td>
<td>YES □ *NO □</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>B. Will BFS tolerate failure without loss of crew/vehicle?</td>
<td>YES □ *NO □</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Explanation required (see below)*

### CHANGE/RETENTION RATIONALE SUMMARY

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>□ FMEA Change Recommended</td>
<td></td>
<td></td>
<td></td>
<td></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 announciating 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
## HARDWARE/SOFTWARE ANALYSIS SUMMARY

<table>
<thead>
<tr>
<th>SUBSYSTEM</th>
<th>FMEA</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>SUBSYSTEM</th>
<th>Forward Reaction Control</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>ANALYSIS RESULT</th>
<th>ITEM/Failure Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>HARDWARE ACCEPTS RISK</td>
<td>Helium Storage Tank - Rupture (03-2F-101010-1)</td>
</tr>
<tr>
<td></td>
<td>Helium Feedline - External Leakage (03-2F-101013-1)</td>
</tr>
<tr>
<td></td>
<td>Quick Fill Disconnect, He - Fails Open, Cap Leaks (03-2F-101070-1)</td>
</tr>
<tr>
<td></td>
<td>Test Quick Disconnect, Propellant - Ext. Leakage/Flight (03-2F-101090-1)</td>
</tr>
<tr>
<td></td>
<td>Propellant Line Flex Assy. - External Leakage (03-2F-102106-1)</td>
</tr>
<tr>
<td></td>
<td>Feedline and Fittings - External Leakage (03-2F-102108-1)</td>
</tr>
<tr>
<td></td>
<td>AC Motor Operated Valve (Tank) - Fails Closed (03-2F-102120-1)</td>
</tr>
<tr>
<td></td>
<td>Quick Disconnect - External Leakage (03-2F-102150-1)</td>
</tr>
<tr>
<td></td>
<td>DC Solenoid Operated Valve - Fails Closed - Premature Operation (03-2F-102170-1)</td>
</tr>
<tr>
<td></td>
<td>Tank Assembly and Propellant Acquisition Device - Small Crack - External Leakage (03-2F-111110-2)</td>
</tr>
<tr>
<td></td>
<td>Tank Assembly and Propellant Acquisition Device - Restricted Flow (03-2F-111110-3)</td>
</tr>
<tr>
<td></td>
<td>Tank Assembly and Propellant Acquisition Device - Loss of Gas in Propellant Acquisition Device (03-2F-111110-4)</td>
</tr>
<tr>
<td></td>
<td>Flex Line and Fittings - External Leakage (03-2F-121308-1)</td>
</tr>
<tr>
<td></td>
<td>Thrust Chamber - Burn Through (03-2F-121312-1)</td>
</tr>
<tr>
<td></td>
<td>Nozzle Extension - Burn-Through (03-2F-121313-1)</td>
</tr>
<tr>
<td></td>
<td>Vernier Thruster - Erratic Operation (03-2F-131310-3)</td>
</tr>
<tr>
<td></td>
<td>Vernier Thruster - Burn-Through (03-2F-131310-4)</td>
</tr>
<tr>
<td></td>
<td>Helium Pressure Regulator - Fails Closed (03-2F-101030-2)</td>
</tr>
<tr>
<td></td>
<td>Tank Assembly and Propellant Acquisition Device - Large Rupture (03-2F-111110-1)</td>
</tr>
<tr>
<td></td>
<td>Purge Quick Disconnect, Propellant - External Leakage During Flight (03-2F-101080-1)</td>
</tr>
<tr>
<td></td>
<td>Helium Quad Check Valve - Fails Closed (03-2F-101095-2)</td>
</tr>
<tr>
<td></td>
<td>Vernier Thruster - Loss of Output (03-2F-131310-1)</td>
</tr>
<tr>
<td>ANALYSIS RESULT</td>
<td>ITEM/Failure Mode</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>NO HARDWARE/SOFTWARE ISSUES</td>
<td>D.C. Solenoid Valve - Fails to Close (03-2F-101020-3)</td>
</tr>
<tr>
<td></td>
<td>D.C. Solenoid Valve - Fails Closed (03-2F-101020-4)</td>
</tr>
<tr>
<td></td>
<td>Helium Pressure Regulator - Fails Open (03-2F-101030-1)</td>
</tr>
<tr>
<td></td>
<td>Relief Valve - External Leakage Overboard (03-2F-101060-1)</td>
</tr>
<tr>
<td></td>
<td>Relief Valve - Burst Disc Ruptures (03-2F-101060-2)</td>
</tr>
<tr>
<td></td>
<td>Relief Valve - Fails to Burst (03-2F-101060-3)</td>
</tr>
<tr>
<td></td>
<td>Relief Valve - Opens Low (03-2F-101060-4)</td>
</tr>
<tr>
<td></td>
<td>Relief Valve - Fails to Open (03-2F-101060-5)</td>
</tr>
<tr>
<td></td>
<td>Helium Quad Check Valve - Fails Open (03-2F-101095-1)</td>
</tr>
<tr>
<td></td>
<td>Injector Plate - Mixture (03-2F-121311-1)</td>
</tr>
<tr>
<td>ANALYSIS RESULT</td>
<td>ITEM/Failure Mode</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<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

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 [ ]

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

*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. GAX will give a class 2 alert upon sensing an out-of-tolerance condition. ($\leq$500 psi)
   Gross leak detection will give a class 2 alert.

8. Backup flight system same as primary.

---

12
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 1C2

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: MC282-0082-0031/-0032
P/N VENDOR: ELID-999040
QUANTITY: 2

ASSEMBLY: PRESSURIZATION ABORT: CRIT. FUNC: 1
CRIT. HW: 1
MISSIONS: HF, FF, UF, SN
PHASE(S): PL, LC, OU, DU, X, LS

RECIPIENT: BLD-9990A
MISSIONS: HF, FF, UF, SN

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

ITEM: TANK
HELIUM STORAGE, FILAMENT WOUND.

FUNCTION:
TO STORE HELIUM AT A MAX WORKING PRESSURE OF 4000 PSI FOR PRESSURIZATION OF THE FWD RCS MODULE PROPPELLANT SUPPLY SYSTEM. TANK CONSISTS OF A DOUBLE MELT TIT LINER WITH DUPONT 49 FIBER 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) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF PRESSURIZATION TO FUEL OR OXIDIZER. (6) 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 IYXX-0302-02.

ORIGINAL PAGE IS OF POOR QUALITY
SUBSYSTEM: FWD - REACTION CONTROL  FMEA NO 03-2F-10101-0 REV: 11/09/72

ASSEMBLY: PRESSURIZATION  ABORT: CRIT. FUNC: 1

P/N REV: 4C202-0082-0031/-0032  CRIT. HDW: 1

P/N VENDOR: BLD-399040  MISSIONS: HFVF X FF OF SM

QUANTITY: 2  PHASE(S): PL LO DO X DO LS

ONE REQ'D PER EACH  PROPELLANT TANK

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

PREPARED BY:  APPOVED BY:  J TAGGART  SSM

DES:  R DIEHL  REL:

ITEM: TANK  HE LIUM STORAGE, FILAMENT WOUND.

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 FIBER AND EPOXY RESIN BONDING 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) SUBSYSTEM (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.

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY:
- (A) FILAMENT WOUND TANKS ARE DESIGNED TO LEAK BEFORE RUPTURE WHICH LIMITS FAILURE PROPAGATION DUE TO SCHRAMPEL. 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 (1.1X WORKING PRESSURE) DURING ACCEPTANCE TESTING. QUAL TESTS INCLUDE 1000 PRESSURE CYCLES EQUAL TO 4 TIMES LIFE REQUIREMENT, 90 DAY CREEP TEST AT MAX WORKING PRESSURE PLUS RANDOM VIBRATION AT ANTICIPATED MISSION LEVELS FOR 48 HR IN EACH AXIS. (C) IN PROCESS INSPECTION INCLUDES RADIOGRAPHIC 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.
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 ☑️ 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 ☐

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

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.

2. Backup flight system same as primary.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION HELIUM - ABORT:
P/N R1: VC70-421701 CRIT. FUNC: 1
P/N VENDOR: MISSIONS: HF VF X FF CF SM CRIT. FuN: 1
QUANTITY: 2 PHASE(S): PL X LG X GO X DO X LS X
ONE SET PER PROPELLANT NUMBER OF SUCCESS PATHS REMAINING
AFTER FIRST FAILURE:
REDUNDANCY SCREEN: A-N/A B-N/A C-N/A
FAILURE DETECTABLE IN FLIGHT?: YES TIME TO EFFECT:
HELIXM TANK PRESSURE DROP AT OFF-NOMINAL RATE: IMMEDIATE
V42P-1110C; 1112C; 1113C; 1114C REFERENCE DOCUMENTS:
GROUND TURNAROUND?...........YES MJ070-0001-01b
SAME AS FLIGHT INSTRUMENTATION 5D72-5h-0103-2
VS70-421001

PREPARED BY: DES A SIEGELIN
APPROVED BY: REL R DIEHL

ITEM: HELIUM FEED LINE AND
FLUID FITTINGS.
FUNCTION:
TO PROVIDE FEED LINE FROM HELIUM TANKS TO HELIUM
REGULATION/PRESSURATION SYSTEM AND TO PROPELLANT
TANKS.
FAILURE MODE: EXTERNAL LEAKAGE . (S)
CAUSE(S): MECHANICAL SHOCK, VIBRATION/FATIGUE, IMPROPER INSTALLATION (WELL),
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
SCALDING 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.
CORRECTING ACTION:
INITIATE ABORT. CHECK VALVES MAINTAIN PROPELLANT TANK RESIDUAL GAS
PRESSURE TO ALLOW POTENTIAL FLUID DRAIN MODE UTILIZATION.
REMARKS/HAZARDS:
NO REDUNDANCY PROVIDED FOR LINES. IF LEAK RATE IS EXCESSIVE PRESSURE
BUILD-UP IN MODULE MAY RESULT IN HAZARD. SEE HAZARD IYXX-0302-02.
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM: FWO - REACTION CONTROL
ASSEMBLY: PRESSURIZATION HELIUM -
P/N/R: 070-421701
P/N: VQ0-421
QUANTITY: 2

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

ASSEMBLY: PRESSURIZATION HELIUM - ABCRT:
CRIT. FUNC: I
CRIT. HDM: I

VENDOR: MISSIONS: HF VF X FF OF SM

QUANTITY: 2

ONE SET PER PROPELLANT

PREPARED BY:
APPROVED BY:
APPROVED BY: (NASA):
DES: A SIEGELIN
DES: R DIEHL
REL: C BELL

ITEM: HELIUM FEED LINE AND FLUID FITTINGS.

