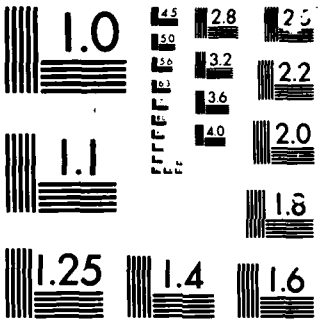
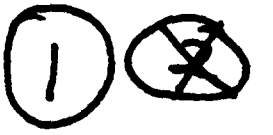
AD-A166 816 SUBSYSTEM HAZARD ANALYSIS FOR THE LSI MODELS 6216A B & C SELF-CONTAINED N..(U) LEAR SIEGLER INC GRAND RAPIDS MI INSTRUMENT DIV J T REEVES 13 MAR 86 GRR-6216-013 1/1

UNCLASSIFIED F09603-85-C-1224 F/G 9/5 NL


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
MICROCOPY
CHART



LEAR SIEGLER, INC.
INSTRUMENT DIVISION

SUBSYSTEM HAZARD ANALYSIS

FOR THE

LSI MODELS 6216A, B, & C

SELF-CONTAINED NAVIGATION SYSTEM

GROUP A

REPORT NO. 6216-013

CONTRACT NO. F09603-85-C-1224

Data Item 0103

PREPARED BY John T. Reeves

DATE 86-3-13

APPROVED BY D.J. Barbel for H. Stork

DATE 86-3-13

PRELIMINARY

LEAR SIEGLER, INC.
INSTRUMENT DIVISION
4141 EASTERN AVE. S.E. GRAND RAPIDS, MI 49508

TABLE OF CONTENTS

1.0 GENERAL - This document constitutes the Subsystem Hazard Analysis (SSHA) for the C-130 Self-Contained Navigation System (SCNS) installation. It provides a safety assessment of the SCNS installation.

1.1 PURPOSE - IAW MIL-STD-882A, the purpose of an SSH is to evaluate the parts making up a system for items that could adversely affect the system safety through component failure, performance degradation, functional failure and inadvertent operation.

1.2 SCOPE - The scope of this analysis for Data Item 0103 is limited to the SCNS installation task "A-kit" components (viz. wiring harness, brackets, racks control panels, relay boxes, circuit breakers), "B-kit" components (viz. ICDUs, BICU, DVS, INU), and the physical interfaces with existing equipment (viz. CADC or Sensors, Radar, Air Data Sensors. These items will be analyzed in respect to safe installation, safe hardware, and safe usage (viz. installation, removal, in-place test, and handling). No system Functional aspects are analyzed.

2.0 APPLICABLE DOCUMENTS -

2.1 GOVERNMENT DOCUMENTS - The following documents of the exact issue shown are used in the preparation of this analysis and report.

MIL-STD-882A	System Safety Program Requirements (paragraph 5.5.1.2).
D-H-7048	System Safety Hazard Analysis Report (paragraph 10.2.2).
DH1-6 (Edition 5)	System Safety Design Handbook
SOW	
84-MMSRE-004-C-130SCNS	C-130 Modification Self-Contained Navigation System (SCNS), Statement of Work for
84-MMSRE-009-C-130	Self-Contained Navigation System (SCNS), Integration, Fabrication and Installation and Test of, C-130 Aircraft

2.2 OTHER DOCUMENTS - See table II and III.

3.0 SYSTEM DESCRIPTION

3.1 GENERAL DESCRIPTION - The SCNS is comprised of a Doppler Velocity Sensor (DVS), Inertial Navigation System (INS), Integration Computation and Display System (ICDS), and the associated installation Group A kit to provide doppler aided INS navigation, INS only, Doppler only and TAS/HDG navigation modes, and control of the various C-130 communication/navigation (comm/nav) systems. The SCNS ICDS consists of three Integrated Control Display Units (ICDU) and one Bus Integration Computer Unit (BICU) for all C-130 aircraft except that the HC-130H will have an additional ICDU for the radio control. A block diagram is shown in figure 1.

In conjunction with the SCNS installation, the following system/components will be removed from the various C-130 configurations.

