SUBSYSTEM: RANGE SAFETY COMMAND DESTRUCT

ITEM NAME: IRD A, IRD B

PART NO.: 10406-0143-803, -804, -805, -806, -807, -808, -809 or 16A03344-9

FM CODE: A06

ITEM CODE: 70-17, 70-18

REVISION: Basic

CRITICALITY CATEGORY: 1R

REACTION TIME: Seconds

NO. REQUIRED: 2

DATE: March 31, 2000 CN 038

CRITICAL PHASES: Boost

SUPERCEDES: March 1, 1996 CN 038

FMEA PAGE NO.: F-14

ANALYST: S. Parvathaneni CN 038

SHEET 1 OF 7

APPROVED: S. Parvathaneni CN 038

FAILURE MODE AND CAUSES: Unscheduled fire command, after a valid arm command, from RS System A IRD and/or RS System B IRD (requires a minimum of two failures in the IRD) caused by:

- o Faulty IRD decoder firmware
- o Multiple failures on the command output subassembly

FAILURE EFFECT SUMMARY: Loss of vehicle, mission and crew. One success path remains after the first dual failure. Operation is not affected until both paths are lost.

REDUNDANCY SCREENS AND MEASUREMENTS:

1. Fail - Open clamp diodes will allow lift off and flight one failure away from this failure mode. These diodes cannot be checked during normal turnaround.

2. Fail - Unable to detect this failure mode without issuing an arm command.

3. Pass - No known credible causes.

RATIONALE FOR RETENTION:

A. DESIGN:

O The RSS IRDs A and B are two identical but separate boxes. The RF inputs are supplied from isolated output ports of the hybrid coupler through two redundant coaxial cables. Power is supplied from redundant batteries via redundant RSS distributor assemblies and cables. Commands from the two IRDs are furnished to the two redundant distributor sides (A and B) via redundant electrical cables.

O One of the functions of the IRD is to provide Arm and Fire commands to the RSDs upon receipt of properly encoded RF commands. These commands are implemented functionally by demodulating the RF command signals, decoding the received tone pairs, comparing the received tone pair format to the flight code stored into memory before launch, and issuing output commands as appropriate. The design of the IRD implements these functions in hardware by providing RS subassemblies, decoder subassemblies, wiring harnesses and ROM based firmware. The specific RSS design feature that was implemented to mitigate all of the listed failure causes is true parallel redundancy.

O The IRD has one vendor source, Cincinnati Electronics. The vendor has been certified as the supplier by completing qualification testing. Cincinnati Electronics qualification is reported in Qualification Test Report RA-13, Vol. 1 through Vol. 3 and certified by USA SRBE COQs A-RSS- 3101-1, A-RSS-3101-2, A-RSS-3101-3 and A-RSS-3101-4.

O All electrical and electromechanical component parts used in the IRD have traceability requirements per SE-019-033-2H. In addition a log book is generated for each IRD assembly at the start of acceptance testing and a complete historical record is maintained for the life of the IRD.

O Faulty IRD Firmware (Jump to output subroutine)

- o The IRD firmware is contained in read-only-memories (ROM). The firmware meets all the requirements of the IRD assembly specification, USA SRBE 10SPC-0132, has flown on all Shuttle missions since STS-6, and is qualified for the twenty-mission level. (BI-1610, BI-1453)

- o The IRD operating program is kept under configuration control and is implemented in fusable link read-only-memories (ROM). Following programming of these memories the parts are screened to the requirements of MIL-STD-975, Grade one, in accordance with approved screening procedures.

- o Inadvertent operating program jumps to the command output subroutines are precluded by use of an "Insurance" (INS) word located in random access memory (RAM) and a command interrupt subroutine which verifies the validity of any command output.

  - o The INS word is a 16 bit word located in RAM in which individual or groups of bits are set, incremented and validated at various critical steps during the message processing, command validation, code verification and command output states. This INS word must be in a pre-defined configuration at each critical step before command processing is allowed to continue by the operating program. Following code validation, command output is accomplished in two steps: removal of the clamp to ground on a command output line and switch of a regulated 28 volt source to the same command output. The INS word is checked and updated before each of these two steps.

- o If an unscheduled jump to this command output could occur due to some unusual environment or condition, the INS word would be in an improper configuration and the IRD would reset and return to signal search looking for a new message.