FUNCTION:
TO PROVIDE FEED LINE FROM HELIUM TANKS TO HELIUM REGULATION/PRESSURATION 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 SUBJECT TO 1.25 PROOF TEST. (C) IN PROCESS INSPECTION INCLUDES NOT 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 REQUIREMENTS. HARDWARE INSPECTION IN ACCORDANCE WITH PLANNING REQUIREMENTS APPROVED BY NASA. (D) MINOR FAILURE HISTORY-CORROSION AND FAB PROBLEMS REPORTED DURING APOLLO PROGRAM AND CORRECTED.
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 3. ☐ NO SOFTWARE DETECTION 5. ☑ ACCEPTANCE RATIONALE BELOW
2. ☐ HARDWARE ACCEPTS RISK 4. ☐ DETECTION DURING CHECKOUT 6. ☑ RECOMMENDED CHANGES BELOW

In-Flight Detectability
X 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: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: MC284-0419-0011/-0C12
P/N VENDOR: Y3835
QUANTITY: 14

MISSIONS: HF VF X HF CF SM
PHASE(S): PL X LD X DO X DO X LS

REDUNDANCY SCREEN: A-PASS E-PASS C-PASS

FAILURES DETECTABLE IN FLIGHT? YES
HELIUM TANK PRESS: V42P 1110, 1112, 1113, 1114
AND PRESS LINE: V42P1115, 1116 AND POSITION IND.
GROUNDP TURNAROUND?..............YES
SAME AS FLIGHT INSTR.

PREPARED BY: R BURKHART
APPROVED BY: R DIEHL

ITEM: VALVE, D.C. SOLENOID
OPERATED, HIGH PRESSURE, HE (2600-4000 PSIA) SOLENOID ACTUATED, 1/2" 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) 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 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 □ |
| **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. | *0 □ | *1 □ | 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 □ | *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. Switch scan will detect failure in OPS-2 only and only on demand.  
   May not be used on STS-1.
SUBSYSTEM: FW3 - REACTION CONTROL  
ASSEMBLY: PRESSURIZATION  
P/N: SI: MC284-0419-0011/0012  
P/N VENDOR: 73E35  
QUANTITY: 4  
: TWO REQ'D PER PRESSURANT  
: FEED ASSEMBLY  
MISSIONS: HF, WF, X, RF, X, FF, OF, SM  
PHASE(S): PL, LG, X, FG, X, DU, X, LS  
NUMBER OF SUCCESS PATHS REMAINING: 1  
REMARKS/HAZARDS:  
POTENTIAL HAZARD IN ABORT SITUATION. SEE CONSOLIDATED CONTROLS FMEA NUMBER 73E35 FMEA 1.

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

ITEM: VALVE, D.C. SOLENOID C HELIUM - PRESSURIZATION SYSTEM)  
OPERATED, HIGH PRESSURE HE (3600-4000 PSIA) SOLENOID ACTUATED, 31-STAPLE, 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): UN: (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICL:  
(A) LOSS OF REDUNDANT PRESSURIZATION PATH. (B, D) 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.

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

SUBSYSTEM: FWO - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N R I: MC284-0419-0011/0012
P/N VENDOR: 73835
QUANTITY: 2

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

HOW:
P/N: VENDOR: 73835
QUANTITY: 4

PREPARED BY: R. BURKHART
APPROVE APPROVED BY: (NASA):
REL: R. DIEHL

ITEM: VALVE, D.C. SOLENOID
OPERATED, HIGH PRESSURE. HÉ (3600-4000 PSIA) SOLENOID ACTUATED, BISTABLE, (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): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
- (A) LOSS OF REDUNDANT PRESSURIZATION PATH. (B, D) NO EFFECT. (C) ABORT DECISION 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.
<table>
<thead>
<tr>
<th>Item</th>
<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>FMEA Number</td>
<td>03-2F-101030-1</td>
<td></td>
</tr>
<tr>
<td>Failure Mode</td>
<td>Fails Open</td>
<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. **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 Controlling 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 Controlling 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

---

**Explanation/Comments:**

1. Detection of this failure mode is not desired as these are redundant series regulators.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: MC284-0418
P/N VENDOR: 743390C1
QUANTITY: 4

FAILURE DETECTABLE IN FLIGHT? N/A
STANDBY UNIT

GROUND TURNAROUND? YES
GROUND CHECKOUT TEST PORTS

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

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

FUNCTION:
TO REGULATE STORED HELIUM PRESSURE FROM 4300 PSIG MAX TOULLAGE
PRESSURE OF 245 (+ OR -3) PSIG FOR PURPOSE OF PROPELLANT FUEL 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,
SHELLS, 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.
SUBSYSTEM  Fwd Reaction Control  FMEA NUMBER  SD75-SH-0016A
ITEM  Helium Pressure Regulator  FAILURE MODE  Fails Closed

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)?  
   *NO ☐ *YES ☑ 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  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.

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.
6. Upon regulator failure the redundant parallel "leg" can be utilized.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORDER 102

SUBSYSTEM :FWO - REACTION CONTROL
ASSEMBLY :PRESSURIZATION
P/N R1 :MC284-0418
P/N VENDOR: 74335001
QUANTITY :4

FAIL. DETECTABLE IN FLIGHT: NA
STANDBY REDUNDANCY

GROUND TURNAROUND?.............YES
GROUND CHECKOUT TEST PORTS

PREPARED BY: DES J. TAGGART REL R DIEHL
APPROVED BY: DES 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 PSIG MAX TO ULLAGE PRESSURE OF 245 (+ OR -3) PSIG FOR PURPOSE OF PROPELLANT FEED TO THRUSTERS. TWO PARALLEL PATHS WITH TWO SERIES REGS ARE PROVIDED FOR EACH PROPELLANT TANK.

FAIL. MODE: Fails closed (F)

(LOW PRESSURE)

CAUSE(S): CONTAMINATION (PARTIAL BLOCKAGE OF PILOT SCREEN) FROZEN MOISTURE PIECE

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF ONE REGULATOR PATH. (B,C) POTENTIAL ABORT BECAUSE UNL RECOVERY FAILURE MAY CAUSE LOSS OF PRESSURIZATION AND SUBSEQUENT VEHICLE LOSS. (D) NONE. (E) FUNCTIONAL CRITICALITY EFFECTS - IF FAILURE OCCUR BEFORE 1ST SEPARATION, LOSS OF HELIUM WOULD PREVENT 1ST 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:
POSSIBLE ABORT BECAUSE ONE ADDITIONAL FAILURE (CLOSED) MAY CAUSE LOSS OF PRESSURIZATION AND SUBSEQUENT VEHICLE LOSS (REQUIRES 2ND OR ULTRA "FAIL." DEPENDENT ON MISSION PHASE. SEE FAIRCHILD FMEA'S RK 74335-1E.
SUBSYSTEM : FWD - REACTION CONTROL

ASSEMBLY : PRESSURIZATION

P/N RI : MC284-0418

P/N VENDOR : 74339001

MISSIONS : HF VF FF TF SM

QUANTITY : 4

PREPARED BY: J. TAGGART

REL : R DIEHL

P/N : C284-0418

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 REGS ARE PROVIDED FOR EACH PROPELLANT TANK.

FAILURE MODE: FAILS CLOSED (F)

(LOW PRESSURE)

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 28 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) TURNTAROUND 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.
SUBSYSTEM  Fwd. Reaction Control
ITEM  Manual Valve

HARDWARE/SOFTWARE ANALYSIS CHECKLIST 03-2F-101050-I
FMEA NUMBER  SD75-SH-0016A
FAILURE MODE  Fails Closed or Open

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 ☐

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

EXPLANATIONS/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 - ORBITER 102

SUBSYSTEM : FWD - REACTION CONTROL
ASSEMBLY : PRESSURIZATION
P/N: MC284-0460-0281/0402
P/N VENDOR: 5760015, 5760016
QUANTITY : 2
ONE REQ'D PER TANK

MISSIONS: MF VF XF DF OF SM
PHASE(S): PL LD GO DG LS
NUMBER OF SUCCESS PATHS REMAINING

AFTER FIRST FAILURE:

REDUNDANCY SCREEN: A-PASS C-PASS

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

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

PREPARED BY:
DES R. GONZALEZ
REL R. DIEHL

APPROVED BY:
DES
REL

ITEM: VALVE, MANUAL-OPERATED
TWO POSITION SELECTOR VALVE (WITH STRUCTURAL INTERLOCK) (MV 101/102)
FUNCTION:
TO PROVIDE ISOLATION OF PROPPELLANT 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-SM-0103-2
VS70-42102
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 [ ]

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 [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 [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 3. [ ] NO SOFTWARE DETECTION 5. [ ] ACCEPTANCE RATIONALE BELOW
2. [x] HARDWARE ACCEPTS RISK 4. [ ] DETECTION DURING CHECKOUT 6. [ ] RECOMMENDED CHANGES BELOW

