

INDEPENDENT ORBITER ASSESSMENT

ASSESSMENT OF THE FMEA/CIL INSTRUCTIONS AND GROUND RULES

14 OCTOBER 1986

MCDONNELL DOUGLAS ASTRONAUTICS COMPANY
HOUSTON DIVISION

SPACE TRANSPORTATION SYSTEMS ENGINEERING AND OPERATIONS SUPPORT

WORKING PAPER NO. 1.0-WP-VA86001-01

INDEPENDENT ORBITER ASSESSMENT
FMEA/CIL INSTRUCTIONS AND GROUND RULES

14 OCTOBER 1986

This Working Paper is Submitted to NASA under
Task Order No. VA86001, Contract NAS 9-17650

PREPARED BY:

S.T. Traves
S.T. Traves
Staff Manager
Reliability

APPROVED BY:

G.W. Knori
G.W. Knori
Technical Manager
Independent Orbiter
Assessment

APPROVED BY:

R.L. Buchanan
R.L. Buchanan
Staff Senior Manager
Safety, Reliability &
Maintainability

APPROVED BY:

W.F. Huning
W.F. Huning
Deputy Program Manager
STSEOS

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
1.0 <u>EXECUTIVE SUMMARY</u>	1
2.0 <u>INTRODUCTION</u>	4
3.0 <u>ASSESSMENT RESULTS</u>	5
3.1 OMISSIONS.....	5
3.2 AMBIGUITIES.....	11
3.3 LIMITED VISIBILITY.....	12
4.0 <u>REFERENCES</u>	16
APPENDIX A: ROCKWELL 100-2G ASSESSMENT ISSUES	
APPENDIX B: NSTS 22206, BASIC, ASSESSMENT ISSUES	
APPENDIX C: PRESENTATION PACKAGE	

<u>Figure</u>	<u>Page</u>
1 Rockwell 100-2G, Figure 10.....	A-2
2 Streamlined Criticality Category Cross Reference..	A-3
3 NSTS 22206 FMEA/CIL Screening Process.....	B-2
4 Streamlined Criticality Category Cross Reference..	B-3

Table

Page

1	FMEA/CIL ASSESSMENT ISSUE IMPACTS.....	15
---	--	----

INDEPENDENT ORBITER ASSESSMENT FMEA/CIL INSTRUCTIONS AND GROUND RULES

1.0 EXECUTIVE SUMMARY

The McDonnell Douglas Astronautics Company was selected in June 1986 to conduct an independent assessment of the Orbiter Failure Mode and Effects Analysis/Critical Items List (FMEA/CIL). Part of this effort involved an examination of the FMEA/CIL preparation instructions and ground rules. Assessment objectives were to identify omissions and ambiguities in the ground rules that may impede the identification of shuttle orbiter safety and mission critical items, and to ensure that ground rules allow these items to receive proper management visibility for risk assessment.

Documentation reviewed included both the Rockwell FMEA/CIL Desk Instructions 100-2G dated 31 January 1984, and the NASA Instructions for Preparation of FMEA/CIL for the STS, Basic, NSTS 22206 dated September, 1986. The Rockwell document has been used for years in the development of the orbiter FMEA/CIL baseline. NSTS 22206 was introduced recently to provide consistency in the approach and preparation of FMEA/CIL across the various NSTS project offices.

Assessment objectives were followed during the performance of the assessment without being influenced by external considerations such as effects on budget, schedule, and documentation growth. Assessment personnel were employed who had a strong reliability background but no previous space shuttle FMEA/CIL experience to ensure an independent assessment would be achieved. Highlights of the assessment are presented below.

NOT ALL ESSENTIAL ITEMS ARE IN THE CIL FOR MANAGEMENT VISIBILITY.

Existing automatic ground rules allow safety critical 1R/3 items to be excluded from the CIL. These items do not receive retention rationale, special attention, or direct Level II management visibility. Retention rationale provides for the documentation of critical item design, test, inspection, and failure history data needed for risk assessment. Inspection, test planning, and maintenance procedures ensure the integrity of the item. Upper-level visibility of all critical items is warranted to maintain awareness of safety and reliability issues.

GROUND RULES OMIT FMEA/CIL COVERAGE OF ITEMS THAT PERFORM CRITICAL FUNCTIONS.

Test ports, mechanical structures, wiring harnesses, and circuit protection devices do not receive adequate FMEA/CIL coverage. These items often perform critical functions that warrant FMEA/CIL identification of their contribution to safety risk. For example, critical failures related to test ports have played a major concern in space and commercial programs. An Eastern Airlines L-1011 aircraft experienced a complete three-engine flameout in flight as a result of leakage from three oil fill plugs. Of equal importance, wiring harnesses are exposed to operational wear, fatigue, and ground turnaround abuse that can cause latent critical failures. Experience shows that ground personnel can damage wiring during routine maintenance and inspection.

ESSENTIAL ITEMS EXCLUDED FROM THE CIL DO NOT RECEIVE DESIGN JUSTIFICATION.

The current ground rules allow some life-critical items to be excluded from the CIL. Design acceptability in the form of retention rationale is required for CIL listed items to determine, in a timely manner, if redesign is necessary or that the risk is acceptable. This design justification exclusion allows potentially high-risk life-essential items to remain unnoticed until operational impacts surface. A Level II awareness void is created through the absence of these life-essential items on the CIL.

FMEAs/CILs ARE NOT UPDATED IN A TIMELY MANNER.

Once the FMEAs and CILs are prepared, experience has shown that the contents eventually become obsolete. A low-risk item with good retention rationale can become a high-risk item as a result of changes and trends that do not get timely reassessment and resolution. Keeping FMEA/CIL data current will provide earlier Level II management awareness of risk changes resulting from design modifications, test and inspection changes, and failure trends.

In addition to the above issues, a number of other issues were identified that correct FMEA/CIL preparation instruction omissions and clarify ambiguities. The assessment was successful in that many of the issues have significant safety implications. Implementation of the recommendations presented in this report will ensure a safer and more reliable orbiter, as well as help meet both the letter and the intent of the Rogers Commission's recommendations.

2.0 INTRODUCTION:

The FMEA/CIL process is a systematic, methodical analysis performed to identify and document identified failure modes at prescribed hardware levels, and to specify the resultant effect of each failure mode on the subsystem, interfaces, mission, crew, and vehicle. The FMEA process requires a thorough and well-defined set of ground rules to guide the analyst in the identification of all potential critical failure modes that exist in the orbiter and Government Furnished Equipment (GFE). With proper management evaluation and resolution of the FMEA results, critical failure modes can either be eliminated or reduced by redesign and/or controls, or be accepted as an "acceptable risk". Items that qualify for the CIL, by virtue of their critical failure modes, are given special attention that is required of CIL items to ensure a safe and dependable orbiter. The CIL can be a powerful management tool if it is utilized as a single reference source and repository of all these kinds of data.

The assessment objectives of this study were to identify ground rule omissions and ambiguities that may impede the identification of orbiter safety and mission critical items and to ensure that, once identified, these items are given proper management visibility, evaluation, and resolution.

The FMEA/CIL ground rules assessment primarily examined the Rockwell Desk Instructions 100-2G, dated 31 January 1984. Rockwell reference documents were included in the review, with the exception of Engineering Operations Manuals (EOM's). Rockwell EOM's were not made available to the IOA contractor. The NASA Task Monitor reviewed the applicable sections and found no issues that would effect the assessment. No Rockwell documentation was reviewed that provided insight into the Rockwell FMEA/CIL management visibility, evaluation, and resolution process.

During the assessment, the Instructions for Preparation of FMEA/CIL for the STS, Basic, NSTS 22206, dated September 1986, was approved by the Program Requirements Control Board (PRCB). Review of the NSTS 22206 document was included as part of the assessment to determine if the Rockwell 100-2G assessment issues were resolved. The NASA document was a significant improvement over the Rockwell document both in scope and clarity of instructions.

3.0 ASSESSMENT RESULTS

The independent assessment was successfully accomplished in an objective and unbiased environment. Important issues were surfaced for enhancing the orbiter safety and reliability goals. Major issues are discussed in the text, and all issues are identified in the appendices, including recommendations. Appendix A presents the issues related to the Rockwell 100-2G ground rules and Appendix B pertains to the NSTS 22206 document. Appendix C presents the assessment issues in briefing chart form.

The following text discussion addresses the issues found in the review of both documents, except when noted, and a matrix is provided for issue traceability and impacts to reference documentation. Issues are segregated into Omissions, Ambiguities and Limited Visibility, Evaluation, and Resolution.

3.1 OMISSIONS

3.1.1 NOT ALL FUNCTIONALLY CRITICAL ITEMS ARE ON THE CIL

Automatic ground rules exist in both Rockwell 100-2G and NSTS 22206 which allow items that perform life and vehicle essential functions to be omitted from the CIL. Specifically, these are redundant items that perform critical functions but pass redundancy screens, and are defined as hardware criticality 3. Life/vehicle or mission essential items that are CIL excluded do not require retention rationale, and do not receive the same special attention and direct Level II visibility that CIL items receive.

Review of NHB 5300.4 (1D-2), page 3-2, item 1D301 3.C states:

Equipment appearing on the CIL will be given special attention in establishing hardware specifications and qualification requirements; in manufacturing, inspection and test planning; and in the formulation of operating and maintenance procedures and mission rules.

It therefore follows that the NASA intent is to give extra attention to items appearing on the CIL. If this indeed is NASA's intent, then Rockwell 100-2G and NSTS 22206 ground rules frustrate this aim by providing means for a functional criticality 1R or 2R item to escape appearing on the CIL. All hardware whose failure could directly lead to the destruction of

the vehicle or death of the crew should be on the Critical Items List and given extra attention. Any other interpretation places secondary considerations ahead of safety.

Allowing hardware to be excluded from the CIL as a result of redundancy or passing paperwork "screens" causes a void in the control/assessment process. Attention and controls during manufacturing, assembly, test, failure reporting, corrective action review, and flight readiness reviews are less effective when all hardware that performs critical functions is not considered, treated, or documented completely and consistently.

Based on the Presidential Commission Report's position on management awareness, it is recommended that all automatic ground rules for excluding functional criticality 1R and 2R items from the CIL be eliminated. If items are to be eliminated, they should be brought forward to the NSTS Program Level II Change Board for approval before they are dropped from further tracking.