AN/APN-147 Doppler
AN/ASN-35 Doppler Computer
ARN-131 Omega
AN/ASN-24 OR PINS (C-130E AWADS only)

Radio controls for

AN/ARC-164 UHF (one control retained)
AN/ARC-186 VHF
AN/ARC-190 HF
AN/ARN-118 TACAN
AN/ARN-127 VOR/ILS
USAF Standard VOR/ILS

The communication and navigation radio control functions will be assumed by the ICDUs except during an emergency use of a UHF backup manual control head.

3.2 MAJOR COMPONENTS - A list of major components is provided in table I.

3.2.1 ICDS - The ICS consists of two major components: the Integrated Control Display Unit (ICDU) and the Bus Integration Computer Unit (BICU). All aircraft configurations utilize fully interchangeable ICDUs: pilot's, co-pilot's, navigator's and

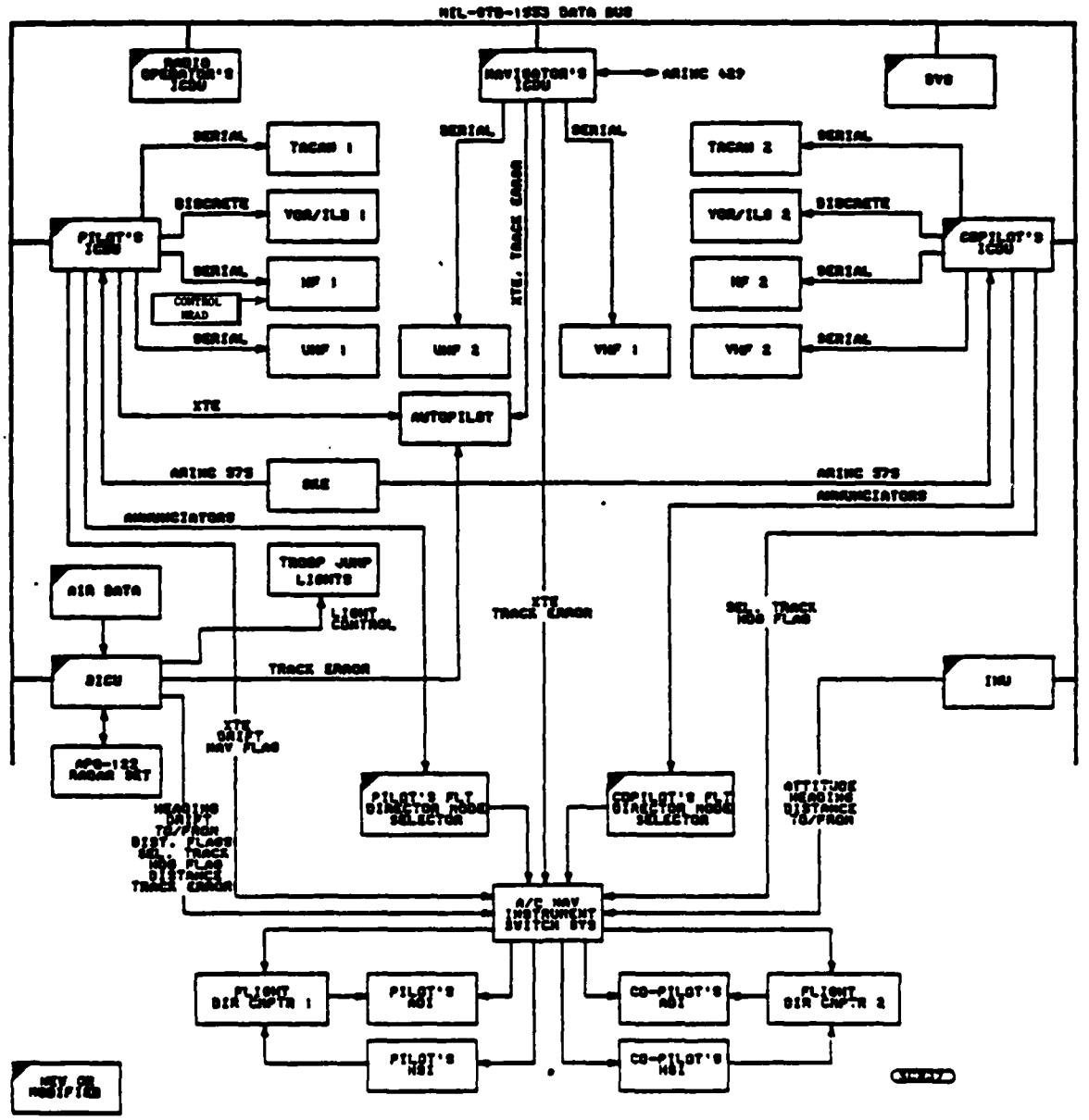


Figure 1. SCNS Block Diagram

Table I. Major Component List

MODEL NO.	GROUP A	GROUP B	DESCRIPTION	LOCATION
LSI-2580F		√	Integrated Control Display Unit	Left side forward on center console for pilot. Right side forward for co-pilot. Nav panel for navigator. Radio operator's panel for HC-130.
LSI-2905A		√	Bus Interface Computer Unit	New equipment rack.
LSI-2905B		√	Bus Interface Computer Unit with Added Radar Interface Card (AWADS)	New equipment rack.
LSI-2590A APN-218		√	Doppler Velocity Sensor	Belly of aircraft
SNU 84-1		GFE	Inertial Navigation Sensor	Aircraft floor below new equipment rack
-	√		Electrical A-Kit	Several variations
-	√		Mechanical A-Kit	Several variations
-	√		Flight Director Mode Select panel modifications	Instrument Panel (also a panel on the pedestal for C-130B)
-	√		SCNS Control Panel	Nav Station
-	√		INU Battery	Battery Compartment

radio operator's (HC-130H). Jumper wires in the the aircraft installation indicate its particular station location to each ICDU. One basic BICU design is utilized in all SCNS configurations with the exception of the BICU for the AWADS aircraft. It adds a third circular connector and SRUs for the radar interface. Connector jumper wires indicate to the BICU into which aircraft model it is installed.

3.2.2 INS - The Inertial Navigation System (INS) consists of three major components: the Inertial Navigation Unit (INU), the INU mount, and the SCNS battery subsystem. The SCNS INU conforms to requirements of of the F^3 SNU 84-1 and SNU 84-3 specifications.