---

**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  FMEA NO 03-2F-101G5C-2  REV:C1/64/7.  
ASSEMBLY: PRESSURIZATION  ASORT: CRIT. FUNC:  
P/N: MG284-0480-0001/-0002  CRIT: Fwd: 3  
P/N VENDOR: 5760015, 5760016  MISSIONS: HF VF X FF OF SM  
QUANTITY: 2  PHASE(S): PL LG X CC X CC X LS  
ONE REQ'D PER TANK  NUMBER OF SUCCESS PATHS REMAINING  
AFTER FIRST FAILURE: 0  
REDUNDANCY SCREEN: A-PAS B-N/A C-PAS:  
FAILURE DETECTABLE IN FLIGHT?: YES  TIME TO EFFECT: 3  
PROPELLANT TANK PRESSURE V42P-1210,1115,1115,1310 SECONDS TO MINUTES  
GROUND TURNAROUND?............YES  REFERENCE DOCUMENTS: MJ070-C001-18  
SAME AS FLIGHT  SB72-SH-0102-2  V570-421061  

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

ITEM: VALVE, MANUAL-OPERATED.  
FUNCTION: TWO POSITION SELECTOR VALVE (WITH STRUCTURAL INTERLOCK) XV 101/102.  
TO PROVIDE ISOLATION OF PROPELLANT TANK(S) FROM PRESSURE CYCLES WHILE  
PERFORMING GROUND C/O AND/OR SERVICING OF PRESSURIZATION SYSTEM.  
FAILURE MODE: EXCESSIVE INTERNAL ( ).  
LEAKAGE.  
CAUSE(S): SEVERE MECHANICAL SHOCK OR VIBRATION CAUSING DETENT MOVEMENT ON A  
DEFICIENT VALVE LOS OF INTERLOCK BY FRACTURE OF UPIVE FINGER OR  
ROCKER, CORROSION, CONTAMINATION, IMPROPER USE.  
EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:  
(LA,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

<table>
<thead>
<tr>
<th>SUBSYSTEM</th>
<th>FMEA NUMBER</th>
<th>ITEM</th>
<th>FAILURE MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fwd Reaction Control</td>
<td>SD75-SH-0016A</td>
<td>Relief Valve</td>
<td>External Leakage Overboard</td>
</tr>
</tbody>
</table>

#### 1.
**DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNOUNCE 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. Leakage of helium will cause a class 2 alarm.

Gross leak detection should occur first.
SUBSYSTEM: FWI - REACTION CONTROL
ASSMFLY: PRESSURIZATION
P/N: MC284-0421-0001/0002
P/N VENDOR: 5760009-101, 5760010-102
QUANTITY: 2
ONE REQ'D PER TANK

ABORT: CRIT. FUNC:
CRIT. Func:

MISSIONS: HF VF X FF OF SM

PHASE(S): PL LG X OO X GO X LS

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

FAILURE DETECTABLE IN FLIGHT?: YES
PRESSURE DECAY IN PRESS- SYSTEM VS2P-1115C AND HOURS
1116C (TANK ULLAGE)

GROUND TURNAROUND? YES
TEST PORT FOR GROUND CHECKOUT AND BACK CHECK

PREPARED BY: R GONZALEZ
APPROVED BY: R DIEHL

ITEM: VALVE, PRESS. RELIEF -
CRCKNG PRESS 315 PSIG, FULL OPEN 340 PSIG, RESEAT 31C 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: EXTERNAL LEAK

CAUSE(S):
Galvanic corrosion, Improper Installation/Handling, Fatigue or Structural Failure.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (C) 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.
HARDWARE/SOFTWARE ANALYSIS CHECKLIST

SUBSYSTEM Fwd. Reaction Control  
ITEM Relief Valve  
FAILURE MODE Burst Disc Ruptures

1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNOUNCE 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  3. [ ] NO SOFTWARE DETECTION  5. [ ] ACCEPTANCE RATIONALE BELOW
2. [x] HARDWARE ACCEPTS RISK  4. [ ] DETECTION DURING CHECKOUT  6. [x] RECOMMENDED CHANGES BELOW

In-Flight Detectability

[X] FMEA CHANGE RECOMMENDED

EXPLANATION/COMMENTS:

1. May see discrete drop in RCS quantity. V42P1115C, 1116C will give class 2 caution and warning alarm.
SUBSYSTEM: FWD - REACTION CONTROL
ASSMVL: PRESSURIZATION
P/N RI: MC284-0421-0001/-0002
P/N VENDOR: 5760109-101, 5760010-102
QUANTITY: 2

FUNCTION: RELIEF VALVE PROVIDED TO PREVENT RISE OF TANK AND LINE PRESSURES TO LEVELS WHICH COULD BE DETRIMENTAL TO SUBSYSTEM.
FAILURE MODE: FAILS OPEN
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,3) 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.

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

ITEM: VALVE, PRESS. RELIEF - CRCKNG PRESS 315 PSIG, FULL OPEN 346 PSIG, RESEAT 31C 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 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,3) 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

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. <strong>DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. <strong>ARE THE ANSWERS TO QUESTIONS 1 AND 2 CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?</strong></td>
<td></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></td>
<td></td>
</tr>
<tr>
<td>5. <strong>CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?</strong></td>
<td></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)? NOTE CHANGE TO FMEA CRITICALITY.</strong></td>
<td></td>
<td></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></td>
<td></td>
</tr>
</tbody>
</table>

**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: PRESSURIZATION

P/N/RI: MC284-0421-0301/-002

P/N VENDOR: 5760009-101, 5760010-102

QUANTITY: 2

ONE REQ'D PER TANK

FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 102

FMEA NO 03-2F - 101050 - 2 REV: 01/04/76

ABORT: CRIT. FUNC: CRIT.

MISSION: HF VF X FF OF SH

P/N: MC284-0421-0301/-002

P/N VENDOR: 5760009-101, 5760010-102

MISSION: HF VF X FF OF SH

QUANTITY: 2

ONE REQ'D PER TANK

FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 102

N/A

NECESSITY: N/A

MISSION: HF VF X FF OF SH

PHASE(S): PL LO X DU X DU X LS

NO: N/A

TIME TO EFFECT:

PRESSURE RISE IN HELIUM SYSTEM V42P-1115C AND SECONDS

PRESSURIZATION ABORT:

CIT. FUNC:

MISSIONS: HF VF X FF OF SH

REPRESSURE RISE IN HELIUM SYSTEM V42P-1115C AND SECONDS

GROUND TURNAROUND?: YES

TURNAROUND TEST PORT PROVIDED

FAILURE DETECTABLE IN FLIGHT?: YES

PRESSURE RISE IN HELIUM SYSTEM V42P-1115C AND SECONDS

GROUND TURNAROUND?: YES

TURNAROUND TEST PORT PROVIDED

PREPARED BY: DES R GONZALEZ

APPROVED BY: DES R DIEHL

ITEM: VALVE, PRESS. RELIEF -

CRACKING PRESS 315 PSIG, FULL OPEN 346 PSIG, RESEAT 316 PSIG (KV 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 BURST

OK BURSTS AT A HIGHER THAN NOMINAL PRESSURE.

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.

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.

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

**SUBSYSTEM** Fwd Reaction Control  
**FMEA NUMBER** 03-2F-101060-4  
**ITEM** Relief Valve  
**FAILURE MODE** Opens Low  

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>YES</th>
<th>NO</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>YES</td>
<td>NO</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>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></td>
<td>YES</td>
<td>*NO</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></td>
<td>YES</td>
<td>NO</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></td>
<td></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></td>
<td></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></td>
<td></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></td>
<td></td>
<td>*O</td>
<td>*1</td>
<td>2X</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>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>YES</td>
<td>*NO</td>
<td></td>
</tr>
<tr>
<td>A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?</td>
<td></td>
<td></td>
<td>YES</td>
<td>*NO</td>
<td></td>
</tr>
<tr>
<td>B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?</td>
<td></td>
<td></td>
<td>YES</td>
<td>*NO</td>
<td></td>
</tr>
</tbody>
</table>

*EXPLANATION REQUIRED (SEE BELOW)*

**CHANGE/RETIEN THEY 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-G001-G002
P/N VENDOR: 57600C09-101, 57600C09-102
QUANTITY: 2
ONE REQ'D PER TANK

ABORT: CRIT.
MISSIONS: HF, VF, FF, OF, SM
PHASE(S): PL, LU, CO, DO, X, LS

AFTER FIRST FAILURE: NUMBER OF SUCCESS PATHS REMAINING
REduNDANCY 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:
DES
REL

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 DETRIMENTAL TO SUBSYSTEM.

FAILURE MODE: PREMATURE/ERRATIC OPERATION (F)
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) CREW/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

39
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

EXPLANATION/COMMENTS:

1. Over pressurization will cause a class 2 alarm, V42P1115C, 1116C.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: MC284-C421-0661-0002
P/N VENDOR: 5760009-101, 5760010-102
QUANTITY: 2

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

ITEM: VALVE, PRESSURE RELIEF -
CRACKING PRESS 315 PSIG, FULL OPEN 340 PSIG, RESEAT 310 PSIG (KV 1C1/102).

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)

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) NONE, (C) POTENTIAL MISSION LOSS

ABORT DECISION: IF EARLY IN MISSION WOULD REQUIRE 2 PRIOR FAILURES.

CORRECTING ACTION:
FIRE ALL THRUSTERS NON-PROPELSIVELY.

REMARKS/HAZARDS:

POTENTIAL TANK RUPTURE ON 3RD ORDER FAILURE NO OTHER RELIEF PATH FOR SYSTEM.

