FAILURE MODES EFFECTS ANALYSIS (FMEA) -- CRITICAL HARDWARE
NUMBER: 04-2-CONTL5-IM-X

SUBSYSTEM NAME: AUXILIARY POWER UNIT (APU)

REVISION : 3 09/04/91

	PART NAME VENDOR NAME	PART NUMBER VENDOR NUMBER
■ LRU :	APU CONTROLLER	MC201-0001-1005
■	SUNDSTRAND	753831

PART DATA

■ EXTENDED DESCRIPTION OF PART UNDER ANALYSIS:
SAFETY MONITORING (ELECTRONIC CONTROL CIRCUIT)

■ QUANTITY OF LIKE ITEMS: 4
FOUR CONTROL CIRCUITS PER APU CONTROLLER, 1 CONTROLLER PER APU

■ FUNCTION:

(1) CLOSES GGVM SHUTOFF VALVE AND PROVIDES ~~A~~ AN OUTPUT SIGNAL TO THE VEHICLE WHICH CAUSES CREW (C&W) TO BE ALERTED AND FUEL TANK ISOLATION VALVES TO CLOSE IF TURBINE SPEED IS BELOW 80%.

(2) CLOSES GGVM SHUTOFF VALVE AND PROVIDES A SIGNAL TO THE VEHICLE WHICH CAUSES CREW (C&W) TO BE ALERTED AND FUEL TANK ISOLATION VALVES TO CLOSE IF TURBINE SPEED IS ABOVE 129%.

(1) PROVIDES AN OUTPUT SIGNAL TO CREW (C+W), CLOSES GGVM SHUTOFF VALVE AND CLOSES FUEL TANK ISOLATION VALVES IF TURBINE SPEED IS BELOW 80%. THIS FUNCTION IS ACTIVATED 10.5 SEC AFTER START INITIATED. TWO MATCHING UNDERSPEED MPU SIGNALS REQUIRED.

(2) PROVIDES AN OUTPUT SIGNAL TO CREW (C&W), CLOSES GGVM SHUTOFF VALVE AND CLOSES FUEL TANK ISOLATION VALVES IF TURBINE SPEED IS GREATER THAN 129% SPEED. ONE MPU OVERSPEED SIGNAL REQUIRED FOR FIRST 10.5 SEC, TWO MATCHING OVERSPEED MPU SIGNALS REQUIRED AFTER 10.5 SEC.

FAILURE MODES EFFECTS ANALYSIS (FMEA) -- CRITICAL FAILURE MODE
NUMBER: 04-2-CONTL5-IM-12

SUBSYSTEM: AUXILIARY POWER UNIT (APU) REVISION# 3 09/04/91 R
LRU :APU CONTROLLER
ITEM NAME: APU CONTROLLER CRITICALITY OF THIS FAILURE MODE:1R2

■ FAILURE MODE:
PREMATURE OUTPUT (PREMATURELY PRODUCES SHUTDOWN SIGNAL).

MISSION PHASE:

PL	PRELAUNCH
LO	LIFT-OFF
DO	DE-ORBIT
LS	LANDING SAFING

■ VEHICLE/PAYLOAD/KIT EFFECTIVITY:

102	:	COLUMBIA
103	:	DISCOVERY
104	:	ATLANTIS
105	:	ENDEAVOUR

■ CAUSE:
CONTROLLER INTERNAL PIECE-PART FAILURES (ONE FAILURE DURING 10.5 SECOND START DELAY, OR TWO FAILURES THEREAFTER), WIRE TO WIRE POWER SHORT, WIRE TO GROUND SHORT.

■ CRITICALITY 1/1 DURING INTACT ABORT ONLY? YES

AOA	ABORT ONCE AROUND
ATO	ABORT TO ORBIT
RTLS	RETURN TO LAUNCH SITE
TAL	TRANS ATLANTIC ABORT

■ REDUNDANCY SCREEN A) PASS
■ B) PASS
■ C) PASS

PASS/FAIL RATIONALE:
■ A)

■ B)

■ C)

FAILURE MODES EFFECTS ANALYSIS (FMEA) -- CRITICAL FAILURE MODE
NUMBER: 04-2-CONTL5-IM-12

- FAILURE EFFECTS -

- (A) SUBSYSTEM:
POSSIBLE LOSS OF ONE APU AFTER ONE GROUND SHORT FAILURE. POSSIBLE RESTART CAPABILITY WITH SAFETY CIRCUIT INHIBITED.

- (B) INTERFACING SUBSYSTEM(S):
POSSIBLE LOSS OF SHAFT POWER TO ONE HYDRAULIC PUMP.

- (C) MISSION:
ABORT DECISION IS REQUIRED IF FAILURE OCCURS PRIOR TO ENTRY COMMITMENT.