3.2.3 DVS - Doppler Velocity Sensor (DVS) consists of the APN-218 Air Force Standard Doppler. The DVS provides basic navigation inputs for SCNS independent doppler navigation capability and for integrated INS/Doppler capability.

3.3 SYSTEM FUNCTIONS - The SCNS primary function is to provide highly accurate and reliable self-contained navigation capability for the MAC C-130 Tactical Airlift Operations. These missions and operations are defined in MACR 55-130, Military Airlift Command Regulation.

3.3.1 MAJOR FUNCTIONS - The SCNS provides the following major functions.

- Navigation modes and position update capability.
- Integrated control and display of navigation, communications, guidance, and steering functions.
- Aircraft guidance and steering - including flight plan, time of arrival, CARP, SAR, and rendezvous.

3.3.2 SECONDARY FUNCTIONS - Additional features are provided to improve performance, reduce crew workload, and minimize aircraft maintenance time. Specifically, these are:

- TACAN mixing to improve navigation accuracy.
- CARP capability that will reduce crew workload and increase mission flexibility.
- Simple, accurate, and quick magnetic compass calibration procedures.

3.4 A-KITS - The "A" kits consists of:

- The interconnecting cables between added LRUs.
- The interconnecting cables and modifications to cables connecting existing LRUs.
- Mounting trays and hardware.
- Sheet metal work as required.
- Control panels
- Blank panels
- Annunciator lights
- Pressure sensors
- Circuit breaker changes and additions.

4.0 SAFETY CRITERIA - Certain safety criteria IAW MIL-STD-882A are followed in the SSHA.

4.1 SYSTEM SAFETY PRECEDENCE - Any items detected as fitting into hazardous categories are treated in the following order:

a. Redesign to eliminate the hazard, if possible.

b. Change operating procedure to eliminate or reduce occurrence.

c. Provide training recommendations to allow personnel to safely work in the presence of the hazard.

d. Label or placard hazards and provide inputs to manuals.

4.2 HAZARD LEVEL CATEGORIES - (Criticality definitions) For the purpose of the hazard analysis, the hazards will be defined and categorized IAW the criticality definitions set forth below (ref. MIL-STD-882A, para. 5.4.3.1).