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

**SUBSYSTEM** Fwd Reaction Control  
**FMEA NUMBER** SD75-SH-0016A  
**ITEM** Fill Quick Disconnect, Helium  
**FAILURE MODE** Fails Open, Cap Leaks

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th><em>Reason</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the flight software detect this failure mode (i.e., automatically</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. 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>0</td>
<td>1</td>
<td>2</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:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Can the BFS be engaged after occurrence?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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. ☑ 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% A)

6. Capped quick disconnect provides one redundant success path.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N RI: MG276-0C17-0402/0403
P/N VENDOR: 75372006-0402/0403
QUANTITY: 2

FUNCTION: PROVIDES HELIUM TANK FILL POINT FOR GROUND OPERATIONS AND LOADING SERVICING.
FAILURE MODE: FAILS OPEN, CAP (S)
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.
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM : FWD - REACTION CONTROL  FMEA NO 03-2F -101070-1  REV:12/08/78
ASSEMBLY : PRESSURIZATION  ABORT:  CRIT. FUNC: 1
P/N R#: MC76-0C17-0402/0403  CRIT. HDW: 1
P/N VENDOR: 75372000-0402/0403  MISSIONS: HF VF X FF OF SM
QUANTITY: 2  PHASE(S): PL X LO X DD X DD X LS X
ONE REQ'D PER TANK

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

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

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

44  1077  SD75-SH-0003
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
2. ☐ Hardware accepts risk
3. ☐ No software detection
4. ☐ Detection during checkout
5. ☐ Acceptance rationale below
6. ☐ Recommended changes below

---

**EXPLANATION/COMMENTS:**

1. Out of Scope. Ground operations only.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - Oracite 1O2

SUBSYSTEM : FWO - REACTION CONTROL
ASSEMBLY : PRESURIZATION
P/N RI : MC276-0017-0402/0403
P/N VENDOR : 75372000-0402/0403
QUANTITY : 2

MISSIONS: HF VF X FF LF SM
PHASE(S): PL X LU 00 0U LS
NUMBER OF SUCCESS PATHS REMAINING
ONE REQ'D PER TANK
AFTER FIRST FAILURE: 0
REDUNDANCY SCREEN: A-N/A B-N/A C-N/A

FAILURE DETECTABLE IN FLIGHT? N/A

GND TURNAROUND? YES
GSE FILL RATE AND HELIUM PRESSURE

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

TIME TO EFFECT: IMMEDIATE
REFERENCE DOCUMENTS:
MJ07C-0001-01E
SD72-SH-0105-2
VS70-421001

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.

FAILURES MODE: RESTRICTED FLOW - (F)
FAILS 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.
SUBSYSTEM  Fwd. Reaction Control

ITEM  Purge Quick Disconnect, Propellant

FAILURE MODE  External Leakage During Flight

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

[ ] FMEA CHANGE RECOMMENDED

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.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - UASITER 1C2

SUBSYSTEM : FWD - REACTION CONTROL
ASSEMBLY : PRESSURIZATION
P/N RI : MC276-0018
P/N VENDOR : 7b3060606
QUANTITY : 14

MISSIONS : HF VF FF OF SM
PHASE(S) : PL LG X LW X DD X LS
NUMBER OF SUCCESS PATHS REMAINING
OUTLETS FOR EACH PROP

FAILURE DETECTABLE IN FLIGHT? : NO
FAILING DETECTABLE IN FLIGHT? : NO
GND TURNAROUND? : YES

ITEM: DISCONNECT, QCX, 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/THRUSTERS AFTER LANDING & PROPELLANT TANKS FILL, VENT & PURGE DURING FLIGHT.

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): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF PROPELLANT FIRST ORDER FAILURE FOR LOOSE RETAINER NUT. (B) POSSIBLE FIRE/EXPLOSION IF FUEL REACTS WITH COMPLEMENTARY OXIDIZER FOR 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:
POSSIBLE CORROSION OF SURROUNDING COMPONENTS. STRUCTURAL CAP CONSIDERED AS STRUCTURE.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N RI: WC276-0018
P/N VENDOR: 76306000
QUANTITY: 14

ABORT: CRIT. FUNC: 1
CRIT. How: I
MISSIONS: HF VF X FF OF SH
PHASE(S): PL LO X 00 X 00 X LS

ASSEMBLY: PRESSURIZATION ABORT: CRIT. FUNC: 1
CRIT. How: I
MISSIONS: HF VF X FF OF SH
PHASE(S): PL LO X 00 X 00 X LS

PREPARED BY: C SCARLETT
APPROVED BY: F NAS5/2106

DE
REL
R DIEHL

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

ITEM: DISCONNECT, QCK, PURGE,
VENT, PROPELLANT WITH STRUCTURAL END CAP AND SPRING LOADED POPPET (1/2") (MD 117, 118, 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, 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): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(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 (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 SUBJECT 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.
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 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.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 1C2

SUBSYSTEM : FWD - REACTIONS CONTROL
ASSEMBLY : PRESSURIZATION
P/N RI : MG276-0018
P/N VENDOR: 78306000
QTY : 14

MISSIONS: HF VF X FF CF SM

PHASE(S): PL X LG GU DO LS

NUMBER OF SUCCESS PATHS REMAINING 1

AFTER FIRST FAILURE:

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

FAIILURE DETECTABLE IN FLIGHT? N/A

TIME TO EFFECT: IMMEDIATE

REFERENCE DOCUMENTS: MJ70-6610-01E

GROUND TURNAROUND? YES

GSE EQUIPMENT FLOW RATE AND TANK OUTPUT

PRESSURE VAZP-1210C, 1310C

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

ITEM: DISCONNECT, QCK, PURGE, VENT, PROPellant WITH STRUCTURAL ENL CAP AND SPRING LOADED POPPET (1/2"), (MD 117, 116, 123, 124, 127, 137, 136, 147, 161, 162, 163, 164).

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

FAIILURE MODE: FAILS CLOSED (F)

DURING GROUND OPERATIONS

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

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) CREW/VEHICLE:
(A) LOSS OF PURGE FUNCTION. (B) NO EFFECT. (C) POTENTIAL LAUNCH DELAY. (D) NONE.

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

REMARKS/HAZARDS:
NONE. NO REDUNDANCY PROVIDED FOR THIS ITEM.
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 ☐]

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 X]

3a. IF NOT, DOES THE CAPABILITY EXISTS 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 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 ☐ 1X ☒ 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 ☐ 1X ☒ NO ☐]

8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:
   A. CAN THE BFS BE ENGAGED AFTER OCCURRENCE? [YES ☒ 1X ☒ NO ☐]
   B. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE? [YES ☒ 1X ☒ 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 & 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.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 1C2

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N: M276-0032
P/N VENDOR: RR42670-567, R642950C-163
QUANTITY: 14
SEVEN REQ'D FOR EACH
PROPELLANT AFTER FIRST FAILURE:

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

PREPARED BY: C SCARLETT
APPROVED BY: DES R DIEHL

ITEM: DISCONNECT, QUICK, TEST
PT. (1/4") WITH SPRING LOADED POPPET AND STRUCTURAL CAP. (M0 101, 162, 163, 104, 107, 108, 109, 110, 111, 112, 113, 14, 175 & 177).
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
CAUSE(S):
VIBRATION, PIECE PART STRUCTURAL FAILURE (POPPET, SEAL), MECHANICAL SHOCK.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION (D) C/OF 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.

CORRECTING ACTION:
UTILIZE AFT MODULES TO ORIENT VEHICLE FOR ENTRY AND COMPLETE ABDK.
REMARKS/HAZARDS:
NONE.
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM: Fwd - Reaction Control
P/N NI: ME276-0032
P/N VENDOR: RR42670-587, R642900-163
P/N: N003-2F-LO1090-1
REV: 11/09/10
SUBSYSTEM: Fwd - Reaction Control
ABORT: CRIT. FUNC: 12
CRIT. HO:
MISSIONS: HF, VF, FF OF SM
PHASE(S): PL, LO, CO, DO, LS
QUANTITY: 14
SEVEN REQ'D FOR EACH
PROPELLANT
REDUNDANCY SCREEN: 4-PASS B-FAIL C-PA
PREPARED BY:
DES: C. Scarlett
REL: R. Diehl
APPROVED BY:
DES: C. Scarlett
REL: R. Diehl
SM: W. Fortwell
APPROVED WITH CHANGES

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 THE SERVICE PANEL.
FAILURE MODE: EXTERNAL LEAKAGE (S)
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 OTHER 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 VERIFI. OF RAW MAT'L. PARTS MFG, IDENTIFICATION, AND PROTECTION, ASSY OPERATIONS, NDE EXAM OF WELDS, BRAZES, AND MAT'L AND EQUIP CONFORMANCE. TURNOVER 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 LH/SM RCS DUE TO PROCESS DEFICIENCIES.
<table>
<thead>
<tr>
<th>Item</th>
<th>Test Quick Disconnect, Propellant</th>
<th>FAILURE MODE</th>
<th>Fails Closed/Ground Ops</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

---

**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: RR4267C-567, R6429C-1&3  
QUANTITY: 14  
MISSIONS: HF, VF, X, FF, UF, SM  
PHASE(S): PL, XL, GO, DD, LS  
NUMBER OF SUCCESS PATHS REMAINING: 1  
REDUNDANCY SCREEN: A-PASS, B-N/A, C-PAS  
FAILURE DETECTABLE IN FLIGHT?: N/A  
GROUND TURNAROUND?: YES  
REFERENCE DOCUMENTS: MJ70-0101EB,  
4267C-567, R6429C-1&3  
1114C  
PREPARED BY: LES C SCARLETT  
APPROVED BY: DES REL 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 THE 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:  
(A) LOSS OF TEST/CHECKOUT DATA. (B) 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.
SUBSYSTEM  Fwd. Reaction Control
ITEM  Helium Quad Check Valve
FAILURE MODE  Fails Open

1. DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNUNCIATE OR TAKE ACTION IN RESPONSE)?
   a. 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)?
   a. 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?
   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. X NO H/S ISSUES  3. X NO SOFTWARE DETECTION
2. X HARDWARE ACCEPTS RISK  4. X DETECTION DURING CHECKOUT
5. X ACCEPTANCE RATIONALE BELOW
6. X RECOMMENDED CHANGES BELOW

EXPLANATION/COMMENTS:
1. Series redundant.
SUBSYSTEM: Fwd - Reaction Control
ASSEMBLY: Pressurization
P/N: MC284-0481-CC01/-0C02
P/N VENDOR: RSC10500-001/-011
QUANTITY: 2
: One per helium supply

