National Aeronautics and
Space Administration

Lyndon B. Johnson Space Center
Houston, Texas
77058

Reply to Attn of: CB

March 31, 1998

TO: XA/ Manager, EVA Project Office
EA/ Director, Engineering Directorate

FROM: CB/Chairman, USA Simplified Aid For EVA Rescue (SAFER) Failure Review Board

SUBJECT: Review of STS-86 USA SAFER failure

The USA SAFER Failure Review Board (FRB) has completed its investigation into the failure of USA SAFER serial number #1005. Please find attached the Board's report which outlines our findings and recommendations. As part of this investigation, a "mini" independent peer review of findings and redesign options under consideration was held.

The JSC Automation, Robotics, and Simulation Division will carry the FRB's work forward through the design review process and will ensure implementation of the FRB's recommendations. The Integrated Product Team (IPT) process headed by XA/A. Huynh will provide guidance from the EVA Project Office.

Only selected excerpts from data gathered and tests conducted are included in this report in an effort to keep the report a reasonable length. All data gathered during this investigation has been assembled by the Automation, Robotics, and Simulation Division and is available on request by contacting the Division Office or the FRB Secretary.

Members of the USA SAFER FRB are to be commended for their hard work. They fully supported the FRB's efforts via timely responses to inquiries, thorough support, and strong efforts to recover from the failure.

Steve Smith
Chairman, USA SAFER Failure Review Board

cc:

AC/M. Foale	DF/S. Rainwater	NA/J. Casper
CB/M. Bloomfield	EC/S. Poulos	NT3/S. Schenfield
CB/S. Parazynski	ER/W. Guy	XA/D. Adlis
CB/D. Leestma	ER/G. Gutkowski	XA/A. Huynh
CB/K. Cockrell	ER/K. Lewis	FRB Members (20)
CB/M. Lee	ER/C. Woolley	

STS-86 USA SIMPLIFIED AID FOR EVA RESCUE (SAFER) FAILURE

MISHAP DATE: October 1, 1997

FAILURE REVIEW BOARD REPORT

March 30, 1998

National Aeronautics and Space Administration

Lyndon B. Johnson Space Center
Houston, Texas

STS-86 USA SAFER FAILURE
MISHAP DATE: October 1, 1997
FAILURE REVIEW BOARD REPORT

The subject failure has been investigated and this report contains the facts, findings and recommendations of the Board. Board members are unanimous in all areas.

CB/Steve Smith
Board Chairman

ER5/Gary Gutkowski
Lead ER/Automation, Robotics and Simulation Division Board Member

EC/Steve Poulos
Lead XA/EVA Project Office Board Member

STS-86 USA SAFER FAILURE
MISHAP DATE: October 1, 1997
FAILURE REVIEW BOARD REPORT

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

National Aeronautics and
Space Administration

Lyndon B. Johnson Space Center
Houston, Texas
77058

Reply to Attn of: CB

March 31, 1998

TO: XA/ Manager, EVA Project Office
EA/ Director, Engineering Directorate

FROM: CB/Chairman, USA Simplified Aid For EVA Rescue (SAFER) Failure Review Board

SUBJECT: Review of STS-86 USA SAFER failure

The USA SAFER Failure Review Board (FRB) has completed its investigation into the failure of USA SAFER serial number #1005. Please find attached the Board's report which outlines our findings and recommendations. As part of this investigation, a "mini" independent peer review of findings and redesign options under consideration was held.

The JSC Automation, Robotics, and Simulation Division will carry the FRB's work forward through the design review process and will ensure implementation of the FRB's recommendations. The Integrated Product Team (IPT) process headed by XA/A. Huynh will provide guidance from the EVA Project Office.

Only selected excerpts from data gathered and tests conducted are included in this report in an effort to keep the report a reasonable length. All data gathered during this investigation has been assembled by the Automation, Robotics, and Simulation Division and is available on request by contacting the Division Office or the FRB Secretary.

Members of the USA SAFER FRB are to be commended for their hard work. They fully supported the FRB's efforts via timely responses to inquiries, thorough support, and strong efforts to recover from the failure.