4.2.1 HAZARD SEVERITY - Hazard severity categories are defined to provide a qualitative measure of the worst potential consequences resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, system, subsystem or component failure or malfunction as follows:

a. CATEGORY I - Catastrophic - May cause death or system loss.

b. CATEGORY II - Critical - May cause severe injury, severe occupational illness, or major system damage.

c. CATEGORY III - Marginal - May cause minor injury, minor occupational illness, or minor system damage.

d. CATEGORY IV - Negligible - Will not result in injury, occupational illness, or system damage.

4.2.2 HAZARD PROBABILITY - The probability of the defined hazard occurring is based on a qualitative judgement for the purpose of this hazard analysis. The probability levels quoted here are from MIL-STD-882A, Para. 5.4.3.2.

DESCRIPTION WORD	LEVEL	SPECIFIC INDIVIDUAL ITEM	FLEET OR INVENTORY
Frequent	A	Likely to occur frequently	Continuously experienced
Reasonably Probable	B	Will occur several times in life of an item	Will occur frequently
Occasional	C	Likely to occur sometime in life of an item	Will occur several times
Remote	D	So unlikely, it can be assumed that this hazard will not be experienced	Unlikely to occur but possible
Extremely Improbable	E	Probability of occurrence cannot be distinguished from zero	So unlikely, it can be assumed that this hazard will not be experienced
Impossible	F	Physically impossible to occur	Physically impossible to occur

5.0 HAZARD ANALYSIS - The sources of data for the SSHA are the drawings for the installation kits, the wiring interconnects interface control drawings, the panel and console modifications, the "B" component outline drawings, system block diagrams, grounding and shielding diagrams, process specifications and test procedures. At the time of preparation of this report, most of the source data was in preliminary form.

Data references are given in table II and III. Any items found during the review of those data are listed on SSHA matrix sheets. Where comments are applicable only to specific models, they will be so annotated. Most source information is very preliminary, therefore, listed items are quite tentative and subject to change in later submittals.

5.1 SSHA MATRIX SHEETS - These sheets are used to list potential hazards, effects on the system and remedial steps to be taken.

5.2 SUMMARY - At this writing, two items were rated in Category II, Critical. Both items are still in the design phase and the concerns are being considered in respect to the final solution. These are:

(1) The method of connecting up the added INS aircraft battery so that a dead battery doesn't draw full current from the bus. It would also seem desirable to make this battery available for other emergency aircraft use. (Non availability can not technically be considered a hazard since no second battery is presently available).

(2) Certain internal or circuit failures could cause the ICDU CRT to bloom to high brightness. If this were to occur to the pilot's CRT during night landing or night formation flight, it could probably have serious consequences. The failure probability is low and the percent time it could occur and present a hazard is low. The possible problem is being analyzed and probabilities will be computed. If simple effective circuitry can be added, it will also be considered.

No inherent safety problems are evident in the "A" Group installation. Many implementation details are yet to be checked as the design is approved at CDR and the final drawings are prepared. When these data are firm enough to represent the final product, this analysis will be updated.

Table II. Drawings Reviewed

ITEM NUMBER	DRAWING NUMBER	STATUS	TITLE	COMMENTS
1	40800	Preliminary	System Interconnect Drawing (A11 C-130)	Reviewed
2	408010	Preliminary	AWADS Changes	
3	408020	In Work	E, H, and WC E & H models	Not available
4	408030	In Work	HC models of H, N, & P	Not available
5	408040	In Work	Late H models	Not available
6	408050	In Work	C-130B	Not available
7	408100	Preliminary	Installation C-130 SCNS	Not available
8	408XXX	In Work	440 sub installation dwgs	Not available
9	SC862/A	System Sketch	None	Reviewed
10	408308	Preliminary	Copilots ICDU mount	Needs rubber pad
11	168647-01-01	Preliminary	SCNS Control Unit	OK
12	L0168648	Preliminary	Control Unit SCNS Display	OK
13	168700	Preliminary	SCNS Control Unit Light Panel	OK
14	L0168720	Preliminary	Control Unit Mode Select C-130	Reviewed

Table II. Drawings Reviewed (Continued)

ITEM NUMBER	DRAWING NUMBER	STATUS	TITLE	COMMENTS
15	408312	Preliminary	Copilot side panel assy	reviewed
16	L0408300	Preliminary	Equipment rack	reviewed
17	L0408605	Preliminary	DVS Adapter Ring	reviewed
18	168396-01-01	Preliminary	ICDU	reviewed
19	LG2905A	Preliminary	BICU Layout	reviewed
20	168124	Preliminary	Chassis, Elect Equip (BICU)	reviewed