FAILURE DETECTABLE IN FLIGHT?: No

GROUND TURNAROUND?: Yes
GROUND TEST PORTS

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

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
<table>
<thead>
<tr>
<th>Question</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</strong></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>No</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>YES</td>
<td>*NO</td>
<td>X</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>YES</td>
<td>NO</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. <strong>As a result of this failure mode, can the software overstress the hardware or induce another failure?</strong></td>
<td>YES</td>
<td>NO</td>
<td>X</td>
</tr>
<tr>
<td>5. <strong>Can this failure mode, in combination with software logic, adversely affect other functions?</strong></td>
<td>YES</td>
<td>NO</td>
<td>X</td>
</tr>
<tr>
<td>6. <strong>How many of these hardware failures can the shuttle tolerate (consider crew action and hardware/software operation)? Note change to FMEA criticality.</strong></td>
<td>0</td>
<td>1</td>
<td>X 2</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. <strong>If the answer to either 1 or 3 is yes:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Can the BFS be engaged after occurrence?</td>
<td>YES</td>
<td>*NO</td>
<td></td>
</tr>
<tr>
<td>B. Will BFS tolerate failure without loss of crew/vehicle?</td>
<td>YES</td>
<td>*NO</td>
<td></td>
</tr>
</tbody>
</table>

**Explanation Required (see below)**

<table>
<thead>
<tr>
<th>Change/Retention Rationale Summary</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. NO H/S ISSUES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. HARDWARE ACCEPTS RISK</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. NO SOFTWARE DETECTION</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. DETECTION DURING CHECKOUT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. ACCEPTANCE RATIONALE BELOW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. RECOMMENDED CHANGES BELOW</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.
ITEM: VALVE, QUAD, CHECK, HE (CV 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, D) No effect unless multiple failures occur. (E) No effect.
(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.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PRESSURIZATION
P/N RI: MC284-0481-0001/0002
P/N VENDOR: RS010500-001/011
QUANTITY: 2
PREPARED BY: DES R. BURKHART
REL R. DIEHL

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

FAILURE MODE: FAILS CLOSED (F)

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. (D) NO EFFECT.

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. (C) AUDIT CONDUCTED ON 1-16-78 INDICATED THAT SUPPLIER QC VERIFIED RAW MAT'L. CERTIFICATION TO SATISFY SHUTTLE DESIGN REQUIREMENTS, VERIFIED PROTECTION OF DETAIL PARTS FROM DAMAGE DURING MFG AND TEST, IN-PROCESS INSPECTION VERIFIED MFG TRAVELER SEQUENCES. TURNOVER 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.

REEDUNDANCY SCREEN: A-PASS B-FAIL C-FAIL

See Section 13.0
SUBSYSTEM: Fwd Reaction Control
ITEM: Propellant Line Flex Assy.

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 [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.
   - 0 [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. [X] 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. 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".
SUBSYSTEM: FW- REACTION CONTROL
ASSM. : PROPELLANT FEED
P/N: CR-2F -12106-1
P/N VENDOR: MC271-0095
Quant. : 2
MISSONS: HF VF X FF CF SM
 Failure Mode: EXTERNAL LEAKAGE

FUNCTION:
TO PROVIDE PROPELLANT FEED TO APPROPRIATE PROPELLANT FEEDLINES.

FAILURE MODE: EXTERNAL LEAKAGE

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.

CORRECTING ACTION:
ATTEMPT TO ISOLATE AND INITIATE ABORT IF REQ'D.

REMARKS/HAZARDS:
PERIODIC 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-C302-CA.
ITEM: PROP LINE FLEX ASSY

FUNCTION:
- TO PROVIDE PROPELLANT FEED TO APPROPRIATE PROPELLANT FEEDLINES.

FAILURE MODE: EXTERNAL LEAKAGE

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

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
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, ADOREDLY 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. 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).
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 1L2

SUBSYSTEM: FMC - REACTION CONTROL
ASSEMBLY: PROPellant FEED.
P/N: V070-421001
P/N VENDOR: MISSIONS: HF VF X FF OF SM
QUANTITY: 1 PHASE(S): PL LO X GO X DO X LS
ABORT: CRIT. FuNG: NUMBER OF SUCCESS PATHS REMAINING
CRIT. FUNC: 1
P/N: VO70-421001

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
TIME TO EFFECT: SEAOD TO DAYS
PROPELLANT TANK PRESSURE V42P-1310C AND MANIFOLD
PRESSURE 1312C & 1315C
REFERENCE DOCUMENTS:
V070-421001

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

PREPARED BY:
DEF ASIEGELIN
REL 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 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 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. 1YYX-0302-04.

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

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

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

PREPARED BY: A SIEGELIN  REL R DIEHL

ITEM: FEEDLINE AND FITTINGS
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 ET SEPARATIONS.

DISPOSITION & RATIONALE (A) DESIGN (B) TEST (C) INSPECTION (D) FAILURE HISTORY
(W) FACTOR OF SAFETY OF 4.0 WILL MINIMIZE FAILURE POTENTIAL.  DYNA TUBE 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 1.25X MAX OPERATING PRESSURE OR 1.1X SURGE (TRANSIT) PRESSURE WHICHEVER IS GREATER.  PERFORMED TUBING CERTIFICATION PER "ORBITER TUBING VERIFICATION PLAN SD75-SH-0205".  (C) IN-PROCESS INSPECT INCLUDES NDT & CHECKS DURING INSTALLATION.  TURNDOWN INSPECTION INCLUDES MONITORING FUNCTIONAL TESTS DURING PRESSURIZATION CYCLE FOR EVIDENCE OF LEAKS.  VISUALLY INSPECT FOR DAMAGE WHERE ACCESSIBLE.  HARDWARE INSPECTION IN ACCORDANCE WITH PLANNING ROUTS APPROVED BY NASA.  (D) MINOR FAILURE HISTORY — CORROSION AND FAB PROBLEMS REPORTED DURING APOLLO PROGRAM AND CORRECTED WITH APPLICABLE TMO/TPC REQUIREMENT.
<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 ANNOUNCE OR TAKE ACTION IN RESPONSE)?</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1a. IF NOT, DOES THE HARDWARE PROVIDE INFORMATION THAT THE FLIGHT SOFTWARE COULD USE TO DETECT THE FAILURE?</td>
<td></td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<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>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<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>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<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>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<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>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?</td>
<td></td>
<td></td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<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>
<td></td>
<td><em>0</em></td>
</tr>
<tr>
<td></td>
<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>N/A</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. 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></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></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>*EXPLANATION REQUIRED (SEE BELOW)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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. "RCS JETS" light on caution and warning panel.
2. The manifolds are in parallel (2 legs) giving one redundant path.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 1G1

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PROPELLANT FEED
P/N K1: MC234-0430-0007-0008
P/N VENDOR: 5750025/575026
QUANTITY: 4

MISSIONS: HF VF X FF OF SM

FAILURE DETECTABLE IN FLIGHT?: YES
THURSTER CHAMBER PRESS., MANIFOLD PRESSURE MONITO

GROUND TURNAROUND?..............YES

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

COMPONENTS: EI-STABLE, \( \text{TANK \text{PRESSURE}=245 \text{PSI} \). 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 KENDEVUS 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 & KMA 5750025.

PREPARED BY: DEG R GONZALEZ
APPROVED BY: DEG R DIELH

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: EI-STABLE, \( \text{TANK \text{PRESSURE}=245 \text{PSI} \). 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 KENDEVUS 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 & KMA 5750025.
SUBSYSTEM : FWO - REACTION CONTROL
ASSEMBLY : PROPELLANT FEED
P/N RI : MC284-0430-0007/-0008
P/N VENDOR: 5750025/5750026
QUANTITY : 4

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.
3) 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 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 PROPOGATION. (C) LOSS OF MISSION. ABORT DECISION. (D) POTENTIAL VEHICLE DAMAGE FROM COLLISION WITH RENDEVOUS TARGET, AFTER SECOND FAILURE. CRIT I 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 SUBJECTED TO ACCEPT TEST VIBRATION. VALVE IS SUBJECTED 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 PSIG, MORE THAN 4 X WORKING PRESSURE. (C) AUDIT CONDUCTED 7-1-76 VERIFY SUPPLIER INSPECTION CONTROL OF PARTS ID AND PROTECTION, MFG PROCESSES, ELECT TERMINATIONS. TURNDOWN INSPECTION INCLUDES MONITORING TEST TO VERIFY ELECTRICAL POWER TO VALVE FOR EVIDENCE OF SHORT CIRCUITY. (D) NO FLIGHT FAILURE EXPERIENCE.
HARDWARE/SOFTWARE ANALYSIS CHECKLIST

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

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 [ ]

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 [ ] 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 [ ]

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 3. [ ] NO SOFTWARE DETECTION 5. [ ] ACCEPTANCE RATIONALE BELOW
2. [X] HARDWARE ACCEPTS RISK 4. [ ] DETECTION DURING CHECKOUT 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.
SUBSYSTEM : FWD - REACTION CONTROL

ASSEMBLY : PROPellant ABORT: CRIT. FUNC: 1
P/N RI : MC276-0018 CRIT. HND: 1
P/N VENDOR: 763010LC MISSIONS: HF VF X FF OF SM
QUANTITY : 6 PHASE(S): PL LO X DO X DO X LS

FAILURE DETECTABLE IN FLIGHT?: YES TIME TO EFFECT:
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 (S)
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 ABORT:
P/N RI: MC276-0018 CR
P/N VENDOR: 76301000 MISSIONS: HF VF X FF OF SM
QUANTITY: 6 PHASE(S): PL LO X OC X DO X LS