Steve Smith
Chairman, USA SAFER Failure Review Board

cc:

AC/M. Foale	DF/S. Rainwater	NA/J. Casper
CB/M. Bloomfield	EC/S. Poulos	NT3/S. Schenfield
CB/S. Parazynski	ER/W. Guy	XA/D. Adlis
CB/D. Leestma	ER/G. Gutkowski	XA/A. Huynh
CB/K. Cockrell	ER/K. Lewis	FRB Members (20)
CB/M. Lee	ER/C. Woolley	

SECTION 1
Failure Review Board Members

Steve Smith	CB/Astronaut Office	Board Chairman
Gary Gutkowski	ER5/Automation, Robotics & Simulation Division (AR&SD)	Lead, EA
Steve Poulos	XA/EVA Project Office	Lead, XA
Rich Bussey	ND365/Ops & Quality Assurance	O&QA
Jeff Bye	ER4/AR & SD	Avionics
Ron Cook	NC63/Safety & Mission Assurance	S&MA
Eric Darcy	EP5/Energy Systems Division (ESD)	Batteries
Chris Estrada	NC63/Safety & Mission Assurance	S&MA
Lee Graham	ND	Systems/Ops
Karl Hamelmann	NS22/S&MA	Reliability
Carol Harris	ER12/AR & SD/EASI	Board Secretary
Hal Hiers	ER2/AR & SD	Software
Brent Hughes	LM/C18	Batteries
Anh Huynh	XA/EVA Project Office	Project Mgt.
Eric Kimball	ND365/Op & Quality Assurance	O&QA
Joe Lepore	LM/C70	Thermal
Kevin Lewis	ER6/AR & SD	Development Mgr.
Tricia Mack	DF4/Mission Operations Directorate (MOD)	EVA Operations
Doug Seiler	ND363/Ops & Quality Assurance	O&QA
Gail Steele	ER/AR & SD/HEI	Systems/Ops
Bill Studak	EP/ESD	Propulsion
Keith Van Tassel	EP5/ESD	Pyrotechnics
Kenny Vassigh	DF4/MOD	EVA Operations
Chuck Woolley	ER5/AR & SD	Development Mgr.

SECTION 2
Executive Summary

NOTE: THE SAFER DESIGN WORN ON STS-86 AND THE SUBJECT OF THIS INVESTIGATION IS THE USA SAFER DESIGN AS OPPOSED TO THE RUSSIAN SAFER DESIGN CURRENTLY UNDER DEVELOPMENT.

On October 1, 1997, Astronauts Scott Parazynski (EV1) and Vladimir Titov (EV2) conducted an EVA from the hatch of Atlantis while the shuttle was docked to the Mir space station. Both EVA crew members wore the USA Simplified Aid For EVA Rescue (SAFER). SAFER is a self contained "jet backpack" that is worn on the EVA suit; it is battery powered with a nitrogen propulsion system. During the EVA, a SAFER would have been activated and used to fly back to the shuttle/station stack if a crew member had become detached. This was the first flight of this SAFER design. The SAFER design worn on missions STS-64 and STS-76 did not feature the same propulsion system features as the STS-86 design.

During the EVA, neither crew member became detached. However, as planned pre-flight, at the completion of the EVA, EV1 performed a test on his SAFER unit. EV1 entered a foot restraint to secure himself and powered on his SAFER unit. He then went through a range of motions to verify the operation of the SAFER. Indications to EV1 were as planned: his hand controller indicated thruster operations (the thruster Light Emitting Diode (LED) was illuminated) and nominal computer operations (automatic attitude hold (AAH) was engaged as indicated by the AAH LED). EV1 could also hear the thrusters opening and closing. He could not feel any thrust from the firings; this was not a surprise as it was determined preflight that the small thrust force (approximately 1.6 pounds) would likely not be felt while the crew member was in a foot restraint. EV1 then powered the SAFER down and the EVA was completed.

Post flight inspection (11/4/97) showed that the SAFER worn by EV1 had not operated as planned: nitrogen gas had not been delivered from the supply tank to any thrusters. It appeared that the NASA Standard Initiator (NSI) pyrotechnic device, which is in place to open the propellant system's pyrotechnic isolation valve, had not fired. Both SAFER units from the flight and the non-flown spare (3 total) were immediately impounded and the EVA Project Office Manager established the SAFER Failure Review Board (FRB).

The three SAFER flight units were fully inspected and photographed at KSC - no significant damage was found. The units were then shipped to JSC. The SAFER FRB established an investigation plan and fault tree. Analysis of the suspect SAFER unit included subsystem standalone, integrated , and thermal testing. JSC personnel were consulted on NSI use and dynamics. The design history of SAFER was thoroughly reviewed.