- o Additionally, if a command output line goes "high" (28 volts) this level will generate an interrupt to the central processing unit (CPU). The interrupt subroutine will perform a check of the INS word to determine that the output sensed is valid. If the output is determined to be invalid, then both halves of the redundant command latches will be reset, thereby, removing logic signals to the command output subassembly. The command output risetime is controlled to allow reset in less than 100 microseconds. The range safety distributor specifications guarantee that the ARM/FIRE latches will not respond to this narrow pulse.

O Multiple Failures on the Command Output Subassembly

- o The command output subassembly contains five identical solid state circuits: ARM, FIRE and three spare command output drivers. When a command output is initiated, redundant logic outputs are set on two data bus latches. When the first latch is set, a clamp to ground is removed from the addressed command output. When the second latch is set a regulated 28 volt supply is switched to the addressed output through a current limit/over-load protection circuit. These redundant control circuits are independent up to the command output line and two failures are required to obtain an inadvertent continuous 28 volt output. This design precludes the possibility of a single point failure resulting in this failure mode.

- o The IRD subassemblies meet all of the requirements of USA SRBE spec 10SPC-0132, have been flown on all Shuttle missions since STS-6 and are qualified to the twenty-mission level. The subassemblies have the following design features that were incorporated to mitigate this cause of failure: (BI-1610, BI-1453)

- o The two-sided printed wiring boards (PWB) were designed to MSFC-STD-154 and contain plated through holes that are used as mechanical reinforcement rather than as an interconnection between two sides of the board. Electrical interconnection is by Z-wire. The receiver subassembly PWBs are mounted into isolated cavities within the top (receiver) housing. Both sides of the PWBs are conformal coated, after testing, except at the outer ground plane area where contact is made to the receiver housing for EMI/RFI shielding. The decoder subassemblies are foam potted to eliminate the possibility of shorts between components and adjacent subassemblies. (BI-1895)

  - o The electrical component parts that are used in the Arm and Fire circuits are either selected from MIL-STD-975, Grade one or are screened to Grade one requirements. The integrated circuits are listed in or screened to the requirements of MIL-STD-975 (Grade one parts) or screened up to the equivalent.

- o All components have thermal stress relief and are soldered to NHB 5300.4 (3A-1).

- o The power output transistors for Arm and Fire are designed to provide an eight hundred percent margin above nominal requirements.

- o A parts traceability program is implemented to respond to GIDEP Alert notices on IRD piece parts.

- o An ESD control program is implemented and utilized during the manufacture and inspection of all IRD subassemblies.

B. TESTING

VENDOR RELATED TESTING

O The IRD testing is done first at the subassembly level, prior to staking, potting or conformal coating. The completed IRD is functionally and environmentally tested in accordance with Acceptance Test Procedure ES155.249. Acceptance testing assures there are no unscheduled or erroneous fire outputs at the time of the test. (All Failure Causes)

O The IRD automated test set contains glitch monitoring circuits on each IRD command output line. These circuits are calibrated to respond to any pulse greater than 2 volts and greater than 100 microseconds. Activation of any one of these circuits when a command has not been issued will interrupt the test sequence and create a test error condition. These glitch circuits are active during any IRD bench or acceptance test, including ambient functional, thermal cycle and vibration.

KSC RELATED TESTING

O Each IRD received at KSC, new or refurbished, is bench tested as required by 10REQ-0021, Appendix E. The bench test verifies there is no unscheduled fire command output during the bench test. (All Failure Causes) ESD protection requirements are implemented IAW 10REQ-0021 para 4.11

O The arm and fire outputs are tested during ACO per 10REQ-0021, paras. 1.2.2.13.3 and 1.2.2.13.6. ESD protection requirements are implemented IAW 10REQ-0021 para 4.11. (All Failure Causes)

O IRD arm and fire outputs are monitored during SIT, Pad Validation Testing (ordnance installation, Part II) and during final countdown by event measurements B55E1877X, B55E1878X, B55E1879X and B55E1880X. (All Failure Causes)

O The IRD power, Arm and Fire signals are monitored by software and a console operator during final countdown and during flight until the separation sequence begins. The occurrence of an arm or fire output during the final countdown or flight is noted by the software and/or console operator and is recorded. Any unscheduled arm or fire output during final countdown initiates a launch delay. (All Failure Causes)

REFURBISHMENT/RECERTIFICATION TESTING

O All IRDs are Refurbished/Recertified for flight and tested in accordance with USA SRBE 10SPC-0131.