FUNCTION:
1
P/N: MC276-0018
CR
PREPARED BY:
APPROVED BY:
APPROVED BY NASA

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
(s)
DURING FLIGHT

CAUSE(S):
1. VIBRATION, AND LOOSENING OF RETAINER NUT, PIECE PART STRUCTURAL FAILURE, MECHANICAL SHOCK.
2. 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:
1. 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 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.
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY</strong></td>
<td>YES</td>
</tr>
<tr>
<td>ANNUNCIATE OR TAKE ACTION IN RESPONSE? )</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>
</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>
</tr>
<tr>
<td>3. <strong>DOES THE FLIGHT SOFTWARE TAKE ACTION TO NEGATE THE EFFECTS OF THE FAILURE</strong> (EITHER BY COMMANDING HARDWARE ACTION OR IMPLEMENTING ALTERNATE PROGRAM LOGIC)?</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>
</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>
</tr>
<tr>
<td>5. CAN THIS FAILURE MODE, IN COMBINATION WITH SOFTWARE LOGIC, ADVERSELY AFFECT OTHER FUNCTIONS?</td>
<td>*YES</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>*O</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>
</tr>
<tr>
<td>8. IF THE ANSWER TO EITHER 1 OR 3 IS YES:</td>
<td></td>
</tr>
<tr>
<td>a. CAN THE BFS BE ENGAGED AFTER OCCURRENCE?</td>
<td>YES</td>
</tr>
<tr>
<td>b. WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?</td>
<td>YES</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:**

Out of scope - ground operations only.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITEER 10L

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PROPELLANT
P/N: MC276-001B
P/N VENDOR: 76510100
QUANTITY: 6

AEORT: NO
MISSIONS: HF VF X FF UF SM
PHASE(S): PL X LD 00 D0 LS

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

THREE REQ PER PROPELLANT AFTER FIRST FAILURE: 0

FAILURE DETECTABLE IN FLIGHT?: NA

GROUND TURNAROUND? YES
GROUND EQUIPMENT FLOW RATE READ OUT

PREPARED BY:
DES C SCARLETT
REL R DIEHL

APPROVED BY:

REFERENCE DOCUMENTS:
MJ670-C051-01b
SD72-Sh-0103-2
VS70-4210C1

ITEM: DISCONNECT, QUICK, FILL PROPELLANT, SPRING LOADED POPPET & STRUCTURAL CAP (MD119-126).
FUNCTION:
TO PROVIDE FOR GRAINING, VENTING, AND BLEEDING PROPELLANT TANKS. IN BOTH HORIZONTAL AND VERTICAL VEHICLE ORIENTATION.

FAILURE MODE: FAILS CLOSED (F)

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

EFFECT(S):
(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.
HARDWARE/SOFTWARE ANALYSIS CHECKLIST 03-2F-102170-1

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

ITEM  DC Solenoid Operated Valve  FAILURE MODE  Fails Closed - Premature Operation


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 ANSWERS 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. 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.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PROPELLANT FEED
P/N: MC284-0420-0011/-0012
P/N VENDOR: 7395-0011/-0012
QUANTITY: 2

FAILSAFE ISSUE:
ONE REQ'D PER PROPELLANT

AFTER FIRST FAILURE:

REDUNDANCY SCREEN:
A-PASS B-PASS U-FAIL

FAILSAFE DETECTABLE IN FLIGHT?: YES
MANIFOLD POSITN INDICATOR V42X1232E
V42X1332E
GROUND TURNAROUND? .............. YES
SAME AS FLIGHT

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

ITEM:

VLCVE, 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 I) SUBSEQUENT TO DOWNSTREAM FAILURE(S) 2) PRIOR TO SYSTEM
ACTIVATION.
FAILSAFE MODE: FAILSAFE 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.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PROPELLANT FEED
P/N RI: MC284-0420-0011-0012
P/N VENDOR: 73895-0011-0012
QUANTITY: 2
P/N VENDOR: 4C284-0420-0011-0012
MISSIONS: HF, VF, X, FF, OF SM
QUANTITY: 2
PHASE(S): PL, LO, OO, X, DO, LS
REDUNDANCY SCREEN: A-PASS, B-PASS, C-FAIL

PREPARED BY:
DEP: R BURKHART
REL: R DIELH
APPROVED BY:
DEP: (NASA)
REL: (NASA)

ITEM: VALVE, DC SOLEN OPERATED -
VERNIER THRUSTER MANIFOLD, (1/4") SI-STABLE, SCLENOID DRIVEN 28VDC.
(LV 157-158)

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

FAILURE MODE: FAIL CLOSED-PREMATURE (F)
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 HDL. (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
SCLENOID WIRING TO PRECLUDE SHORTS. (B) QUAL TEST INCLUDES 40 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 SCLENOID VALVE FOR
EVIDENCE OF SHORT CIRCUIT. SUPPLIER AUDIT CONDUCTED 8/31/77 VERIFIED
SUPPLIE INSPECTION EXCERCISED 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
WASHINGTON PROCESSING.
HARDWARE/SOFTWARE ANALYSIS CHECKLIST 03-2F-11110-1

SUBSYSTEM Fwd Reaction Control
ITEM Tank Assembly and Propellant
ACQUISITION DEVICE
FMEA NUMBER SD75-SH-0016A
FAIURE NODE Large Rupture

1. Does the flight software detect this failure mode (i.e., automatically announce 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 over-stress 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

In-Flight Detectability

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: MC282-0061-0001/0002

P/N VENDOR: 555332000-009/010

QUANTITY: 2

MISSIONS: HF, VF, X, FF of SH

PHASE(S): PL, LU, DU, X, GG, XL, LS

ONE REQ'D NUMBER OF SUCCESS PATHS REMAINING

PER PROPELLANT AFTER FIRST FAILURE:

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

FAILURE DETECTABLE IN FLIGHT?: YES

TIME TO EFFECT:

MONITOR TANK Pressures V42P1310C, 1312C, 1316C, 116C

GROUND TURNAROUND? ............ YES

SAME AS FLIGHT

PREPARED BY:

APPROVED BY:

DES R BEMIS

REL R DIEHL

ITEM: TANK ASSY, PROPELLANT

INCLUDING PROPELLANT ACQUISITION DEVICE AND COMPARTMENT ENCLOSURE (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 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 KCS 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 HAZARD FROM FIRE, EXPLOSION DUE TO FREE FUEL IN MODULE.

REFERENCE HAZARDS 1YXX-0302-02 AND 1YXX-0302-04.
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PROPELLANT FEED
P/N REF: MC282-0061-0001/0002
P/N VENDOR: 855C3320000-009/010
QUANTITY: 2
MISSION: HF, VF, FF, NF, SM
PHASE(S): PL, LO, X, ON, X, DO, X, LS

PREPARED BY:
APPROVED BY:

DES: R BENIS
REL: R DIEHL

PREPARED 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 PSI + OR - 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 FACTSA 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 PENTRANT, PROOF PRESSURE (1.33 MAX OPER PRESSURE), AND EXTERNAL LEAK TESTS DURING ACCEPTANCE TESTING. TANKS SUBJECTED TO 90 DAY PROPELLANT EXPOSURE, 800 PRESSURE CYCLES, 40 MINUTES PER AXIS OF 3.9 GRMS RANDOM VIBRATION AND BURST PRESSURE DURING QUAL PROGRAM. (C) TURNOAROUND 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 AGF 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 ☐
2. Hardware Accepts Risk ☑
3. NO SOFTWARE DETECTION ☐
4. DETECTION DURING CHECKOUT ☐
5. ACCEPTANCE RATIONALE BELOW ☐
6. RECOMMENDED CHANGES BELOW ☐

---

EXPLANATION/COMMENTS:

1. V42P11115C, 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: FWE - REACTION CONTROL
ASSEMBLY: PROPELLANT FEED
P/N: XC282-0061-C001/C002
P/N VENDOR: 255C3320000-C09/C1C
QUANTITY: 2
ONE REQ'D
PER PROPELLANT

MISSIONS: HF VF X FF OF SM
PHASE(S): PL X LD X CD X CD X LS

FAILURES 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
REL: R DIEHL

APPROVED BY:

ITEM: TANK ASSY, PROPELLANT
INCLUDING PROPELLANT ACQUISITION DEVICE AND COMPARTMENT CARRIER (IN 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 FAILURES.

EFFECT(S): ON (A) SUBSYSTEM (B) INTERFACES (C) MISSION ID (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 AREAS 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/HELIUM LOST.

REMARKS/HAZARDS:
POTENTIAL HAZARD FROM FREE PROPELLANT IN MODULE. NO REDUNDANCY PROVIDED FOR THIS ITEM. REFERENCE HAZARD 1YXX-0302-05.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: PROPELLANT FEED
P/N RI: MC282-0061-0001/0002
P/N VENDOR: 855C3320000-009/010
QUANTITY: 2

- ABORT CRIT. FUC: 2
- MISSIONS: HF VF X FF OF SM
- PHASE(S): PL X LO X CO X DO X LS
- PREPARED BY: APPROVED BY: APPROVED BY (NASA):
- DES R BEHIS DES R BEHIS DES R BEHIS
- REL R DIEHL REL R DIEHL REL R DIEHL

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 IF IGNITION SOURCE PRESENT (SECOND FAILURE).

DISPOSITION & RATIONALE
- DESIGN (A) TEST (B) INSPECTION (D) FAILURE HISTORY:
- (A) DESIGN FACTOR OF SAFETY IS 1.5 MIN. DEVELOPMENT TESTS INCLUDE HELD CYCLE LIFE (800 CYCLES), FRACTURE MECHANICS, FORGING EVALUATION, AND TUBE SWAGING. (B) TANKS SUBJECTED TO RADIOGRAPHIC, FLUORESCENT PENETRANT, PROOF PRESSURE (1.33X 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 RANDOM 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).
**HARDWARE/SOFTWARE ANALYSIS CHECKLIST**

**SUBSYSTEM** Fwd. Reaction Control

**ITEM** Tank Assembly and Propellant

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

**FAILURE MODE** Restricted Flow

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</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></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. <strong>ARE THE ANSWERS TO QUESTIONS 1 AND 1a CONSISTENT WITH THE FMEA EVALUATION OF IN-FLIGHT DETECTABILITY?</strong></td>
<td>YES</td>
<td>*NO</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>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. <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>
</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>YES</td>
</tr>
<tr>
<td>8. <strong>IF THE ANSWER TO EITHER 1 OR 3 IS YES:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. <strong>CAN THE BFS BE ENGAGED AFTER OCCURRENCE?</strong></td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>B. <strong>WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?</strong></td>
<td>YES</td>
<td>NO</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. "Fail Off" detection in RCS RM.
2. "No redundant tanks."
3. "No correcting action...abort..."
4. Same as primary.