FAILURE AND MAIN CONTRIBUTING FACTOR

The NSI in the SAFER (serial #1005) did not fire. Therefore, the pyrotechnic propellant isolation valve did not open and nitrogen gas was not sent to the SAFER's thrusters.

The NSI did not fire because there was a change in the NSI resistance as the NSI "fire" current pulse was applied to the NSI by the avionics circuit. This caused the NSI "fire" current level (designed at 4.1 amps) to drop (to 2.8 amps) below the "all fire" (3.5 amps) NSI current specification. The NSI resistance was measured at 1.09 ohms before installation into the SAFER. During application of the "fire" pulse, the resistance changed due to "ohmic heating" to approximately 1.6 ohms. The change in resistance caused the 4.1 amp NSI "fire" pulse to drop to 2.8 amps because of the avionics circuit constant voltage design. At 2.8 amps, the probability of firing the NSI is approximately 60%.

CONTRIBUTING FACTORS

The electrical characteristics of the NSI were not completely understood by the SAFER community during the design process. Thus the firing circuit design did not accommodate an important attribute of the NSI. The circuit was designed assuming the NSI resistance was 1.05 +/- 0.1 ohms as listed on the manufacturer's data sheet.

The SAFER avionics circuit could not supply more than 2.8 amps as the NSI resistance increased because of its "constant voltage" design (V=IR, Voltage = Current x Resistance). Aboard the shuttle, there is only one other known NSI system with this circuit approach (the non-critical aft hazardous gas sampling system). A typical NSI circuit uses a capacitive discharge approach to fire the NSI. In capacitive circuits, large, excessive amounts of power are delivered to the NSI.

Based on the manufacturer's specification of NSI resistance R = 1.05 +/- 0.1 ohms, an inaccurate NSI emulator, a 1 ohm resistor, was selected and used extensively during design, certification and acceptance. The emulator was never verified against a real NSI being fired. Several development tests were classified as "successful" erroneously because the inaccurate emulator was used.

The avionics circuit was changed after the Critical Design Review (CDR) due to a thermal test failure to fire an NSI which was traced to SAFER battery thermal limitations. Rather than changing the battery design, the avionics was changed to reduce battery load from 160 watts to 60 watts. The pre-CDR avionics design would likely have fired the NSI (if given sufficient battery power) because it used a 24 volt source versus the STS-86 flown design which used a 5 volt source.

There were significant schedule pressures. Three flight units were required to be on dock at KSC only 100 days after the thermal test failure.

The post-CDR design provided little margin. The design current (4.1 amps) was very close to the all-fire (3.5 amps) current and near an asymptote in a curve (Figure 10) of NSI current versus probability of NSI firing.

Only two NSI firings were attempted with the avionics redesign. Although both firing attempts were successful, they are considered "luck" based on probabilities (at 2.8 amps the probability of success is approximately 60%). The "successful" firings were therefore misleading. Both firings were conducted on the Certification Unit; no firings were ever attempted in any of the flight units.

Current traces of the NSI firing pulse were not taken during the two successful NSI firings. Access was difficult and it was felt that the successful firing of the NSI was sufficient data. Current traces taken during the NSI firings would have shown that the increasing NSI resistance was causing an unanticipated decrease in the current from the avionics to the NSI.

FINDING (not necessarily a contributing factor)

The post-CDR circuit design was not thoroughly reviewed by a significant number of knowledgeable, technical individuals nor independent experts. It was only reviewed by JSC ER personnel. The configuration control process did not require XA and/or EA to conduct a board review in order to approve the design change or to approve the test plan for the redesign. The process did not require the generation of a Change Request documenting the technical changes. Only a Change Request to technical requirements was required and approved.

MAJOR RECOMMENDATIONS and CHANGES

The SAFER avionics will be redesigned. Two options are under consideration. One of the options converts the constant voltage firing circuit to a capacitive discharge circuit.

The redesigned avionics should provide increased margin over the STS-86 flown design.

JSC development organizations developing products in-house must thoroughly follow JSC product development and project management guidelines. Thorough implementation of these guidelines will guarantee proper design review board membership and active member participation.

JSC design review guidelines should be modified to more clearly state the need for independent expert participation.

The technical change/configuration control process should be reviewed immediately and modified such that technical changes are thoroughly reviewed, approved, and documented.

An accurate NSI emulator should be developed , verified, and used for testing.

All NSI firings should be characterized with an inductive probe in order to accurately understand and document NSI current.

The redesign certification testing program should include a statistically significant number of NSI firings.