3.1.2 ITEMS THAT PERFORM CRITICAL FUNCTIONS ARE EXCLUDED FROM FMEA/CIL COVERAGE.

Existing FMEA ground rules allow for certain hardware items and failure modes to be excluded from analysis requirements. NSTS 22206 is a significant improvement over Rockwell 100-2G, in reducing omissions, especially in the structures area. However, the NSTS 22206 rules still allow for less-than-desirable FMEA analysis in areas such as test ports, wire harnesses, connectors, and power interruption devices.

- a. Critical test ports related failures have played a major concern in Space and Commercial programs. An Eastern Airlines L-1011 experienced a flameout of all three engines as a result of leakage around the oil fill plugs. A Delta 86 rocket failure occurred, a probable cause being an oxidizer purge port plug failure. Rockwell 100-2G ruled out separate test port analyses and NSTS 22206 still does not flag their importance. It is recommended that an instruction be added to emphasize that capped and plugged test ports be analyzed individually, so that their contribution to critical failure modes is identified, and that their importance be adequately relayed to those agencies which handle maintenance.

- b. Wire harnesses, cables, and connectors carry critical commands, controls, and power functions throughout the orbiter. Except for verification that adjacent connector pin shorts do not result in loss of crew or vehicle, no FMEAs or additional analyses are required. These items are exposed to operational wear, fatigue, potential errors and ground turnaround abuse. Latent failures are of concern as a result of these conditions which could have critical consequences. It is therefore recommended that wire harnesses, cables, and connectors be analyzed to identify that they carry critical functions and be treated as CIL items if merited by criticality. In this way they will receive additional inspections and tests beyond those accomplished for similar items carrying nonessential functions.
- c. "Fails to operate" for fuses is specifically omitted by Rockwell 100-2G, and review of FMEA specific rules reveal that circuit breaker "failure to trip" was not considered in the Rockwell FMEAs. Neither did NSTS 22206 address circuit protection devices. The tendency of an analyst is to omit this failure mode from the analysis using the argument that a failure is necessary before the device is required, and the FMEA considers only one failure at a time. Circuit protection is a special item similar in concept to a safety or emergency item. It should be assumed the failure exists and the device must work. Circuit protection devices are sized to protect the downstream wiring and equipment. A failure to interrupt with a downstream failure could result in fire due to overheating of wiring and/or equipment. Another consequence is: if upstream circuit protection is sensitive to the problem, the upstream or main bus protection device will interrupt the circuit to isolate the failure. This main-bus loss will simultaneously interrupt power to many functions, which could have "lateral" system wide critical consequences. It is recommended that specific "fails to operate" instructions be added for circuit protection devices and be part of the FMEA analysis to flag the criticality and potential hazard of each device.

3.1.3 NOT ALL FUNCTIONALLY CRITICAL ITEMS REQUIRE FORMAL DISPOSITION AND RATIONALE (DESIGN JUSTIFICATION)

Design acceptability in the form of retention rationale is required for all items listed on the CIL. Inadequate retention rationale would make the critical item a redesign candidate. Good rationale showing that a critical item is of low risk would be grounds for a waiver and Level II acceptance.

Since retention rationale is of sufficient importance in determining high risk, it should be required and documented for all items that perform critical functions on the orbiter. Paragraphs 3.1.1 and 3.1.2 discuss those items that are not included on the CIL. These exclusions could allow a potential high risk life essential item to be excluded from NSTS Program Level II Change Board awareness. This is also additional rationale to support the recommendation that all 1R and 2R items be included on the CIL.

3.1.4 IN-FLIGHT TESTING IS NOT FORMALLY CROSS LINKED WITH CRITICAL ITEMS AS IS DONE WITH OMRSDs FOR GROUND TURNAROUND

No provisions exist in Rockwell 100-2G to ensure that FMEA/CIL identified failure modes are detected during ground turnaround. The Preliminary Draft of NSTS 22206 contained a provision to maintain an Operational Maintenance Requirements and Specification Document (OMRSD) matrix to track FMEA/CIL items in the OMRSD. Although the matrix was not adopted as part of the approved NSTS 22206, Basic version documentation, the matrix will be maintained as an independent entity and will make reference to the FMEA/CIL identified items.

In-flight verification of redundancy and the assurance that failure modes do not exist is at least as important as ground turnaround. Therefore, it is recommended that a matrix similar to the OMRSD matrix be adopted to provide tracability between in-flight checkout and critical items to provide an awareness by both the crew and the ground in advance of potential problems.

3.1.5 REDUNDANCY SCREENS ALLOW OMISSIONS

All 1R/3 and 2R/3 items are tested against three redundancy screens. These critical function items are not included in the CIL if they pass the screens.

Issues were identified related to all three screens.

- a. The first screen is: "The redundant elements are capable of checkout during the normal mission turnaround sequence."

"Capable of checkout" allows for conjecture on the part of the FMEA preparer. Provisions that are included in a design to provide checkout capability may never be used due to omission or later deletion of checkout procedures.

It is recommended that the words be changed to "elements are checked out" to assure the screen is passed.

- b. The second screen is: "Loss of a redundant element is readily detectable during flight."

"Readily detectable" does not assure safety of the crew or vehicle unless detection is accomplished in a timely manner.

No definition exists in Rockwell 100-2G to define "readily detectable." While NSTS 22206 does contain a definition, even that can be improved upon.

It is recommended that the following definition be adopted into both NSTS 22206 and Rockwell 100-2G.

"Readily detectable requires the capability of getting a crewmember to respond to a problem notification via real-time monitored displays, on-board alerts, visual indications or ground notification. Ground notification must not be considered unless sufficient time is available to perform corrective action to preclude the critical consequences of the failure, using worst case telemetry and data."

- c. The third screen is: "All redundant hardware items can be lost by a single credible cause or event such as contamination or explosion."

This screen does not consider fire as one of the single events or causes for failing this screen. Crew and vehicle safety are of prime concern and fire can cause loss of redundancy. Since the FMEA/CIL is a information source used to assure adequate safety visibility, it should identify all failure modes that result in potential ignition points and inadvertent fuel sources.

It is therefore recommended that a fourth screen be added to both Rockwell 100-2G and NSTS 22206 that states "Upon failure does this item provide ignition points and/or fuel to cause and/or support a fire?"

d. The "readily detectable" screen is not applicable to a select group of hardware items as defined in NSTS 22206. Included in this group are

1. Standby redundancy (redundant paths where only one path is in operation at a given time), and

2. Mechanical linkages.

Failed redundant elements that may be depended upon in the event of a primary item failure could have serious consequences if advanced knowledge of the failure is unknown. Contingency planning may be possible provided that the ground and/or crew are aware of the failure.

Unless periodic in-flight checkout is accomplished to verify the exempted items operational status, it is recommended that these item be considered to "fail" under the "readily detectable" screen and that this recommendation be adopted into both Rockwell 100-2G and NSTS 22206.

3.2 AMBIGUITIES

3.2.1 CRITICALITY DEFINITIONS ARE CONFUSING AND NEED SIMPLIFICATION

A dual system of criticality is used where an item is labeled with both a Functional Criticality and a Hardware Criticality. This criticality identification system allows many life/vehicle items to be simultaneously labeled with both a life/vehicle essential and a nonessential notation. This system is not only confusing, but it fogs the importance of the critical contribution of an item. To eliminate confusion and conflicting data, a more comprehensive singular system is recommended that eliminates hardware criticality and introduces the number of functional paths for completeness.

Examples: 1R(3) = Life or Vehicle essential, possessing three redundant paths

2R(3) = Mission essential, with three redundant paths

This method provides a more meaningful criticality identification without presenting conflicting information.

3.2.2 FMEA AND CIL FORMATS ARE NOT STANDARDIZED

The FMEA/CIL documentation for the STS was not standardized, nor was there any instructions to provide format standardization. Rockwell, Hamilton Standard, and SPAR all have different formats. Standardized formats would enhance the FMEA/CIL review process, even when specific NASA Project Offices and/or contractors are not required to fill in all data fields. Standardized formats for the FMEA and CIL should be incorporated into NSTS 22206 to ensure consistency and uniformity across the NSTS.

3.3 LIMITED VISIBILITY, EVALUATION, AND RESOLUTION OF CRITICAL ITEMS

3.3.1 LEVEL II CENTRAL SOURCE VISIBILITY OF CRITICAL FUNCTION ITEMS

Based on the Presidential Commission Report's position on management awareness, recommendations associated with issues presented in paragraphs 3.1.1, 3.1.2, and 3.1.3 should be adopted to assure that all items that perform critical functions are on the CIL, and that retention rationale is generated for those items. In this way, redundant designs with moderate-to-high retention risks that could otherwise slip through the system would get timely Program Level II attention.

Perhaps a Review Panel could be created with a SR&QA representative, a Program Level II representative, and an appropriate subsystem manager. The panel would assess CIL items and their retention rationale for program risk. Those items that are of low risk, meet proper redundancy levels, and pass redundancy screens would get Level II awareness but not require further detailed Level II review. The three member panel would provide necessary checks and bounds among safety, design, and administration.

The CIL should be the single management tool that flags safety and reliability risk changes by maintaining the retention rationale current to design, test, inspection, and failure history. (See paragraph 3.3.3 regarding retention rationale.) Elevation of risk as a result of status change should be used to trigger a higher level of visibility for Level II review.

3.3.2 CRITICAL FUNCTION ITEM EXCLUSION FROM THE CIL SHOULD BE APPROVED BY PROGRAM LEVEL II

The existing FMEA/CIL ground rules allow omissions to the CIL process as discussed in paragraphs 3.1.1, 3.1.2, 3.1.3 and 3.3.1. The resulting recommendations will provide greater Level II visibility to all items that perform critical functions.

Some critical function items that are a low risk, redundant, and mission critical will pass all screens, and will not be tracked on the CIL; therefore, the prerogative to remove those items from the CIL can be made by Level II on a item-by-item basis. In this way, Level II has control of the CIL without being deprived of full critical item awareness.

3.3.3 DATA IN THE FMEA AND CIL IS ALLOWED TO BECOME OBSOLETE

Once the FMEA and CIL are prepared, experience has shown that the contents are often not kept up to date. CIL retention rationale provides very important data that are used to justify designs and grant waivers. Allowing these data to become obsolete can allow a low-risk item with good retention rationale to become a high-risk item as a result of some seemingly minor changes or trends that do not get a FMEA/CIL reassessment. Retention Rationale as adopted by NSTS 22206 is as follows.

- a. Design - Identify design features which minimize the occurrence of the failure mode and causes.