- (D) CREW, VEHICLE, AND ELEMENT(S):
NO EFFECT UNTIL SECOND SYSTEM LOST. POSSIBLE LOSS OF VEHICLE IF TWO OF THREE APUS ARE LOST. LOSS OF ONE APU DURING POWERED FLIGHT WILL RESULT IN THE ASSOCIATED SSME GOING INTO HYDRAULIC LOCK-UP AND COULD RESULT IN LOSS OF ORBIT CAPABILITY OR BE CATASTROPHIC (WITH ADDITIONAL SSME VALVE FAILURE). (REF. FLIGHT RULE 10-13)

- (E) FUNCTIONAL CRITICALITY EFFECTS:
SINGLE INTERNAL CONTROLLER PIECE PART FAILURE OR SINGLE MPU FAILURE RESULTING IN OVERSPEED SIGNAL WILL CAUSE THIS FAILURE MODE DURING FIRST 10.5 SEC OF APU START. THE APU MAY BE RESTARTED WITH THE SAFETY CIRCUIT INHIBITED (USING INJECTOR COOLING IF NECESSARY) IF IT IS DETERMINED THE OVERSPEED WAS 'FALSE'. FOLLOWING 10.5 SECONDS A SINGLE GROUND SHORT OR TWO INTERNAL CONTROLLER PIECE PART OR MPU FAILURES REQUIRED.

- DISPOSITION RATIONALE -

- (A) DESIGN:
FOUR SEPARATE SPEED CONTROL CIRCUITS FEED INTO A PARALLEL/SERIES COMBINATION OF VALVE DRIVER SWITCHES (FET). ELECTRICAL COMPONENTS ARE REQUIRED TO BE QUALIFIED, PROPERLY DERATED, AND APPLIED PER MC201-0001, PARAGRAPH 3.3.2.2. ELECTRICAL PARTS SELECTED FROM MF0004-400 (OPPL) B PLUS.

CONFORMAL COATING PER SUNDSTRAND SPEC CP 17.32-01. CLEANLINESS PER MA0110-201. CONTROLLER VIBRATION DAMPED AT MOUNTING.

THE OPPL CALLS FOR GLASSIVATION FOR INTEGRATED CIRCUIT DIE, SINGLE SEAL FOR TANTALUM WET SLUG CAPACITORS, ETC. DERATING OF EEE PARTS IS EXPANDED BEYOND THE SIMPLISTIC (75% x RATED) REQUIREMENTS OF THE CONTRACT.

FAILURE MODES EFFECTS ANALYSIS (FMEA) -- CRITICAL FAILURE MODE
NUMBER: 04-2-CONTLS-IM-12

■ (B) TEST:
CONTROLLER IS FUNCTIONALLY TESTED DURING ATP. CONTROLLER IS SUBJECTED TO AVT. CONTROLLER IS THERMAL TESTED DURING ATP - RANGE 70 DEG F, 130 DEG F, 30 DEG F.

CONTROLLER IS QUALIFIED FOR QAVT, EMI, THERMAL VACUUM (-65 DEG F TO 165 DEG F, 80 K FT FOR 10 CYCLES), HUMIDITY AND FLIGHT VIBRATION.

ALL EEE PARTS ARE SUBJECTED TO SCREENING AND BURN-IN TESTS TO DETECT MARGINAL PARTS AND TO CAUSE INFANT MORTALITY FAILURES.

OMRSD: CONTROLLER/CCU TESTS ARE PERFORMED ON EACH CONTROLLER EVERY FLOW DURING GROUND TURNAROUND TO VERIFY ALL FOUR SAFETY CIRCUITS. IN ADDITION, IT VERIFIES THAT THERE ARE NO GROUND SHORTS.

■ (C) INSPECTION:
RECEIVING INSPECTION:
VISUAL AND DIMENSIONAL INSPECTIONS ARE PERFORMED ON ALL INCOMING PARTS. MATERIAL AND PROCESSES CERTIFICATIONS ARE VERIFIED.

CONTAMINATION CONTROL:
CLEANLINESS IS VERIFIED BY INSPECTION.

ASSEMBLY/INSTALLATION:
MANUFACTURING, ASSEMBLY, AND INSTALLATION REQUIREMENTS ARE VERIFIED BY INSPECTION.

CRITICAL PROCESSES:-
SOLDERING TO NH8 5300.4(3A) IS VERIFIED BY INSPECTION.

TESTING:
TEST EQUIPMENT AND TOOL CALIBRATION ARE VERIFIED BY INSPECTION. ATP IS WITNESSED AND VERIFIED BY INSPECTION.

HANDLING/PACKAGING:
HANDLING, PACKAGING, STORAGE, AND SHIPPING PROCEDURES ARE VERIFIED BY INSPECTION.

■ (D) FAILURE HISTORY:
NONE

■ (E) OPERATIONAL USE:
LOSS OF ONE APU WILL RESULT IN SWITCHING TO HIGH SPEED AND INHIBIT ON OTHER TWO APUS DEPENDING ON MISSION PHASE. PERFORM HOT RESTART IN INHIBIT MODE TO GAIN SECOND APU, IF DEEMED SAFE.

PRINT DATE: 09/04/91

SD5C27CH
ATTACHMENT
PAGE S

FAILURE MODES EFFECTS ANALYSIS (FMEA) -- CRITICAL FAILURE MODE
NUMBER: 04-2-CONTL5-IM-12

- APPROVALS -

RELIABILITY ENGINEERING	D. R. ATAPATTU	
DESIGN ENGINEERING	D. J. ZWICK	
QUALITY ENGINEERING	W. R. HIGGINS	10/4/91
NASA RELIABILITY		11/7/92
NASA SUBSYSTEM MANAGER		1-24-92
NASA QUALITY ASSURANCE		11/2/91