---

FMEA CHANGE RECOMMENDED

85
SUBSYSTEM : FWO - REACTION CONTROL
ASSEMBLY : PROPELLANT FEED
P/N RI : KG282-0061-0001/0002
P/N VENDOR: S532320GC-006232
QUANTITY : 2
ONE REQ'D PER PROPELLANT

FAILURE DETECTABLE IN FLIGHT?: YES
ENGINE PERFORMANCE

GROUND TURNAROUND:.............NO

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

REMARKS/HAZARDS:
COMPLETE LOSS OF FRCS USAGE THEREFORE ALL ATTITUDE CONTROL MUST BE ACCOMPLISHED BY ARCS.

ITEM: TANK ASSY, PROPELLANT
INCLUDING PROPELLANT ACQUISITION DEVICE AND COMPARTMENT SHELLER. (TK 1G3).

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/HELIUM INGESTION. (B) NONE.
(C) LOSS OF MISSION DUE TO LOSS OF PROPELLANT. (D) NONE UNLESS FAILURE
OCURRS WHEN MODULE REQUIRED FOR ET SEPARATION.

CORRECTING ACTION:
NONE AVAILABLE - CLOSE DOWN FRCS AND ABORT MISSION.

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

SUBSYSTEM : FWD - REACTION CONTROL

ASSEMBLY : PROPELLANT FEED ABORT:

P/N RI : MC282-0051-0001/0002 CRIT. FUNC: 1

P/N VENDOR : 855C332 0000-009/010 CRIT. HDW: 1

- QUANTITY : 2 MISSIONS: HF VF X FF OF SH
- ONE REQ'D
- PER PROPELLANT PHASE(S): PL LO X NO X DO X LS

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

PREPARED BY: DES R BEMIS DES
APPROVED BY: SSM
APPROVED BY: NASA
APPROVED WITH CHANGES

ITEM: TANK ASSY, PROPELLANT
INCLUDING PROPELLANT ACQUISITION DEVICE AND COMPARTMENT BARPIER. (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/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, 40 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 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 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 [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 [ ] 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 [x]

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 [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 [ ] No [x]

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 [ ] No [x] *Explanation required (see 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: MG28Z-6661-0001/0002
P/N VENDOR: 656C32000C-000/010
MISSIONS: BF VF X FT OF SM
QUANTITY: 2
P/N VENDOR: 55C33/200C/000 MISSIONS: -F VF X

FUNCTION:
TIT STORE/SUPPLY PROPELLANT TO REACTION CONTROL ENGINE MANIFOLDS.
NOMINAL STORAGE PRESSURE 245 PSIG + OR -15 (1.5 SAFETY FACTOR).
FAILURE 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) CREW/VEHICLE:
(A) EXCESSIVE GAS FLOW TO THRUSTERS COULD CAUSE TANK BARRIER FAILURE.
(B) POTENTIAL DAMAGE TO THRUSTERS IF UNDETECTED.
(C) AVOID DECISION.
(D) POSSIBLE LOSS OF CREW/VEHICLE IF FAILURE OCCURS PRIOR TO LT SEPARATION.

CORRECTING ACTION:
SHUT DOWN RCS AND ABORT MISSION.

REMARKS/HAZARDS:
IF UNDETECTED, THE THRUSTERS COULD BE DAMAGED WHICH COULD CAUSE ENTRY UNCERTAINTY.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsystem: FWD - Reaction Control</td>
<td>FMEA No. 03-2F - 111110-4</td>
</tr>
<tr>
<td>Assembly: Propellant Feed</td>
<td>Abort: CPIT, Func: 2</td>
</tr>
<tr>
<td>P/N RI</td>
<td>MC202-0061-0001/0002</td>
</tr>
<tr>
<td>P/N Vendor: 555C3320000-009/010</td>
<td>Missions: HF, VF, X, FF, DF, SM</td>
</tr>
<tr>
<td>Quantity</td>
<td>2</td>
</tr>
<tr>
<td>Phase(s):</td>
<td>PL X LO X CO X DO X LS</td>
</tr>
<tr>
<td>Preparied By:</td>
<td>APPROVED BY:</td>
</tr>
<tr>
<td>Des</td>
<td>R BEMIS</td>
</tr>
<tr>
<td>REL</td>
<td>R OIEHL</td>
</tr>
<tr>
<td>Redundancy Screen:</td>
<td>A-N/A, B-N/A, C-N/A</td>
</tr>
<tr>
<td>Item: Tank Assy, Propellant</td>
<td>See Section 13.0</td>
</tr>
<tr>
<td>Function:</td>
<td>To store/supply propellant to reaction control engine manifolds. Normal storage pressure 245 psig or -15 (1.5 safety factor).</td>
</tr>
<tr>
<td>Failure Mode:</td>
<td>Loss of gas retention in (s)</td>
</tr>
<tr>
<td>Propellant Acquisition Device (PAD):</td>
<td></td>
</tr>
<tr>
<td>Cause(s):</td>
<td>Vibration, Shock, Propellant contamination (Chemical or dirt)</td>
</tr>
<tr>
<td>Effect(s):</td>
<td>(A) Subsystem (B) Interface (C) Mission (D) Crew/Vehicle:</td>
</tr>
</tbody>
</table>
| Disposition & Rationale | (A) Design factor of safety is 1.5 min. Development tests include weld cycle LI FF (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, 48 minutes per axis of 3.9 grms random vibration and burst pressure during qual program. (C) Turnaround inspection includes periodic bubble point checks of the PAD. 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 ☐

2a. **If Not, Does the Hardware Provide Information That the Flight Software Could Use to Detect the Failure?**
   - YES ☑ NO ☐

2b. **Are the Answers to Questions 1 and 2a Consistent with the FMEA Evaluation of In-Flight Detectability?**
   - YES ☑ NO ☐

3a. **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 ☐

3b. **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 2 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. V42P1115C, 1116C will give class 2 alarm.

   Gross leak detection applies.
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-G & G load.
  - 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 (2nd order failure) during a RIMS abort the loss of a manifold results in the loss of two down firing thrusters which results in crit 1. 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.
SUBSYSTEM: FWD - REACTION CONTROL

ASSEMBLY: THRUSTER

P/N: MC271-0084

P/N VENDOR: 74713-THRU 74717

QUANTITY: 30

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 WITH REACTANT (2ND ORDER FAILURE) DURING A RTLS ABORT 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 102136-1. (D) NO HISTORY OF FAILURE IN FLIGHT. (NEW DEVELOPMENT ITEM FOR MANNED FLIGHT APPLICATION.)
<table>
<thead>
<tr>
<th>Item</th>
<th>Failure Mode</th>
<th>FMEA Number</th>
<th>HARDWARE/SOFTWARE ANALYSIS CHECKLIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Injector Plate</td>
<td>Improper Mixture Ratio</td>
<td>SD75-SH-0016A</td>
<td>03-2F-121311-1</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 [ ] 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 [X] No [ ]

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.**
   - N/A [X] Yes [ ]

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/reasons required (see below):*

<table>
<thead>
<tr>
<th>Change/Retention Rationale Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. [X] Hardware Accepts Risk</td>
</tr>
</tbody>
</table>

**Explanation/Comments:**

1. "Fail Off" in RCS RM if sufficiently blocked.
SHUTTLE FAILURE MODE AND EFFECTS ANALYSIS - ORBITER 102

SUB-SYSTEM: FWL - REACTION CONTROL
ASSEMBLY: THRUSTER, PRIMARY
P/N: MC467-0C28
P/N VENDOR: X3C663
QUANTITY: 14
MISSIONS: HF VF FF SF SM

ASSEMBLY: FB1
P/N: MC467-0C25
P/N VENDOR: X3C663
QUANTITY: 14
MISSIONS: HF VF FF SF SM

ASSEMBLY: FB2
P/N: MC467-0C26
P/N VENDOR: X3C663
QUANTITY: 14
MISSIONS: HF VF FF SF SM

FUNCTION:
- TO RECEIVE FUEL AND OXIDIZER FROM THRUSTER INLET VALVES AND PROVIDE DOUBLET MIXING AT 1.60 OX TO FUEL (WEIGHT) RATIO FOR A HYPERSONIC 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):
- (A) LOSS OF ONE THRUSTER IN A GIVEN AXIS. (B) GN&C CONTROL SWITCHING REQUIRED. (C, D) 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

FUNCTION:
TO RECEIVE FUEL AND OXIDIZER FROM THRUSTER INLET VALVES AND PROVIDE DOUBLET MIXING AT 1.60 OX TO FUEL (WEIGHT) RATIO FOR A HYPERGOLIC REACTION WHICH PRODUCES 825 POUNDS OF THRUST AT 70,000 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):
(A) LOSS OF ONE THRUSTER IN A GIVEN AXIS. (B) GNC CONTROL SWITCHING REQUIRED. (C&D) NO EFFECT. (E) 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:
(A) 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. (B) TOTAL FLOW & FLOW DISTRIBUTION CHECKED BY WATER FLOW TEST AND VERIFIED BY BURN TEST DURING THRUSTER ACCEPTANCE TESTS. (C) FIBER OPTICS USED TO VISUALLY INSPECT INJECTOR HOLES FOR EVIDENCE OF BURRS AND CONTAMINATION PRIOR TO ASSEMBLY AUDIT CONDUCTED ON 9-2-76 VERIFIED THAT 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 ACCESSABLE FOR EVIDENCE OF DAMAGE & SYSTEM FLUID SAMPLINGS FOR DETECTION OF CONTAMINATION. (D) NO FAILURES OF THIS TYPE ON APOLLO.
## Component: Fwd. Reaction Control