Test - Identify specific tests accomplished to detect failure modes and causes during acceptance tests, certification test, and checkout tests.

Inspection - Note that specific inspection points are used to determine that specific failure mode causes are not inadvertently manufactured into the hardware. Note inspection requirements in mission turnaround relative to

- d. History - Provide an indication that the hardware or software has been used successfully and that a history of generic failures is not developing. If the hardware is new to this program, so state.

- e. Operations - Describe operational effect of the hardware failure and actions which may be taken by the crew following the failure, crew training which could minimize the effect of the hardware failure, and mission constraints which are imposed to minimize the effect of the hardware failure. Include in-flight checkout procedures performed which prevent improper operation/loss of redundancy.

Rockwell 100-2G requires retention rationale with the exception of item "e".

It is recommended that the FMEA and CIL, including the five retention rationale items, be maintained under active control to assure updates to these entries are kept current with any approved design, test, and inspection changes, new failure history, or operational use.

In this way, a FMEA/CIL re-assessment will prevent potential safety and reliability degradation to the shuttle orbiter as a result of changes.

3.4 ISSUE IMPACT MATRIX

This FMEA/CIL Ground Rules Assessment has identified issues that can effect several requirement and instructional documents. An impact matrix is presented in Table 1 to identify these issues, and to identify those documents that are impacted as a result of each recommendation. The documents identified in the impact matrix are NHB 5300-4 (1D-2), JSC 0770 Volume V, JSC 0770 Volume X, Rockwell 100-2G, and NSTS 22206 (September 86).

Since the issues were basic to Rockwell Desk Instructions 100-2G and NSTS 22206, all issues effected these documents. However, since NHB 5300.4 and JSC 07700 deal with higher level requirements, a much lesser level of impact was incurred on them.

TABLE 1 - FMEA/CIL ASSESSMENT ISSUE IMPACTS

ASSESSMENT ISSUE	NHB 5300.4 (1D-2)	JSC 07700 VOL V	JSC 07700 VOL X	RI DESK INST 100-2G	NSTS 22206, BASIC
CIL AUTOMATIC EXCLUSIONS (LIMITED VISIBILITY)	IMPACT (1D301 #3.B)	N/A	N/A	IMPACT	IMPACT
FUNCTIONAL/HARDWARE CRITICALITY (CONFUSION)	N/A	N/A	N/A	IMPACT	IMPACT
DELETE HARDWARE CRITICALITY ADD FUNCTIONAL PATHS	N/A	N/A	N/A	IMPACT	IMPACT
KEEP RETENTION RATIONALE UP TO DATE	N/A	IMPACT (TABLE 4.15,#9)	N/A	IMPACT	IMPACT
CLARIFY RETENTION RATIONALE TESTS - CHECKOUT	N/A	IMPACT (TABLE 4.15,#9)	N/A	IMPACT	IMPACT
INFLIGHT TEST VERIFICATION MATRIX	N/A	N/A	N/A	IMPACT	IMPACT
FIRM UP REDUNDANCY SCREENS	IMPACT (1D301 #3)	IMPACT (TABLE 4.14,#12)	IMPACT (3.5.1.1.2)	IMPACT	IMPACT
REVISE REDUNDANCY SCREEN EXCLUSIONS AND "FAIL" CRITERIA	N/A	N/A	IMPACT (3.5.1.1.2)	IMPACT	IMPACT
PROVIDE A FIRE RELATED REDUNDANCY SCREEN	IMPACT (1D301 #3)	N/A	IMPACT (3.5.1.1.4)	IMPACT	IMPACT
INCLUDE FMEA EXCLUDED ITEMS AND FAILURE MODES	N/A	N/A	N/A	IMPACT	IMPACT
STANDARD FMEA/CIL FORMAT	N/A	N/A	N/A	IMPACT	IMPACT

LEGEND: IMPACT - CHANGE REQUIRED
N/A - NOT ADDRESSED

4.0 REFERENCES

1. Rockwell Reliability Desk Instructions (Flight Hardware FMEA/CIL) No. 100-2G, dated January 31, 1984.
2. NASA Instructions for Preparation of FMEA/CIL for the STS, Basic, NSTS 22206, dated September 1986.
3. NASA Instructions for Preparation of FMEA/CIL for the STS, Basic, Preliminary Draft, JSC 22206, dated June 1986.
4. NASA Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program, NHB 5300-4 (1D-2), dated October 1979.
5. JSC 07700, Volume V, Information Requirements Descriptions, dated September 30, 1983.
6. JSC 07700, Volume X, Space Shuttle Flight and Ground System Specification, dated September 30, 1983.

Appendix A

Rockwell 100-2G Assessment Issues

1. Reference: RI, 100-2G, Figure 10.

Instructions: Figure 10, Attached.

Problem: This figure is the road map for defining which orbiter items appear on the CIL. Two criticality categories are used: functional (which does not consider redundancy) and hardware (considers redundancy). Items that perform critical functions, but meet defined redundancy levels, and pass screens and are excluded from the Critical Items List (CIL). Exclusion creates a void in the control/assessment process. Attention and controls during manufacturing, assembly, test, failure reporting, corrective action review, and flight readiness reviews are less effective when all hardware that perform critical functions is not considered or treated. As a result, potential problems (latent manufacturing/design defects) with hardware may slip through the assessment process without management knowing the seriousness of the effects of failure.

Recommendation: Based on the Presidential Commission Report's position on management awareness, it is our recommendation that all automatic ground rules for excluding functional criticality 1R or 2R items from the CIL be eliminated and that, if items are to be eliminated, they be brought forward to the NSTS Program Level II change board for approval. In support of this position, it is recommended that the figure be replaced with a new figure shown as "Streamlined". Hardware criticality, in Rockwell 100-2G Figure 10, is replaced with a notation showing how many paths are available to accomplish the critical function.

CRITICALITY CATEGORY
CROSS REFERENCE TABLE



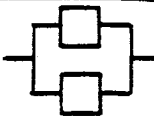
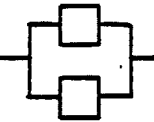
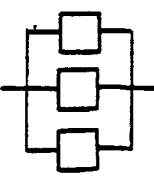
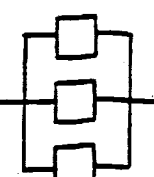


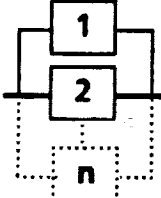
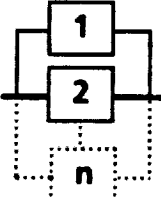
FUNCTION / LEVEL OF REDUNDANCY	BLOCK DIAGRAM	CRITICALITY CATEGORY	
		FUNCTIONAL DEFINITIONS	HARDWARE DEFINITIONS
LIFE OR VEHICLE ESSENTIAL / NO REDUNDANCY		1 (CIL)	1 (CIL)
MISSION ESSENTIAL / NO REDUNDANCY		2 (CIL)	2 (CIL)
LIFE OR VEHICLE ESSENTIAL / DUAL REDUNDANCY		1R (CIL)	2 (CIL)
MISSION ESSENTIAL / DUAL REDUNDANCY		PASSED SCREEN 2R	FAILED SCREEN 2R (CIL)
LIFE OR VEHICLE ESSENTIAL / TRIPLE REDUNDANCY		1R	1R (CIL)
MISSION ESSENTIAL / TRIPLE REDUNDANCY		2R	2R (CIL)
ALL NON-ESSENTIAL / ALL LEVELS OF REDUNDANCY		3	3

FIGURE 10

THESE LIFE AND MISSION
ESSENTIAL ITEMS ARE
EXCLUDED FROM THE CIL

Figure 1 - Rockwell 100-2G, Figure 10

"STREAMLINED" **CRITICALITY CATEGORY CROSS REFERENCE TABLE**

FUNCTION / LEVEL OF REDUNDANCY	BLOCK DIAGRAM	CRITICALITY CATEGORY DEFINITIONS
LIFE OR VEHICLE ESSENTIAL / NO REDUNDANCY		1 CIL
MISSION ESSENTIAL / NO REDUNDANCY		2 CIL
LIFE OR VEHICLE ESSENTIAL / DUAL (OR GREATER) REDUNDANCY		1R (n) CIL
MISSION ESSENTIAL / DUAL (OR GREATER) REDUNDANCY		2R (n) CIL
ALL NON-ESSENTIAL / ALL LEVELS OF REDUNDANCY		3

R - FUNCTIONAL REDUNDANCY AVAILABLE
n - NUMBER OF FUNCTIONAL PATHS (LIKE AND UNLIKE)
CIL - DENOTES THAT ITEM IS ON CRITICAL ITEMS LIST

Figure 2 - Streamlined Criticality Category Cross Reference

2. Reference: RI 100-2G; paragraph 3.3; item 9.
- Instructions: "FMEAs will not be required on structures, wire harnesses, cables, and electrical connectors."
- Problem: The orbiter, being a reusable craft, is exposed to repeated usage stress, maintenance, and handling. As a result, fatigue, wear, and potential errors may result in compromise to equipment, including those items that have been excluded from FMEA/CIL requirements. This allows potential critical failure modes to be overlooked and critical hardware that deserves CIL status not to be monitored. Structures with sealing surfaces or other functions that are an integral part of the hardware function, and harnesses and connectors with inter-pin or inter-wire shorts that cause critical inadvertent commands are examples.
- Recommendation: Do a FMEA to identify critical functions of structures, wire harnesses, cables, and electrical connectors. Track critical function hardware on CIL.
3. Reference: RI 100-2G; Appendix B, paragraph 3.1.2, item 10.
Specific Ground Rules and Criteria
o STS 82-0028, para. 3.2, item 3.
o STS 82-0033, para. 3.2, item 3.
- Instructions: "The failure mode 'Fails to Operate' will not be addressed for fuses."
- Problem: Instructions exclude "Fails to Operate" only for fuses, however Specific Ground Rules and Criteria also exclude circuit breakers from the reference STS 82 FMEA's. Fuses and circuit breakers are used to protect downstream wiring and equipment from excessive current. A real hazard exists if significantly higher-than-rated value devices are installed, or if circuit breakers fail-to-trip. Potential fire or ignition sources will exist as a result of a failure of the item(s) being protected.
- Recommendation: Include "Fails to Operate" as a failure mode for fuses and circuit breakers to flag the criticality and potential hazard in the analysis.

4. Reference: RI 100-2G, paragraph 4.2.21, item 5.

Instructions: "Do not consider fire as one of the single events or causes in failing Screen 'C'."