Table III. Specifications and Documents Reviewed

ITEM NUMBER	DRAWING NUMBER	STATUS	TITLE	COMMENTS
1	CA1047-002	Preliminary	System Specification for the C-130 Self Contained Navigation System (SCNS) for the C-130B, C-130E (non AWADS), C-130H, HC-130N, HC-130P, WC-130E, and WC-130H Aircraft	
2	CA1047-001	Preliminary	Interface Specification for the C-130 Self Contained Navigation System (SCNS) for the C-130B, C-130E (non AWADS), C-130E (AWADS), C-130H, HC-130H, HC-130N, HC-130P, WC-130E, and WC-130H Aircraft	
3	CA1047-003	Preliminary	System Specification for the C-130 Self Contained Navigation System (SCNS) for the HC-130H Aircraft	
4	CA1047-004	Preliminary	System Specification for the C-130 Self Contained Navigation System (SCNS) for the C-130E (AWADS) Aircraft	

Table III. Specifications and Documents Reviewed (Continued)

ITEM NUMBER	DRAWING NUMBER	STATUS	TITLE	COMMENTS
5	CB1047-001	Preliminary	Critical Item Development Specification for the Integrated Control/Display Unit (ICDU) of the C-130 Self Contained Navigation System (SCNS) for the C-130B, C-130E (non AWADS), C-130E (AWADS), C-130H, HC-130H, HC-130N, HC-130P, WC-130E, and WC-130H Aircraft	Safety grounding paragraph added
6	CB1047-002	Preliminary	Critical Item Development Specification for the Bus Integration Computer Unit (BICU) of the C-130 Self Contained Navigation System (SCNS) for the C-130B, C-130E (non AWADS), C-130H, HC-130H, HC-130N, HC-130P, WC-130E, and WC-130H Aircraft	Safety grounding paragraph added
7	CB1047-003	Preliminary	Computer Program Development Specification for the Integrated Control/Display Unit (ICDU) of the C-130 Self Contained Navigation System (SCNS) for the C-130B, C-130E (non AWADS), C-130E (AWADS), C-130H, HC-130H, HC-130N, HC-130P, WC-130E, and WC-130H Aircraft	

Table III. Specifications and Documents Reviewed (Continued)

ITEM NUMBER	DRAWING NUMBER	STATUS	TITLE	COMMENTS
8	CB1047-005	Preliminary	Addendum to Critical Item Development Specification. Specification No. CB1047-002, for the Bus Integration Computer Unit (BICU) of the C-130 Self Contained Navigation System (SCNS) for the C-130E (AWADS) Aircraft	
9	YV1237	Preliminary	The Program/Hardware Interface Specification (PHIS) for the Integrated Control/Display Unit (ICDU) Model 2580F	
10	YV1238	Preliminary	The Program/Hardware Interface Specification (PHIS) for the Bus Integration Computer Unit (BICU) Model 2905A and 2905B	

SYSTEM SCNS

SUBSET Group A

SUBSYSTEM HAZARD ANALYSIS

PAGE 1 OF 3
ISSUE DATE _____ REV _____

ITM NO.	OP MODE	FAILURE MODE	FAILURE EFFECT	HAZARD DESCRIPTION	CL	LV	CONTROLS & COMMENTS
1.	All	Damage in area of Mux Bus Coupler Location	Loss of coupling between system LRUs	1553 Mux Bus Couplers concentrated in one location. Vulnerable to damage	IV	E	Was changed to distribute 2 port couplers with "A" and "B" bus separated physically
2.	All	Discharged INS Battery	High current charge rate	Extremely high current charge rate might cause excess hydrogen and oxygen out-gassing into battery compartment, overheating of wiring and battery, possible explosion or acid leakage	II	B	It would appear that some form of charge current limiting would be in order, however, batteries across the bus have been used for years and the added battery is connected the same as the existing aircraft battery. This needs investigating to determine if it has not been sufficiently addressed
3.	All	Main aircraft battery discharged	Critical operation or functions not available in emergency	Failure to start aircraft in emergency. Loss of essential Instruments in a flight emergency.	III	C	Provide ability to electrically substitute INS battery for aircraft battery under emergency conditions i.e., a bus tie-in
4.	VOR NAV	Controlling ICDU fails	VOR controlled by that ICDU is inoperative due to loss of primary power	Loss of VOR NAV capability when pilots and C.P. ICDUs are inoperative	III	D	Still provides dual redundancy although VORs could be operated from any ICDU over MUX bus if they could be powered up