### Item: Thrust Chamber

#### Failure Mode: Burn Through

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</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>X (Yes)</td>
</tr>
<tr>
<td>2a. If not, does the hardware provide information that the flight software could use to detect the failure?</td>
<td>X (Yes)</td>
</tr>
<tr>
<td>2. Are the answers to Questions 1 and 1a consistent with the FMEA evaluation of in-flight detectability?</td>
<td>X (Yes)</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>X (Yes)</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>X (Yes)</td>
</tr>
<tr>
<td>4. As a result of this failure mode, can the software overstress the hardware or induce another failure?</td>
<td>X (Yes)</td>
</tr>
<tr>
<td>5. Can this failure mode, in combination with software logic, adversely affect other functions?</td>
<td>X (Yes)</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>2 (Yes)</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>X (Yes)</td>
</tr>
<tr>
<td>8. If the answer to either 1 or 3 is Yes:</td>
<td></td>
</tr>
<tr>
<td>a. Can the BFS be engaged after occurrence?</td>
<td>X (Yes)</td>
</tr>
<tr>
<td>b. Will BFS tolerate failure without loss of crew/vehicle?</td>
<td>X (Yes)</td>
</tr>
</tbody>
</table>

### Change/Retention Rationale Summary

- X HARDWARE ACCEPTS RISK
- 3. NO SOFTWARE DETECTION

<table>
<thead>
<tr>
<th>Change/Retention Rationale</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. No H/S issues</td>
<td></td>
</tr>
<tr>
<td>2. Hardware accepts risk</td>
<td></td>
</tr>
<tr>
<td>3. No software detection</td>
<td></td>
</tr>
<tr>
<td>4. Detection during checkout</td>
<td></td>
</tr>
<tr>
<td>5. Acceptance rationale below</td>
<td></td>
</tr>
<tr>
<td>6. Recommended changes below</td>
<td></td>
</tr>
</tbody>
</table>

**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.

**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.
SUBSYSTEM: Reaction Control Assembly: Thruster, Primary
P/N: MC467-0028
P/N VENDOR: X5C958
Quantity: 14
P/N: X5C958
Vendor: X5
Missions: HF VF X FF OF SM
Quantity: 14

Prepared by: W. Searcy
Approved by: R. Diehl

SYSTEM: THRUSTER, PRIMARY ABORT: CRIT. FUNC: 1
CRIT. HWD: 1

FAILURE MODE: OVERHEAT/BURNTHROUGH
DUE TO INADEQUATE COOLING.

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

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.
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 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 COLUMBIUM 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 [ ] X

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 [ ] 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

**FMEA CHANGE RECOMMENDED**

**EXPLANATION/COMMENTS:**

3a. Instrumentation is available for software redesign.
SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: THRUSTER, PRIMARY
P/N: MC467-0528
P/N VENDOR: X30872
QUANTITY: 14

FAILURE DETECTABLE IN FLIGHT?: NO

GROUND TURNAROUND?: YES

visual inspection

PREPARED BY: DES W SEARCY

APPROVED BY: DES R DIEHL

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 DEFECT.

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 - CRIT 1 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 MALAKY 1YXX-0302-01.
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.

CAUSE(S):
- High temperature in local spot due to film cooling failure (contaminated injector coolant holes), Vibration, Shock, Weld or material defect.
- Failure propagates - critical for RTLS abort if thrust 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 Disilicide coating to withstand $2.0 \text{ g} \times \text{Hz}^2$ random vibration. Temp tests demonstrate excellent ductile/brittle qualifies for coated C-103 Columbium.
- (C) Turnaround inspection to include visual inspection for evidence of burn through & where accessible, use of fiber-optics for inspecting access holes, Supplier inspection includes fluoride penetrant 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 were met with identification of parts, MFG processes, corrosion protection, contamination control and environments.

102 Z036 SD75-SM-0003
### Fwd. Reaction Control

**Item:** Vernier Thruster  
**Failure Mode:** Loss of Output  
**FMEA Number:** SD75-SH-0016A

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 1. | **DOES THE FLIGHT SOFTWARE DETECT THIS FAILURE MODE (i.e., AUTOMATICALLY ANNOUNCE 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:**  
| 8a. | **CAN THE BFS BE ENGAGED AFTER OCCURRENCE?**  
| 8b. | **WILL BFS TOLERATE FAILURE WITHOUT LOSS OF CREW/VEHICLE?**  

---

**EXPLANATION/COMMENTS:**

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

2. 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.

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

4. The thrust chamber pressures can be downlinked.
SUBSYSTEM : FW - REACTION CONTROL
ASSEMBLY : THRUSTER ASSY
P/N RI : MC467-0029
P/N VENDOR: 

QUANTITY : 2
PHASE(S): PL LO CC X DO LS
ONE REQ'D PER SIDE

:(DOWN FIRING)

failure detectable in flight?. YES

THRUSTER CHAMBER PRESS V42P-1555A, 1556A IMMEDIATE

GROUND TURNAPOUND?.............YES

POSITION INDICATION

PREPARED BY:

DESI J. TAGGART
REL R. DIEHL

APPROVED BY:

DESI

ITEM: THRUSTER, VERNIER
(EN 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 X5DUCERS.

failure mode: loss of output (F)

INLET VALVES/BLOCKED INJECTOR/STAND-OFF'S.

cause(s):

contamination, piece part structural failure, improper solenoid 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.

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.
SHUTTLE CRITICAL ITEMS LIST – OPBTER 102

SUBSYSTEM: FWD – REACTION CONTROL
ASSEMBLY: THRUSTER ASSY
P/N RI: MC467-0029
P/N VENDOR:
QUANTITY: 2
ONE REQ'D PER SIDE
(DOWN FIRING)

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

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

ITEM: THRUSTER, VERNIER
FUNCTION:
TO PROVIDE THRUST FOR LOW LEVEL ACCELERATIONS ASSOCIATED WITH POINTING MANEUVERS AND THREE AXIS ATTITUDE HOLD. THRUSTEP FIRES 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 SCL OND 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.
## Item: Vernier Thruster

### Failure Mode: Erratic Operation

<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></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 over-stress 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)?</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>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>X</td>
</tr>
<tr>
<td>B. Will BFS tolerate failure without loss of crew/vehicle?</td>
<td>Yes</td>
<td>X</td>
</tr>
</tbody>
</table>

*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

**FMEA Change Recommended: No In-Flight Detectability**

### 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 : MC467-0029

P/N VENDOR: MISSIONS: HF VF X FF FF SM

QUANTITY : 2

P/N: MC467-O0 9 CRIT. KF : 2

VENDOR: MISSIONS: HF VF X FF FF SM

QUANTITY: 2

PHASE(S): PL LO DO X DO LS

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

FAILURE DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURE MODE: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A

FAILURE MOLD: ERRATIC OPERATION (F)

LOW/HIGH THRUST OR INTERMITTENT OPERATION

FAILURES DETECTABLE IN FLIGHT?: YES

THRUSTER CHAMBER PRESS. INDICATION V42P-1555A

1556A
SUBSYSTEM : FWD - REACTION CONTROL
ASSEMBLY : THRUSTER ASSY
P/N RI : 4C467-0029
ASSEMBLY : THRUSTER ASSY
P/N VENDOR : MISSIONS: HF VF X FF OF SM
QUANTITY : 2
PHASE(S) : PL LO GO X DO LS
P/N CRIT. HQD: 2
CRITICAL ITEM LIST - ORBITER 102

PREPARED BY: 
APPROVED BY:

FUNCTION:
- TO PROVIDE THRUST FOR LOW LEVEL ACCELERATIONS ASSOCIATED WITH POINTING MANEUVERS AND THREE AXIIS 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) INTERFACES (C) MISSION (D) CREW/VEHICLE:
- (A) LOSS OF VERNIER CONTROL (B) INTERFACE SWITCHING OF POWER AND GN&C CONTROL TO LARGE THURSTERS. (C) POSSIBLE EARLY MISSION TERMINATION 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.
- 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 MATERIAL 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]
   - 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: [X] No: [ ]
   - 5. Can the flight software use the information to detect the failure?
   - 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?
   - 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. [X] 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

Explanations/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. This is a criticality 1 failure and cannot be tolerated.
3. The thrust chamber pressures can be downlinked.
4. Same as primary.
ITEM: THRUSTER, VERNIER  
(EM 157/158)  
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/BURNTROUGH (F)  
CAUSE(S):  
MAX PRESSURE SPIKES, SURFACE DEFECTS IN THE PROTECTIVE DISILICIDE 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.
SHUTTLE CRITICAL ITEMS LIST - ORBITER 102

SUBSYSTEM: FWD - REACTION CONTROL
ASSEMBLY: THRUSTER ASSY
P/N RI: MC467-0029
P/N VENDOR: MISSIONS: HF VF X FF OF SM
QUANTITY: 2

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

CAUSE(S):
MAX PRESSURE SPIKES, SURFACE DEFECTS IN THE PROTECTIVE DISILICIDE COATING FOR CHAMBER WALL AND VIBRATION.

EFFECT(S): ON (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.

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 COLUMBNIUM 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 MAT'L, 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 Organization Phone
   Edward Vonusa NASA X-1470
   Dave Latham JSC Reliability 527-0323
   (Boeing)
   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-2908

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 1a.
   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 V4211116C. (Explanation 1.)
   03-2F-101060-2: Add "X", No Block, question 1a.
   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 V4211113C, 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: 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-102170-1: Under 1 Explanation, add measurements V42X1333X, 1233X. Change class 2 to 3.

03-2F-111110-1: Under 1 Explanation, add V42P1312C and delete 1313C and 1314C.

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.