Problem: The FMEA should provide a complete listing of potential ignition points and inadvertent fuel sources to assure adequate safety visibility. Failure to identify these sources may allow less than adequate separation features to be approved.

Recommendation: Add a Screen "D": "Upon failure, does this item provide ignition points and/or fuel to cause and/or support a fire?"

5. Reference: RI 100-2G, paragraph 4.3.1, item 2.

Instructions: "Test ports, when capped, shall be treated as a structural part of the component and not be considered further."

Problem: The rule allows test ports, when capped (plugs also assumed), to be excluded from the FMEA. This allows an area of potential critical consequences to be overlooked as a result of procedure error or cap/plug failure. Examples include: the test ports between the SRB redundant seals, which were considered as a potential failure point early in the Challenger investigation; and the Delta 86 flight failure, where an oxidizer purge port plug was one of two most probable causes of failure.

Recommendation: Include capped and plugged test ports in the analysis so that individual contributions to critical failure modes will be evaluated.

6. Reference: RI 100-2G; paragraph 4.1.24

Instructions: "CIL Retention Rationale

- a. Design -- Identification of design features which minimize the occurrence of the failure mode and causes.
- b. Test -- Identification of specific tests accomplished to detect failure mode and causes during acceptance tests, certification tests, and checkout tests.
- c. Inspection -- Statement that specific inspection points are included to determine that specific failure mode causes are not inadvertently manufactured into the hardware.
- d. Failure history -- Provide an indication that the hardware or similar hardware has been used successfully and that a history of generic failures does not exist. If the hardware is new to this program, so state."

Problem: This retention rationale, after being generated by the FMEA/CIL, becomes obsolete unless the FMEA/CIL are living documents. Experience has shown that this type of data is frequently not kept up to date.

Category 1R and 2R items that pass redundancy screens or are N/A are excluded from the Retention and Rationale. High risk items (e.g., those that might have marginal designs, be sensitive to handling, environments, test damage, etc.) do not get the attention and controls that they deserve. This rationale is too generic and does not reflect orbiter experience.

Recommendation: Do not exclude 1R and 2R items from Disposition and Rationale unless reviewed and approved by Level II.

Maintain the FMEA/CIL under formal documentation control to assure it is kept current and it reflects future changes that affect the analysis results and critical item determinations.

Include flight tests as well as ground tests under item b.

Provide and maintain an updated failure history based on C/O, in-flight, and post-flight problem discoveries (i.e., seal erosion was noted to be occurring on several flights prior to 51L). Trends that may influence the FMEA should be used to update the analysis and be identified in the control/assessment process.

7. Reference: RI 100-2G; paragraph 4.1.24

Instructions: "CIL Retention Rationale
Failure history - provide an indication that the hardware or similar hardware has been used successfully and that a history of generic failure does not exist. If the hardware is new to this program, so state."

Problem: Rationale is too general and does not specifically require program experience.

Recommendation: Rewrite -- "Failure history -- provide data to support that the hardware or similar hardware has been used successfully and provide any failure history that does exist. As program experience is gained, update this data. If the hardware is new to the program, so state."

8. Reference: RI 100-2G; paragraph 4.1.21

Instructions: "Redundancy Screens
o The redundant elements are not capable of checkout during the normal mission turnaround sequence.
o Loss of a redundant element is not readily detectable by the flight crew.
o All redundant elements can be lost by a single credible cause or event such as contamination or explosion."

Problem: The first screen allows elements to pass if only capable of checkout. Capability may show good intentions but does not assure actual checkout. The second screen specifies "readily detectable." This does not assure detection if detection provisions can be re-programmed or overridden. The third screen excludes fire, which is as credible as contamination or explosion.

Recommendation: Passing the first screen should require actual, verifiable checkout procedures supported by a requirement. Passing the second screen should also require actual and verifiable indications that cannot be procedurally deleted if the indication is not hardwired or part of a caution and warning or alarm system. The term "readily detectable" should be defined as follows:

Readily detectable requires the capability of getting a crew member to respond to a problem notification via real-time monitored displays, on-board alerts, visual indications or ground notification. Ground notification must not be considered unless sufficient time is available to perform corrective action to preclude the critical consequences of the failure, using worst case telemetry and data.

Add a fourth Screen "D": "Upon failure, does this item provide ignition points and/or fuel to cause and/or support a fire?"

9. Reference: RI 100-2G, None

Instructions: None (Omission)

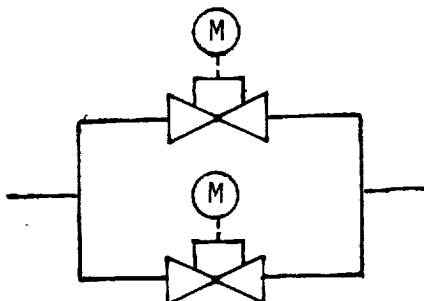
Problem: No provisions exist in Rockwell 100-2G to assure that FMEA/CIL identified failure modes are detected during ground turnaround. The Preliminary Draft of NSTS 22206 contained a provision to maintain a OMRSD matrix to track FMEA/CIL items against the OMRSD. Although the matrix was not adopted as part of the approved NSTS 22206, Basic, it will be maintained as an independent entity and will make reference to the FMEA/CIL identified items. In-flight verification of redundancy and the assurance that failure modes do not exist is at least as important as ground turnaround.

Recommendation: It is recommended that a matrix similar to the OMRSD matrix be adopted to provide tracability between in-flight checkout and critical items, to provide an awareness by both the crew and the ground in advance of potential problems.

10. Reference: RI 100-2G; paragraph 3.3, Appendix B, paragraph 3.1.1, item 13a.
- Instructions: "Hazards associated with the loss of fluid in excess of requirements will be documented and covered by hazard analysis, but will not affect criticality."
- Problem: By not effecting criticality under described conditions, a void exists in the CIL related to items that can propagate hazards. Release of fluids in excess of requirements that are the result of credible failure modes and pose a flammability hazard could effect criticality.
- Recommendation: Rewrite to include: "Where released fluids are flammable or oxidizers and the possibility of an ignition source exist as a result of released fluids, the worst-case criticality should be noted and the appropriate notations entered under "HAZARDS" for Safety action."
11. Reference: RI 100-2G; paragraph 3.3, item 10.
- Instructions: "Logic diagrams (Desk Instruction 100-1, Reliability Evaluation) will be developed only where required to provide proper correlation between schematics and FMEAs."
- Problem: Logic diagrams in Reference 100-1 are success oriented (See Example). This appears to be a useful procedure to understand the items under analysis. However, no coverage is given to negative aspects of getting inadvertent actions. The occurrence of an undesired event can sometimes be worse than no event. It should be noted, however, that RI 100-2G does list inadvertent operation as a failure mode.
- Recommendation: Add to Rockwell 100-1: instructions: "conduct negative logic as well as success logic so that visibility will be provided for the effects of inadvertent actions."

11. (Continued)

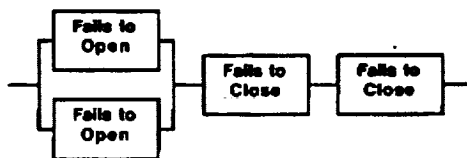
Example: Two parallel motor controlled valves:



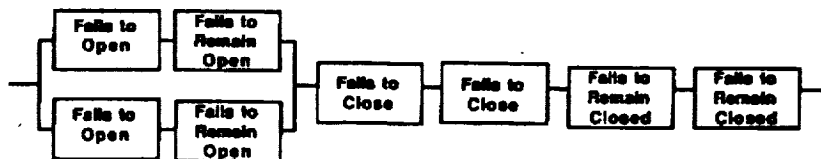
Logic diagram:

Spurious commands due to software/equipment failure or human error could result in a valve failing to remain closed after normal closure had been accomplished and verified.

Rockwell 100-1 diagram:



More complete logic diagram:



12. Reference: RI 100-2G, paragraph 4.6.

Instructions: "...NASA will...perform FMEAs...NASA will provide Rockwell with a copy...Rockwell will evaluate the interface effects on the Orbiter.

The accountability of CIL items for GFE will be to NASA. Those CIL items resulting from interface failure modes will be a part of the Rockwell CIL."

Problem: Are the GFE and CFE FMEAs performed to the same rules as the Orbiter? What are the rules, exceptions, etc.?

Recommendation: Consistent format and ground rules should be followed by all so they can be properly integrated, and any unique requirements documented.

13. Reference: RI 100-2G, Appendix B; paragraph 3.1.1, item 2.

Instructions: "Criticality 1R and 2R assumes failure of all like and unlike redundancy: A backup item, if when it is called upon to work, performs a function different from the item it is backing up, should be classified based upon the effect if it does not work when operated. If the backup item performs the same function as the item it is backing up, the backup should be classified as an unlike redundant item."

Problem: The instruction is not clear. Is the instruction telling the analyst to classify the backup item with the criticality of the primary system function when the item is called upon to operate as a backup? The final sentence seems to be in error. If a backup item performs the same function as the item it is backing up, it could be like redundant, not unlike.

Recommendation: Rewrite item 2 as follows:
Criticality 1R and 2R considers both like and unlike redundancy. Like redundancy is backup redundant hardware of the same type that performs the same function. Unlike redundancy is alternate hardware performing a primary function; however, if called upon, it can be used to support a function different from its primary assignment. An alternate item, when it is called upon to support a function different than its primary assignment, should be assigned criticality categories commensurate with both its primary and alternate functions, and the FMEA should indicate both roles and potential effects. The worst case criticality should be the primary criticality listing and the second criticality, if lower, should be discussed in the effects statement.

14. Reference: RI 100-2G, Appendix B; paragraph 3.1.1, 13c.
- Instructions: "Where external or internal leak paths are protected by static or dynamic redundant (verifiable) seals, the leak path effect will be reduced by one criticality level."
- Problem: The reduction by one criticality level creates the potential to propagate misleading information regarding designs when FMEA summaries and CIL data are generated.
- Recommendation: Seals and leak paths should reflect worst-case criticality with redundancy levels provided in the analysis and retention rationale.
15. Reference: RI 100-2G, paragraph 3.3, item 9.
- Instructions: "Separation of redundant functions will be verified by selective review of design schematics to ensure that the requirements for separation have been incorporated and complied with."
- Problem: Design schematics may be inadequate to reveal spatial relations.

Recommendation: Use hardware "as-built" drawings and mockups to recognize spatial relations that could reveal the credibility of potential failure modes and validate separation of redundant paths (JSCM 8080, Standard No. 4).