CLASS: I CATASTROPHIC
II CRITICAL
III MARGINAL
IV NEGLIGIBLE

LEVEL: A - FREQUENT
B - REASONABLE PROBABLE
C - OCCASIONAL
D - REMOTE
E - EXTREMELY IMPROBABLE
F - IMPOSSIBLE

SYSTEM SCNS SUBSYSTEM

SUBSET Group A HAZARD ANALYSIS

ISSUE DATE _____ REV _____

ITM NO.	OP MODE	FAILURE MODE	FAILURE EFFECT	HAZARD DESCRIPTION	CL	LV	CONTROLS & COMMENTS
5.	VOR NAV	Failure in SCNS control panel or power source	No VOR NAV ability	An alternate solution to 6 above is to power the VORs directly from the SCNS control panel. Any ICDU could then operate either VOR. Loss of SCNS power will result in loss of radio aids in either case. (See next item.)	III	D	This problem would only occur with combat damage or any overload problem opening the circuit breaker. This could also happen with 6 above. This is the better solution of the two.
6.	All	SNCS Control Panel power fail	Loss of all SNCS functions. Loss of all SCNS controlled radios (UHF #1 available through manual control)	Total loss of mission effectiveness. Loss of all IFR NAV equipment. Single point failure.	II	D	This probability is extremely remote except for combat damage. Since the system is intended for combat use, it has been considered. A second protected backup power-on switch will be installed for emergency use. This reduces to CL = IV and LV = E.
7.	Flight	Loss of electrical power	Loss UHF #1 as well as all other comm radios	Loss of last available comm radio	III	D	Radio powered from isolated DC and battery bus and in emergency is controlled from a backup standard control head. This is best backup presently available (make switchable power source to INS Battery for additional redundancy).

CLASS: I CATASTROPHIC
II CRITICAL
III MARGINAL
IV NEGLIGIBLE

LEVEL: A - FREQUENT
B - REASONABLE PROBABLE
C - OCCASIONAL
D - REMOTE
E - EXTREMELY IMPROBABLE
F - IMPOSSIBLE

SYSTEM SCNS

SUBSET Group A

SUBSYSTEM HAZARD ANALYSIS

ISSUE DATE _____ REV _____

ITM NO.	OP MODE	FAILURE MODE	FAILURE EFFECT	HAZARD DESCRIPTION	CL	LV	CONTROLS & COMMENTS
8.	Flight	Attitude reference source failure and switching.	Possible unexpected effects on AFCS stability or decoupling. May effect yaw damper.	Switching references or obtaining references from mixed sources may occur upon certain failures and redundancy switching.	III	C	This possible condition has not been evaluated and will be reported on in the next SSHA edition.
9.	Night flight	ICDU CRT failure to control brightness.	Sudden CRT screen blooming to full brightness.	Temporary blinding pilot to outside view of critical moment of air drop landing or formation flight.	II	E	The hazard could be serious as would any blinding effect be. The probability of the failure is low and will be analyzed to the piece part and reliability numbers attained. If it were to occur, the timing would also have to be critical; hence the timing probability is low. There are not many failsafe schemes to control this low probability but innovative BIT circuits will be explored.
10.	Flight	BICU fails-turned off.	AWADS Radar unusable.	AWADS Radar needed for weather avoidance and possibly Map mode.	III	D	The BICU reliability will probably exceed that of the Radar. It would be desirable however to design the control and interconnect to the Radar to allow a default mode for scanning of weather or the ground (Map) even without lateral, pitch, or roll stabilization control. This will be evaluated and reported in the next SSHA edition.

CLASS: I CATASTROPHIC
II CRITICAL
III MARGINAL
IV NEGLIGIBLE

LEVEL: A - FREQUENT
B - REASONABLE PROBABLE
C - OCCASIONAL
D - REMOTE
E - EXTREMELY IMPROBABLE
F - IMPOSSIBLE

END

FILMED

5-86

DTIC