The acceptance testing for each redesigned flight unit should be modified to include NSI firings.

A **flight test** for the redesigned SAFER should be manifested at the first opportunity. Discussions have commenced on this topic with the EVA Project Office (XA) , the Automation, Robotics and Simulation Division (ER) , the Mission Operations Directorate (DF and DA), and the Flight Crew Operations Directorate (CB).

Further NSI testing should be performed in order to more completely characterize NSI performance in a constant voltage circuit. A thorough NSI "user guide" should be published.

SUMMARY

The USA SAFER design flown on STS-86 did not work for several noted reasons. The SAFER design team did not know that the NSI resistance would change. Thus, the resulting circuit design did not address this phenomenon. A more robust design review process or more thorough testing may have caught this flaw pre-flight. Only documenting the successful NSI test firings with an inductive current probe would have definitely identified the need to change the avionics design. Changes will be made to the circuit design, to the design review process, to the configuration control process, and to the testing process. The test plan for the redesign will be thoroughly reviewed as it is the key part of the failure recovery plan.

The specifics of all of the recommendations are in Section 6.

Several miscellaneous design change recommendations (also in Section 6), mainly to the battery, were also established by the FRB in order to improve the pre-EVA checkout capability of SAFER. These improvements will increase our confidence in a SAFER unit before it is donned for an EVA.

SECTION 3
Failure Description

NOTE: THE SAFER DESIGN WORN ON STS-86 AND THE SUBJECT OF THIS INVESTIGATION IS THE USA SAFER DESIGN AS OPPOSED TO THE RUSSIAN SAFER DESIGN CURRENTLY UNDER DEVELOPMENT.

The Simplified Aid For EVA Rescue (SAFER) unit is a self contained "jet backpack" that is worn on the back of the EVA suit (Figure 1). A SAFER unit must be worn by EVA crew members when the shuttle is docked with the a space station. During the EVA, SAFER would be used by a crew member if he/she became detached from the shuttle/space station stack. Upon becoming detached, the crew member would deploy the SAFER hand controller, power the unit on, and fly back to the shuttle/space station stack.

SAFER is powered by an external 36-volt battery pack located on the bottom of the SAFER avionics package . The nitrogen propulsion system (Figure 3) consists of a tank, a pyrotechnic ("pyro") valve, a manual isolation valve, a regulator, a relief valve, and 24 thrusters. The manual isolation valve is opened by the crew member before exiting for an EVA. The pyro valve is opened when the SAFER unit is turned on by taking the hand controller power switch to ON. The switch throw results in the generation of an electrical signal sent by the avionics to a pyrotechnic NASA Standard Initiator (NSI). The NSI is a simple system consisting of a thin wire (the 'bridge wire") which passes through the propellant (Figures 5 and 6). Current is applied to the bridge wire which heats up and eventually breaks (potentially explosively under high current). The NSI fires as the bridge wire heats and the resulting expanding gas opens the pyro valve. The NSI is used extensively on each shuttle flight (Figure 7). A pyrotechnic valve was selected because it hermetically seals the nitrogen supply tank to guarantee the units can last for at least 1 year between servicing as required for International Space Station operations. The SAFER thrusters may either be fired automatically by the SAFER avionics in an attempt to establish a stable attitude when in Automatic Attitude Hold, or by the crew member moving the hand grip on the hand controller.

On October 1, 1997, Astronauts Scott Parazynski (EV1) and Vladimir Titov (EV2) conducted an EVA from the hatch of Atlantis while the shuttle was docked to Mir. Both wore SAFER units. During the EVA, neither crew member became detached. However, as planned pre-flight, at the completion of the EVA, EV1 performed a test on his SAFER unit. EV1 entered a foot restraint to secure himself and powered on his SAFER unit. He then went through a range of motions to verify the operation of SAFER. Indications to EV1 were as planned: his hand controller indicated thruster firings and nominal SAFER computer operations ("attitude hold"). EV1 could also hear the thrusters opening and closing. He could not feel thrust from the firings; this was not a surprise as it was determined preflight that the small thrust force would likely not be felt while the crew member was in a foot restraint. EV1 then powered the SAFER down and the EVA was complete.

Post flight inspection (11/4/97) at the Kennedy Space Center (KSC) by Johnson Space Center (JSC) personnel showed that the SAFER unit worn by EV1 had not operated as planned: nitrogen gas had not been delivered from the supply tank to any thrusters. A JSC Discrepency Report was generated (Figure 4). Analysis and testing determined that the NSI had never fired and therefore the pyrotechnic valve had never opened.