Appendix B

NSTS 22206, Basic, Assessment Issues

1. Reference: NSTS 22206, Figure 1.

Instructions: Figure 1 Attached

Problem: This figure is a logic road map for defining which orbiter items appear on the CIL. Two criticality categories are used: functional (which does not consider redundancy) and hardware (considers redundancy). Items that perform critical functions, but meet defined redundancy levels, and pass screens and are excluded from the Critical Items List (CIL). This exclusion creates a void in the control/assessment process. Attention and controls during manufacturing, assembly, test, failure reporting, corrective action review, and flight readiness reviews are less effective when all hardware that performs critical functions is not considered or treated. As a result, potential problems (latent manufacturing/design defects) with hardware may slip through the assessment process without management knowing the seriousness of the effects of failure.

Recommendation: Based on the Presidential Commission Report's position on management awareness, it is our recommendation that all automatic ground rules for excluding functional criticality 1R or 2R items from the CIL be eliminated and that, if items are to be eliminated, they be brought forward to the NSTS Program Level II change board for approval. In support of this position, it is recommended that the figure be replaced with a new figure shown as "Streamlined" replacement. Hardware criticality, in NSTS 22206 Figure 1, is replaced with a notation showing how many paths are available to accomplish the critical function.

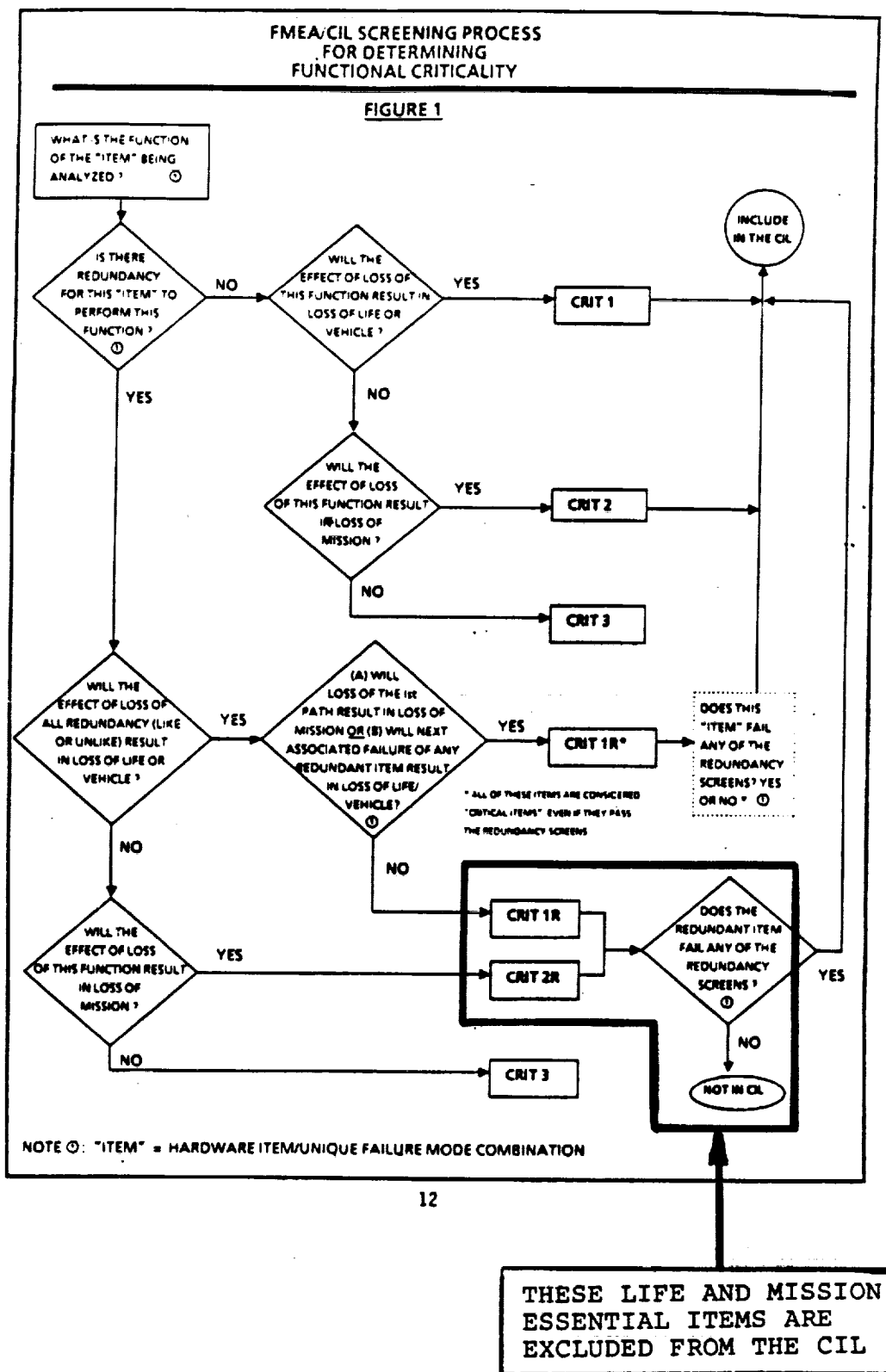


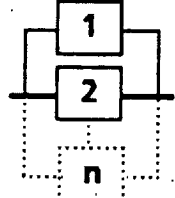
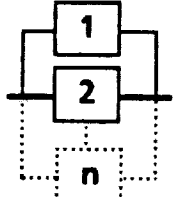


Figure 3 - NSTS 22206 (Figure 1) FMEA/CIL Screening Process

"STREAMLINED"
CRITICALITY CATEGORY CROSS REFERENCE TABLE

FUNCTION / LEVEL OF REDUNDANCY	BLOCK DIAGRAM	CRITICALITY CATEGORY DEFINITIONS
LIFE OR VEHICLE ESSENTIAL / NO REDUNDANCY		1 CIL
MISSION ESSENTIAL / NO REDUNDANCY		2 CIL
LIFE OR VEHICLE ESSENTIAL / DUAL (OR GREATER) REDUNDANCY		1R (n) CIL
MISSION ESSENTIAL / DUAL (OR GREATER) REDUNDANCY		2R (n) CIL
ALL NON-ESSENTIAL / ALL LEVELS OF REDUNDANCY		3

R - FUNCTIONAL REDUNDANCY AVAILABLE
n - NUMBER OF FUNCTIONAL PATHS (LIKE AND UNLIKE)
CIL - DENOTES THAT ITEM IS ON CRITICAL ITEMS LIST

Figure 4 - Streamlined Criticality Category Cross Reference

2. Reference: NSTS 22206, paragraph 2.3.1, item e.
- Instructions: "FMEAs are not required on wire harnesses, cables, and electrical connectors."
- Problem: The orbiter, being a reusable craft, is exposed to repeated usage stress, maintenance, and handling. As a result, fatigue, wear, and potential errors may result in compromise to equipment, including those items that have been excluded from FMEA/CIL requirements. This allows potential critical failure modes to be overlooked and critical hardware that deserves CIL status not to be monitored. Structures with sealing surfaces or other functions that are an integral part of the hardware function, and harnesses and connectors with inter-pin or interwire shorts that cause critical inadvertent commands are examples.
- Recommendation: Do a FMEA to identify critical functions of structures, wire harnesses, cables, and electrical connectors. Track critical function hardware on CIL.
3. Reference: NSTS 22206, paragraph 2.3.4, item (3).
- Instructions: "Does not consider fire as one of the single events or causes in failing Screen 'C'."
- Problem: The FMEA should provide a complete listing of potential ignition points and inadvertent fuel sources to assure adequate safety visibility. Failure to identify these sources may allow less than adequate separation features to be approved.
- Recommendation: Add a Screen "D": "Upon failure, does this item provide ignition points and/or fuel to cause and/or support a fire?"

4. Reference: NSTS 22206, paragraph 2.3.3, item 1.

Instructions: "The criticality of instrumentation and test ports shall be assessed according to their function. Where instrumentation (e.g., pressure transducer penetrates the wall of a component or line and structural failure of the joint would result in gross leakage, the failure mode shall be considered as a failure of the component or line. The criticality of the instrumentation, therefore, would not be affected in such instances."

Problem: The instruction does not strongly emphasize the importance of test ports. Critical test ports related failures have played a major concern in Space and Commercial programs. An Eastern Airlines L-1011 experienced a flameout of all three engines as a result of leakage around the oil fill plugs. A Delta 86 rocket failure occurred, a probable cause being an oxidizer purge port plug failure.

Recommendation: Provide a separate instruction to include capped and plugged test ports in the analysis so that individual contributions to critical failure modes will be evaluated.

5. Reference: NSTS 22206, Table 4, Number 10, items a,b,c,d.

Instructions: "CIL Retention Rationale

- a. Design -- Identification of design features which minimize the occurrence of the failure mode and causes.
- b. Test -- Identification of specific tests accomplished to detect failure mode and causes during acceptance tests, certification tests, and checkout tests.
- c. Inspection -- Statement that specific inspection points are included to determine that specific failure mode causes are not inadvertently manufactured into the hardware.
- d. Failure history -- Provide an indication that the hardware or similar hardware has been used successfully and that a history of generic failures does not exist. If the hardware is new to this program, so state."

Problem: This retention rationale, after being generated by the FMEA/CIL, becomes obsolete unless the FMEA/CIL are living documents. Experience has shown that this type of data is frequently not kept up to date.

Category 1R and 2R items that pass redundancy screens or are N/A are excluded from the Retention and Rationale. High risk items (e.g., those that might have marginal designs, be sensitive to handling, environments, test damage, etc.) do not get the attention and controls that they deserve. This rationale is too generic and does not reflect orbiter experience.

Recommendation: Do not exclude 1R and 2R items from Disposition and Rationale unless reviewed and approved by Level II.

Maintain the FMEA/CIL under formal documentation control to assure it is kept current and it reflects future changes that affect the analysis results and critical item determinations.

Include flight tests as well as ground tests under item b.

Provide and maintain an updated failure history based on C/O, in-flight, and post-flight problem discoveries (i.e., seal erosion was noted to be occurring on several flights prior to 51-L). Trends that may influence the FMEA should be used to update the analysis and be identified in the control/assessment process.

6. Reference: NSTS 22206, Table 13, item 14.

Instructions: "Redundancy Screens

- o The redundant elements are not capable of checkout during the normal mission turnaround sequence.
- o Loss of a redundant element is not readily detectable by the flight crew.
- o All redundant elements can be lost by a single credible cause or event such as contamination or explosion."