O All USA SRBE/TBE Florida Operations Refurbished /Recertified IRDs are acceptance tested IAW 10SPC-0131.
(All Failure Causes)

C. INSPECTION

VENDOR RELATED INSPECTION

O Supplier QA performs receiving inspection and maintains traceability of all electrical parts.

- o USA SRBE PQAR SIP 1270

O Supplier Quality and USA SRBE Quality inspect the assembly, soldering, and monitor potting operations:

- o USA SRBE Quality - SIP 1270

O Supplier Quality and USA SRBE Quality witness/verify Acceptance Test. (All Failure Causes)

- o USA SRBE Quality - SIP 1270

O Critical Processes/Inspections/Operations:

- o Soldering per NHB 5300.4(3A-1)
- o Encapsulating per vendor procedure ES155.246

KSC RELATED INSPECTION

O USA SRBE QA monitors and accepts all bench tests of IRDs. (All Failure Causes)

CN 038

O USA SRBE QA witnesses torquing of IRD mounting bolts during installation on SRB forward skirt equipment panel.

O USA SRBE QA witnesses electrical bonding resistance checks between IRD and panel.

O Connector receptacles are inspected for damaged, bent, broken or corroded contacts per 10REQ-0021, para. 1.2.1.1.9.

CN 038

O USA SRBE QA witnesses IRD isolation testing after IRD installation on SRB forward skirt equipment panel.

O RSS Arm and Fire testing is performed during ACO per 10REQ-0021, paras. 1.2.2.13.3 and 1.2.2.13.6. (All Failure Causes)

O Verify open loop response by all five receiver/decoder subsystems using test code for SRSS per OMRSD File II, Vol. 1, requirement number S00000.380.

O Verify operation of SRSS with flight code (closed loop) per OMRSD File II, Vol. 1, requirement number S00000.390.

O After each flight USA SRBE QA inspects the IRD for compliance with USA SRBE 10SPC-0131.

REFURBISHMENT/RECERTIFICATION INSPECTION

O All previously flown IRDs are inspected in accordance with USA SRBE 10SPC-0131.

O Quality representatives witness the acceptance testing of all USA SRBE/TBE Florida Operations refurbished IRDs per the design specification 10SPC-0132. (All Failure Causes)

D. FAILURE HISTORY

O Failure Histories may be obtained from the PRACA database.

E. OPERATIONAL USE

o Not applicable to this failure mode.

F. WAIVER/DAR

o BI-1610, 7-26-88, CCBD SB3-01-1384

- SPECIFIED REQUIREMENT:

  The EEE parts control program shall be in accordance with the specific requirements for Criticality 1 and 2 equipment of 85M03936B.

- DEPARTURE:

  Some EEE parts (diodes, opto-isolator and ICs) did not meet requirements of 85M03936B.

- JUSTIFICATION:

  There has been no failure of these parts in flight or in the field through 97 flight uses and 3,227 hours of use. The IRDs are dual redundant on each SRB and simplex on the ET. The calculated mean-time-between-failure, using MIL-HDBK-217B failure rates for the parts actually procured and installed, exceeds 10SPC-0132 specification requirement.

o BI-1453, 11-16-84, CCBD SB3-00-9398

- SPECIFIED REQUIREMENT:

  MIL-M-38510 Linear Microcircuit Products manufactured by Fairchild's Linear Division were not "cooled down under bias" after performance of the required burn-in-screen.

- DEPARTURE:

  C E P/N ITS-M-11952 (Generic 741) LDC 8301 manufactured by Fairchild and listed on Gidep Alert VV-A-84-03 (4236) is used in power supply assembly P/N 392304

- JUSTIFICATION:

  Devices were subjected to additional testing after receipt from Fairchild. Tests included DPA, Burn-in, Parameter Measurement, etc

o BI-1895, 1-28-91, CCBD SB3-01-3957

- SPECIFIED REQUIREMENT:

  PWBs design shall be in accordance with MSFC-STD-154. The minimum size of solder pads with component lead holes of 0.030 inch and smaller shall be determined by encircling with 0.010 inch copper, and lead holes greater than 0.030 inch shall be determined by encircling with 0.015 inch copper.

- DEPARTURE:

  IRD PWBs have component lead holes greater than .030 inch which have annular rings less than .015 inch.

- JUSTIFICATION:

  PWBs are acceptable for flight since they meet or exceed the new requirement which allows holes to have a minimum annular ring size of .005 inches.