Problem: The first screen allows elements to pass if only capable of checkout. Capability may show good intentions but does not assure actual checkout. The second screen specifies "readily detectable." This does not assure detection if detection provisions can be re-programmed or overridden. The third screen excludes fire, which is as credible as contamination or explosion.

Recommendation: Passing the first screen should require actual, verifiable checkout procedures supported by a requirement. Passing the second screen should also require actual and verifiable indications that cannot be procedurally deleted if the indication is not hardwired or part of a caution and warning or alarm system. The term "readily detectable" should be defined as follows:

Readily detectable requires the capability of getting a crew member to respond to a problem notification via real-time monitored displays, on-board alerts, visual indications or ground notification. Ground notification must not be considered unless sufficient time is available to perform corrective action to preclude the critical consequences of the failure, using worst case telemetry and data.

Add a fourth Screen "D": "Upon failure, does this item provide ignition points and/or fuel to cause and/or support a fire."

7. **Reference:** NSTS 22206

Instructions: None (Omission)

Problem: The Preliminary Draft of NSTS 22206 contained a provision to maintain a OMRSD matrix to track FMEA/CIL items against the OMRSD. Although the matrix was not adopted as part of the approved FMEA/CIL NSTS 22206, Basic version documentation, it will be maintained as an independent entity and will make reference to the FMEA/CIL identification items. In-flight verification of redundancy and the assurance that failure modes do not exist is at least as important as ground turnaround.

Recommendation: It is recommended that a matrix similar to the OMRSD matrix be adopted to provide tracability between in-flight checkout and critical items, to provide an awareness to both the crew and the ground in advance of potential problems.

8. Reference: NSTS 22206, paragraph 1.3, item d.

Instructions: Devise the analysis worksheet and complete for every identified failure mode.

Problem: The FMEA/CIL documentation for the STS were not standardized nor were there any instructions to provide format standardization. Rockwell, Hamilton Standard, and SPAR all had different formats. Standardized formats would enhance the FMEA/CIL review process, even when specific NASA Project Offices and/or contractors are not required to fill in all data fields.

Recommendation: Standardized formats for the FMEA and CIL should be incorporated into NSTS 22206 to ensure consistency and uniformity across the NSTS.

9. Reference: NSTS 22206

Instructions: None (Omission)

Problem: "Fails to operate" for fuses is specifically omitted by Rockwell 100-2G and review of FMEA specific rules reveal that circuit breaker "failure to trip" when required was not considered in the Rockwell FMEAs. NSTS 22206 did not address circuit protection devices. The tendency of an analyst is to omit this failure mode from the analysis using the argument that a failure is necessary before the device is required, and the FMEA considers only one failure at a time. Circuit protection is a special item similar in concept to a safety or emergency item. It should be assumed that the failure exists and the device must work. Circuit protection devices are sized to protect the downstream wiring and equipment. Failure to interrupt, upon downstream failure, could result in fire due to overheat of wiring and/or equipment. Another consequence is that, if upstream circuit protection is sensitive to the

problem, the upstream or main bus protection device will interrupt the circuit to isolate the failure. This main bus loss will interrupt power to many functions simultaneously, and could have wide spread lateral systemic critical consequences.

Recommendation: Provide specific instructions to consider the "Fails to Operate" failure mode for circuit protection devices and require that each device be identified as to its criticality and potential hazard.

10. Reference: NSTS 22206, 2.3.3, item j.

Instructions: "When worst case effect of a specific failure mode results in a launch delay, the criticality shall be classified as criticality 3. Other prelaunch failure modes shall be classified according to their worst case effect."

Problem: Ground rules exclude launch delays that impact worst-case missions which have specific launch window(s) and/or few launch opportunities to accomplish a specific mission.

Recommendation: Prelaunch failure modes that result in a launch delay shall be classified with the appropriate criticality.

Appendix C

Independent Orbiter Assessment

FMEA/CIL Instructions and Ground Rules Briefing,
Presented to the STS Orbiter and GFE Projects Office/R.A. Colonna
on 22 September 1986.

INDEPENDENT ORBITER ASSESSMENT

FMEA/CIL INSTRUCTIONS AND GROUND RULES

PERFORMED BY

MCDONNELL DOUGLAS ASTRONAUTICS COMPANY

PRESENTED BY

S. T. TRAVES

STAFF MANAGER, RELIABILITY

MDAC-HB

MDAC-HOUSTON

MCDONNELL DOUGLAS

CORPORATION

22 SEPTEMBER 1986



AGENDA

- OBJECTIVES
- DOCUMENTS REVIEWED
- ASSESSMENT HIGHLIGHTS
- DETAILED ASSESSMENTS
- SUMMARY

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS



CORPORATION

ASSESSMENT OBJECTIVES

- IDENTIFY OMISSIONS AND/OR AMBIGUITIES THAT MAY IMPEDE CRITICAL ITEM IDENTIFICATION
- ENSURE THAT CRITICAL ITEMS ARE GIVEN PROPER VISIBILITY, EVALUATION, AND RESOLUTION

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION



DOCUMENTATION REVIEWED

- ROCKWELL 100-2G, FLIGHT HARDWARE FMEA/CIL
DESK INSTRUCTIONS, DATED 31 JANUARY 1984
- NSTS 22206, INSTRUCTIONS FOR PREPARATION OF
FMEA/CIL FOR THE STS, BASIC, DATED SEPTEMBER
1986

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS



CORPORATION

ASSESSMENT HIGHLIGHTS

- FMEA/CIL DOCUMENTATION FORMATS ARE NOT STANDARDIZED
- DUAL CRITICALITY DEFINITION SYSTEMS COMPLICATE FMEA/CIL PROCESS
- GROUND RULES OMIT ANALYSES OF FAILURES ON SELECTED ITEMS
- NOT ALL ESSENTIAL ITEMS ARE IN THE CIL FOR MANAGEMENT VISIBILITY
- ESSENTIAL ITEMS NOT IN THE CIL RECEIVE NO DESIGN JUSTIFICATION
- FMEAs/CILs ARE NOT UPDATED IN A TIMELY MANNER

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION

DETAILED ASSESSMENTS

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS



CORPORATION

REDUNDANCY SCREENS LIMIT VISIBILITY

INSTRUCTION: CRITICALITY CATEGORY CROSS REFERENCE TABLE

PROBLEM: • AUTOMATIC GROUND RULES ALLOW CRITICALITY CATEGORY 1R/3 AND 2R/3 ITEMS TO BE EXCLUDED FROM THE CIL

- EXCLUDED ITEMS DO NOT REQUIRE RETENTION RATIONALE
- SOME CRITICAL FAILURE MODES ARE NOT REPORTED TO LEVEL II

RECOMMENDATION: ELIMINATE AUTOMATIC GROUND RULES THAT EXCLUDE 1R/3 AND 2R/3 ITEMS FROM THE CIL

(REFERENCE) RI, 100-2G, FIGURE 10; NSTS 22206, FIGURE 1

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION

CRITICALITY CATEGORY
CROSS REFERENCE TABLE



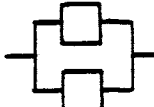
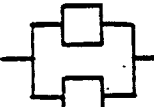
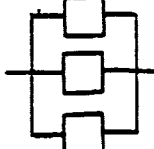
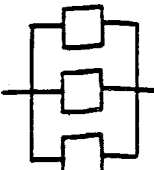
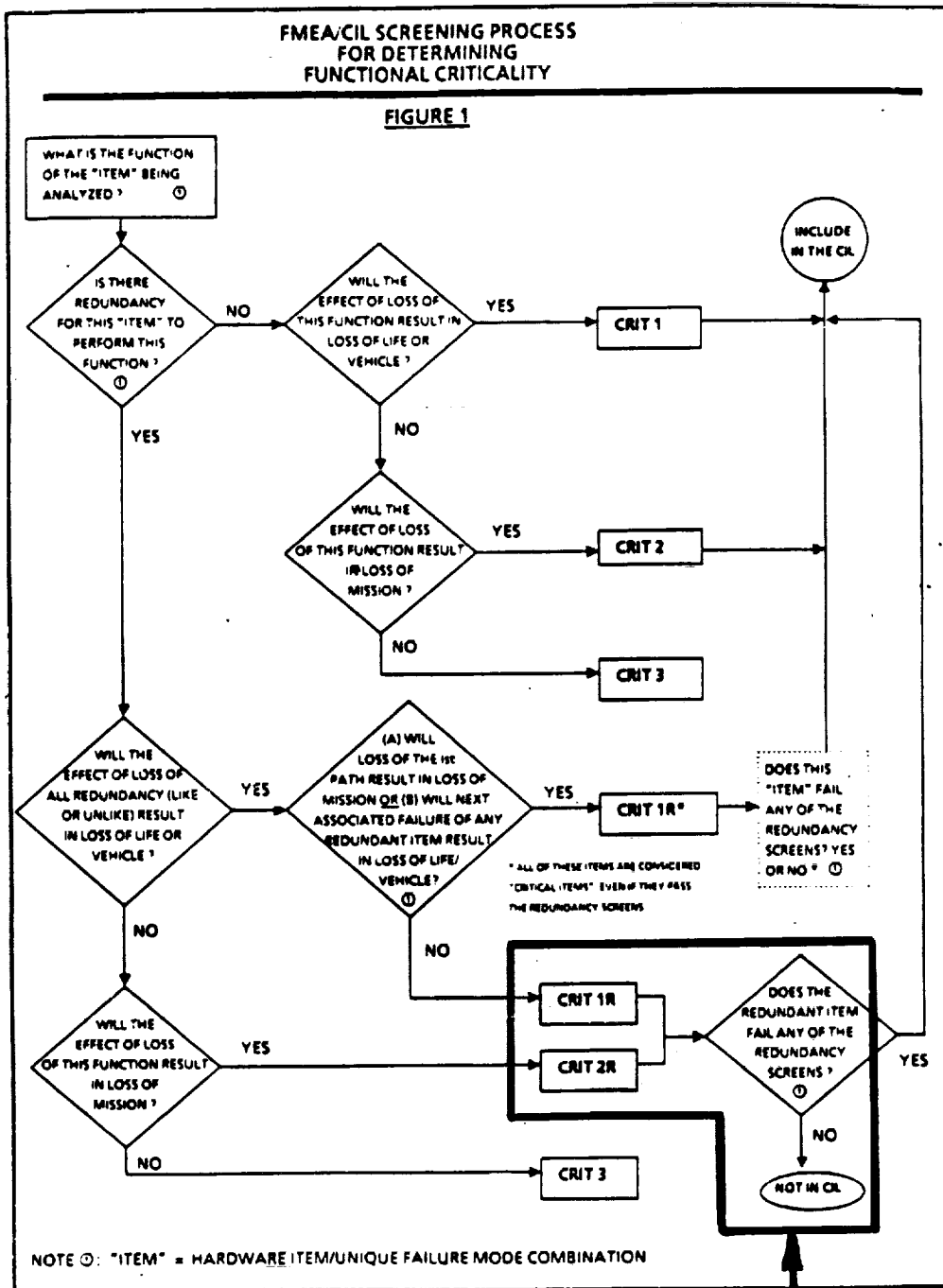
FUNCTION / LEVEL OF REDUNDANCY	BLOCK DIAGRAM	CRITICALITY CATEGORY	
		FUNCTIONAL DEFINITIONS	HARDWARE DEFINITIONS
LIFE OR VEHICLE ESSENTIAL / NO REDUNDANCY		1 (CIL)	1 (CIL)
MISSION ESSENTIAL / NO REDUNDANCY		2 (CIL)	2 (CIL)
LIFE OR VEHICLE ESSENTIAL / DUAL REDUNDANCY		1R (CIL)	2 (CIL)
MISSION ESSENTIAL / DUAL REDUNDANCY		PASSED SCREEN 2R	FAILED SCREEN 2R (CIL)
LIFE OR VEHICLE ESSENTIAL / TRIPLE REDUNDANCY		1R	1R (CIL)
MISSION ESSENTIAL / TRIPLE REDUNDANCY		2R	2R (CIL)
ALL NON-ESSENTIAL / ALL LEVELS OF REDUNDANCY		3	3

FIGURE 10

THESE LIFE AND MISSION
ESSENTIAL ITEMS ARE
EXCLUDED FROM THE CIL

FMEA/CIL SCREENING PROCESS FOR DETERMINING FUNCTIONAL CRITICALITY

FIGURE 1



12

THESE LIFE AND MISSION
ESSENTIAL ITEMS ARE
EXCLUDED FROM THE CIL

ORIGINAL PAGE IS
OF POOR QUALITY

HARDWARE CRITICALITY CREATES CONFUSION

INSTRUCTION: CRITICALITY CATEGORY CROSS REFERENCE TABLE

PROBLEM: • HARDWARE CRITICALITY WEAKENS THE IMPORTANCE OF LIFE AND MISSION ESSENTIAL ITEMS

- EXISTENCE OF TWO CRITICALITY CATEGORY DEFINITIONS CAUSES UNNECESSARY CONFUSION

EXAMPLE: 1R/3

1R = LIFE OR VEHICLE ESSENTIAL-REDUNDANT
3 = NON-ESSENTIAL

RECOMMENDATION: USE ONLY FUNCTIONAL CRITICALITY

(REFERENCE) RI, 100-2G, FIGURE 10; NSTS 22206, FIGURE 2

MDAC-HOUSTON

____ MCDONNELL DOUGLAS

CORPORATION



CRITICALITY CATEGORY
CROSS REFERENCE TABLE

FUNCTION / LEVEL OF REDUNDANCY	BLOCK DIAGRAM	CRITICALITY CATEGORY	
		FUNCTIONAL DEFINITIONS	HARDWARE DEFINITIONS
LIFE OR VEHICLE ESSENTIAL / NO REDUNDANCY		1 (CIL)	1 (CIL)
MISSION ESSENTIAL / NO REDUNDANCY		2 (CIL)	2 (CIL)
LIFE OR VEHICLE ESSENTIAL / DUAL REDUNDANCY		1R (CIL)	2 (CIL)
MISSION ESSENTIAL / DUAL REDUNDANCY		PASSED SCREEN 2R	FAILED SCREEN 2R (CIL) 3
LIFE OR VEHICLE ESSENTIAL / TRIPLE REDUNDANCY		1R (CIL)	3
MISSION ESSENTIAL / TRIPLE REDUNDANCY		2R	2R (CIL) 3
ALL NON-ESSENTIAL / ALL LEVELS OF REDUNDANCY		3	3

FIGURE 10

NON-ESSENTIAL?

LIFE ESSENTIAL!

IMPROVED FUNCTIONAL CRITICALITY DEFINITION

INSTRUCTION: CRITICALITY CATEGORY CROSS REFERENCE TABLE

PROBLEM: EXISTING CRITICALITY DEFINITIONS DO NOT IDENTIFY THE NUMBER OF REDUNDANT FUNCTIONAL PATHS

RECOMMENDATIONS: INCLUDE THE NUMBER OF FUNCTIONAL PATHS AS PART OF THE CRITICALITY CATEGORY FUNCTIONAL DEFINITIONS AS SHOWN IN TABLE

EXAMPLES: 2R(2) = MISSION ESSENTIAL, TWO PATHS
1R(3) = LIFE OR VEHICLE ESSENTIAL, THREE PATHS

(REFERENCE) RI, 100-2G, FIGURE 10; NSTS 22206, FIGURE 1

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION



CRITICALITY CATEGORY
CROSS REFERENCE TABLE



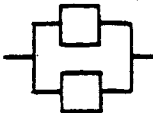

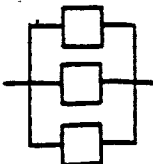
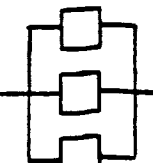


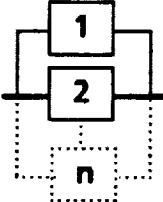
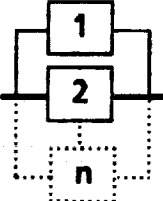
FUNCTION / LEVEL OF REDUNDANCY	BLOCK DIAGRAM	CRITICALITY CATEGORY	
		FUNCTIONAL DEFINITIONS	FUNCTIONAL DEFINITIONS WITH PATHS
LIFE OR VEHICLE ESSENTIAL / NO REDUNDANCY		1 CIL	1 CIL
MISSION ESSENTIAL / NO REDUNDANCY		2 CIL	2 CIL
LIFE OR VEHICLE ESSENTIAL / DUAL REDUNDANCY		1R CIL	1R(2) CIL
MISSION ESSENTIAL / DUAL REDUNDANCY		2R CIL	2R(2) CIL
LIFE OR VEHICLE ESSENTIAL / TRIPLE REDUNDANCY		1R CIL	1R(3) CIL
MISSION ESSENTIAL / TRIPLE REDUNDANCY		2R CIL	2R(3) CIL
ALL NON-ESSENTIAL / ALL LEVELS OF REDUNDANCY		3	3

FIGURE 10

REVISED TO CONFORM
WITH RECOMMENDED
CHANGES.

ORIGINAL PAGE IS
OF POOR QUALITY

"STREAMLINED"
CRITICALITY CATEGORY CROSS REFERENCE TABLE

FUNCTION / LEVEL OF REDUNDANCY	BLOCK DIAGRAM	CRITICALITY CATEGORY DEFINITIONS
LIFE OR VEHICLE ESSENTIAL / NO REDUNDANCY		1 CIL
MISSION ESSENTIAL / NO REDUNDANCY		2 CIL
LIFE OR VEHICLE ESSENTIAL / DUAL (OR GREATER) REDUNDANCY		1R (n) CIL
MISSION ESSENTIAL / DUAL (OR GREATER) REDUNDANCY		2R (n) CIL
ALL NON-ESSENTIAL / ALL LEVELS OF REDUNDANCY		3

R - FUNCTIONAL REDUNDANCY AVAILABLE
n - NUMBER OF FUNCTIONAL PATHS (LIKE AND UNLIKE)
CIL - DENOTES THAT ITEM IS ON CRITICAL ITEMS LIST

KEEP FMEA/CIL CURRENT

INSTRUCTION: CIL RETENTION RATIONALE a) DESIGN, b) TEST,
c) INSPECTION, d) FAILURE HISTORY

PROBLEM: BECOMES OBSOLETE UNLESS KEPT UP TO DATE

RECOMMENDATION: PROVIDE A MEANS TO MAINTAIN THE FMEA/CIL UNDER ACTIVE
CONTROL TO ASSURE UPDATES ARE CONCURRENT WITH APPROVED
DESIGN, TEST AND INSPECTION CHANGES AND NEW FAILURE
HISTORY

(REFERENCE) RI, 100-2G, PARAGRAPH 4.1.24; NSTS 22206, PARAGRAPH 2.2.3, AND TABLE 4.

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION

CLARIFY CHECKOUT TESTS

INSTRUCTION: CIL RETENTION RATIONALE

TEST-IDENTIFICATION OF SPECIFIC TESTS ACCOMPLISHED TO
DETECT FAILURE MODE AND CAUSES DURING ACCEPTANCE
TESTS, CERTIFICATION TESTS, AND CHECKOUT TESTS

PROBLEM: "CHECKOUT TESTS" NEEDS CLARIFICATION TO INCLUDE PRELAUNCH
AND FLIGHT TESTS

RECOMMENDATION: AMPLIFY "CHECKOUT TESTS" TO INCLUDE GROUND TURNAROUND,
PRELAUNCH, AND IN-FLIGHT TESTS

(REFERENCE) RI, 100-2G, PARAGRAPH 4.1.24; NSTS 22206, PARAGRAPH 2.2.3, AND TABLE 4.

MDAC-HOUSTON _____

MCDONNELL DOUGLAS

CORPORATION

IDENTIFY IN-FLIGHT CHECKOUT

INSTRUCTION: FMEA/CIL OMRSD MATRICES ARE REQUIRED TO ASSURE THAT IDENTIFIED FAILURE MODES ARE NOT PRESENT

PROBLEM: • OMRSD APPLIES ONLY TO GROUND TURNAROUND

• DOES NOT CONSIDER IN-FLIGHT CHECKOUT REQUIREMENTS

RECOMMENDATION: • PREPARE A SIMILAR MATRIX FOR IN-FLIGHT COVERAGE

(REFERENCE) NSTS 22206, PARAGRAPH 2.2 (FMEA), ITEM C AND
PARAGRAPH 2.2.3 (CIL), ITEM e.

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS



CORPORATION

IF CHECKOUT REQUIRED, SAY SO

INSTRUCTION: REDUNDANCY SCREEN

THE REDUNDANT ELEMENTS ARE CAPABLE OF CHECKOUT
DURING THE NORMAL MISSION TURNAROUND SEQUENCE

PROBLEM: ALLOWS ELEMENTS TO PASS IF ONLY CAPABLE OF CHECKOUT

RECOMMENDATION: REQUIRE THAT THE ITEM IS CHECKED OUT TO PASS THE SCREEN

(REFERENCE) RI, 100-2G, PARAGRAPH 4.1.21; NSTS 22206,
PARAGRAPH 2.3.4 AND TABLE 3.

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS



CORPORATION

DEFINE "READILY DETECTABLE"

INSTRUCTION: REDUNDANCY SCREEN

LOSS OF A REDUNDANT ELEMENT IS READILY DETECTABLE
DURING FLIGHT

PROBLEM: "READILY DETECTABLE" DOES NOT ASSURE TIMELY DETECTION

RECOMMENDATION: ADD THE FOLLOWING INSTRUCTION FOR THIS SCREEN:

READILY DETECTABLE REQUIRES THE CAPABILITY OF GETTING A
CREW MEMBER TO RESPOND TO A PROBLEM NOTIFICATION VIA
REAL-TIME MONITORED DISPLAYS, ON-BOARD ALERTS, VISUAL
INDICATIONS OR GROUND NOTIFICATION. GROUND NOTIFICATION
MUST NOT BE CONSIDERED UNLESS SUFFICIENT TIME IS AVAILABLE
TO PERFORM CORRECTIVE ACTION TO PRECLUDE THE CRITICAL
CONSEQUENCES OF THE FAILURE, USING WORST CASE TELEMETRY
AND DATA

(REFERENCE) RI, 100-2G, PARAGRAPH 4.1.21; NSTS 22206,
PARAGRAPH 2.3.4 AND TABLE 3.

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION

REDUNDANCY SCREEN MECHANICAL ITEMS

INSTRUCTION: MECHANICAL LINKAGES ARE EXCLUDED FROM REDUNDANCY SCREEN

PROBLEM: • MECHANICAL LINKAGES SHOULD BE TREATED THE SAME AS STANDBY REDUNDANT ITEMS WHOSE STATUS IS NOT KNOWN UNTIL CALLED UPON TO OPERATE

- STANDBY ITEMS FAIL THIS SCREEN IF THEIR STATUS IS NOT KNOWN UNTIL OPERATION

RECOMMENDATION: ALL REDUNDANT ITEMS SUCH AS CRANKS, RODS, AND JOINTS THAT ARE NOT CONSIDERED "STRUCTURE", AND ARE NOT CHECKED OUT PRIOR TO OPERATION, SHOULD "FAIL" THIS SCREEN AND BE INCLUDED ON THE CIL

(REFERENCE) NSTS 22206, PARAGRAPH 2.3.1 AND 2.3.4, ITEM b.2.

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION

PROVIDE FIRE SCREEN "D"

INSTRUCTION: DO NOT CONSIDER FIRE AS ONE OF THE SINGLE EVENTS OR CAUSES IN FAILING SCREEN "C"

PROBLEM: SINCE FIRE CAN CAUSE A LOSS OF REDUNDANCY, THE FMEA SHOULD PROVIDE A COMPLETE LISTING OF POTENTIAL IGNITION POINTS AND INADVERTENT FUEL SOURCES TO ASSURE ADEQUATE SAFETY VISIBILITY

RECOMMENDATION: ADD A SCREEN "D"
"UPON FAILURE, DOES THIS ITEM PROVIDE IGNITION POINTS AND/OR FUEL TO CAUSE AND/OR SUPPORT A FIRE?"

(REFERENCE) RI, 100-2G, PARAGRAPH 4.1.21, ITEM 5; NSTS 22206,
PARAGRAPH 2.3.4 AND TABLE 3.

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION

REQUIRE ADDITIONAL FMEAs

INSTRUCTION: "FMEAs ON WIRE HARNESSES, CABLES, AND ELECTRICAL CONNECTORS ARE NOT REQUIRED . . ."

PROBLEM: • OPERATIONAL FATIGUE, WEAR, AND POTENTIAL ERRORS MAY RESULT IN COMPROMISE TO EQUIPMENT THAT ARE EXCLUDED FROM FMEA/CIL REQUIREMENTS

- ALLOWS POTENTIAL CRITICAL FAILURE MODES TO BE OVERLOOKED AND STATUS NOT TO BE MONITORED

RECOMMENDATION: DO A FMEA TO IDENTIFY CRITICAL FUNCTIONS OF WIRE HARNESSES, CABLES, AND ELECTRICAL CONNECTORS

(REFERENCE) RI, 100-2G, PARAGRAPH 3.3, ITEM 9; NSTS 22206,
PARAGRAPH 2.3.1, ITEM e.

MDAC-HOUSTON

MCDONNELL DOUGLAS

CORPORATION

PLUG FMEA HOLE

INSTRUCTION: TEST PORTS, WHEN CAPPED, SHALL BE TREATED AS A STRUCTURAL PART OF THE COMPONENT AND NOT BE CONSIDERED FURTHER

PROBLEM: ● ALLOWS AN AREA OF POTENTIAL CRITICAL CONSEQUENCES TO BE OVERLOOKED AS A RESULT OF CAP/PLUG FAILURE

● EXAMPLES

- THE TEST PORT BETWEEN THE SRB REDUNDANT SEALS, WHICH WAS CONSIDERED AS A POTENTIAL FAILURE POINT EARLY IN THE CHALLENGER INVESTIGATION
- DELTA 86 FLIGHT FAILURE, WHERE AN OXIDIZER PURGE PORT PLUG WAS ONE OF THE TWO MOST PROBABLE CAUSES OF FAILURE
- EASTERN AIRLINES L-1011 OIL TEST PORT PLUGS CAUSED A TRIPLE ENGINE FLAMEOUT

RECOMMENDATION: INCLUDE CAPPED AND PLUGGED TEST PORTS IN THE FMEA ANALYSIS SO THEIR CONTRIBUTION TO CRITICAL FAILURE MODES WILL BE IDENTIFIED

(REFERENCE) RI, 100-2G, PARAGRAPH 4.3.1, ITEM 2; NSTS 22206,
PARAGRAPH 2.3.3, ITEM i.

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION

ALL ORDNANCE ON CIL

INSTRUCTION: ALL ORDNANCE AND PYROTECHNIC ITEMS WILL BE LISTED IN THE CIL ACCORDING TO THE MOST SEVERE EFFECT OF A PREMATURE OPERATION

PROBLEM: • DOES NOT CONSIDER CONSEQUENCES OF "FAILS TO OPERATE"

RECOMMENDATION: • AS A MATTER OF SAFETY, ALL ORDNANCE SHOULD BE CIL LISTED REGARDLESS OF CRITICALITY

- INCLUDE "FAILS TO OPERATE" AS A FAILURE MODE

(REFERENCE) NSTS 22206, PARAGRAPH 2.3.1, ITEM d.

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION

FUSE AND CIRCUIT BREAKER FAILURE MODES

INSTRUCTION: • THE FAILURE MODE "FAILS TO OPERATE" WILL NOT BE ADDRESSED FOR FUSES

- SUBSYSTEM UNIQUE GROUND RULES HAVE EXCLUDED CIRCUIT BREAKER "FAILURE TO TRIP"

PROBLEM: • A HAZARD EXISTS IF FUSES "FAIL TO OPERATE" OR IF CIRCUIT BREAKERS "FAIL TO TRIP" AT NOMINAL VALUES

- POTENTIAL FIRE OR IGNITION SOURCES WILL EXIST AS A RESULT OF A FAILURE OF THE ITEM(S) BEING PROTECTED

RECOMMENDATION: INCLUDE "FAILS TO OPERATE" AS A FAILURE MODE FOR FUSES AND CIRCUIT BREAKERS TO FLAG THE CRITICALITY AND POTENTIAL HAZARD IN THE ANALYSIS

(REFERENCE) RI, 100-2G, APPENDIX B, PARAGRAPH 3.1.2, ITEM 10.

SPECIFIC GROUND RULES AND CRITERIA:

- FMEA STS 82-0028, PARAGRAPH 3.2, ITEM 3.
- FMEA STS 82-0033, PARAGRAPH 3.2, ITEM 3.

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION

STANDARD FMEA/CIL FORMATS

INSTRUCTION: "DEVISE THE ANALYSIS WORKSHEET AND COMPLETE FOR EVERY IDENTIFIED FAILURE MODE"

PROBLEM: THE FMEA/CIL GENERATION/REVIEW/ASSESSMENT PROCESS INVOLVES MANY CONTRACTORS AND NASA CENTERS, WHICH RESULTS IN SEVERAL FORMATS WITH DIFFERING RULES

RECOMMENDATION: • STANDARDIZED FORMATS ARE NEEDED TO PROVIDE CONSISTENCY AND UNIFORMITY FOR COORDINATION OF DATA BETWEEN ORGANIZATIONS

- A WORKING PANEL SHOULD DEVISE STANDARDIZED FORMATS FOR THE FMEA AND CIL WITH BOTH INCORPORATED INTO NSTS 22206

(REFERENCE) NSTS 22206, PARAGRAPH 1.3, ITEM d.

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION

ASSESSMENT RECOMMENDATION SUMMARY

- CORRECT OMISSIONS
 - INCLUDE ALL FUNCTIONAL CRITICALITY 1, 1R, 2 AND 2R ITEMS ON CIL
 - PROVIDE FMEA COVERAGE TO ITEMS CURRENTLY GROUND RULED OUT
 - PROVIDE ACTUAL REFERENCED TEST PROCEDURES TO SUPPORT PASSING REDUNDANCY SCREENS FOR IN-FLIGHT TESTS
 - REQUIRE DISPOSITION AND RATIONALE FOR ALL FUNCTIONAL CRITICALITY 1, 1R, 2 AND 2R ITEMS
- CLARIFY AMBIGUITIES
 - SIMPLIFY CRITICALITY DEFINITIONS
 - STANDARDIZE FMEA AND CIL FORMATS
- ASSURE PROPER VISIBILITY, EVALUATION, AND RESOLUTION
 - REQUIRE THAT LEVEL II HAVE GREATER VISIBILITY OF CRITICAL FUNCTION ITEMS
 - SPECIFY THAT CIL ITEM EXCLUSION BE APPROVED BY PROGRAM LEVEL II
 - SPECIFY THAT DATA IS KEPT CURRENT IN BOTH THE FMEA AND CIL

MDAC-HOUSTON

_____ MCDONNELL DOUGLAS

CORPORATION