SECTION 4

Method of Investigation

The SAFER failure was discovered on November 4, 1997. The failed unit (Serial #1005), the second flight unit (Serial # 1004 worn by EV2), the spare flight unit (Serial #1003), and their three batteries (Serial #'s 1010, 1008, and 1009) were immediately impounded at KSC. On November 5, the Manager of the NASA EVA Project Office, XA/Greg Harbaugh, asked Astronaut CB/Steve Smith to chair an STS-86 USA SAFER Failure Review Board (FRB). The FRB immediately took control of the impounded SAFER equipment. FRB membership was established by mid-November.

The first two FRB meetings were used to establish a SAFER configuration block diagram (Figure 2), a corresponding fault tree (Figure 8, which shows the final (12/10/97) FRB fault tree), and a general troubleshooting course of action (Figure 9). From these items, the FRB determined what testing should be accomplished at KSC before shipment back to JSC. Shipment was determined to have no effect on the condition of the units and only a thorough, physical inspection activity was scripted. The Boeing truck used to ship EVA hardware between KSC and JSC was obtained and sent to KSC so that the units could be quickly returned to JSC and kept under configuration control during transport.

The physical inspection at KSC (11/13/97) found no damage to structure; only minor MLI damage was found. The inspections were documented thoroughly with still and video photography. The units were placed on the Boeing truck and sent to JSC. The fault tree and general course of action were discussed and revised in preparation for the trouble shooting effort at JSC.

Several facts came out of these discussions and thorough subsystem reviews:

- Nearly all of the SAFER subsystems and their components are zero fault tolerant for operation. This is the design philosophy of the SAFER as it is a piece of emergency equipment.
- The avionics is designed to produce an NSI "fire pulse" amplitude (4.1 amps) that is near an extreme asymptote in a curve of NSI current versus probability of NSI firing (Figure 10). The "all fire" NSI current level (100 % probability) is 3.5 amps; at 2.5 amps, the probability is approximately 50%.
- The SAFER avionics used a constant voltage source (Figure 15) to generate the NSI firing pulse with little design margin. The great majority of NSI circuits use a capacitive discharge circuit to supply the NSI fire pulse. Capacitive discharge circuits are designed to supply substantial power and margin. (Note: it was later documented, in early December, that these circuits are also insensitive to changes in NSI resistance.)
- Only the single SAFER Certification Unit (#1002) went through a complete thermal and vacuum test process during which only 2 NSI's were actually fired (one cold case at -4F (R=1.09 ohms) and one hot case at +137F (R=1.11ohms)).
- A 1 ohm resistor was used as an NSI emulator during many tests.
- During the actual NSI firing events, the NSI current was not recorded because of difficult access for an inductive probe and because the success of the NSI firing was assumed to be "enough."
- NSI's were never test fired in any flight SAFER units. Flight units were accepted based on a simplified test regime and by similarity to the Certification Unit .
- The SAFER "Self Test" does not check the complete NSI firing circuitry. The Self Test only checks the continuity of the NSI with a 5 milliamp trickle current.
- The SAFER "Self Test" does not thoroughly check battery capability.
- All 3 of the battery's strings must be operational to reliably fire the NSI.
- NSI's are incredibly reliable if supplied with enough current. Nearly 100 NSI's are used every shuttle mission (Figure 7) and to anyone's memory, none had ever failed to fire. They are simple, reliable devices.

Testing then began (11/17/97). Subsystems from the incident SAFER unit were tested independently at ambient temperatures to verify their operation. The NSI resistance was measured to be 1.09 ohms, the same resistance value measured pre-flight. This verified that the NSI had not been fired during the flight and explained why the propulsion pyro valve had not been opened. The NSI was almost completely eliminated from the suspect list because of its simplicity, design, and performance history. The battery (Serial #1010) was tested and its voltage was an acceptable 33.4 volts and the battery operated nominally under 1, 2, and 3 amp loads. The avionics system was then tested using a battery emulator: as designed, the avionics (Figure 15) generated a 4.1 amp, 47 millisecond (ms) "fire" pulse as measured (Figure 12) through the 1 ohm resistor serving as an "NSI emulator." The pulse duration is controlled by the main SAFER microprocessor and it is several times the minimum requirement (5 ms) found through analysis and test. Throughout testing the duration was found to be very repeatable.

The battery and avionics were then tested together at ambient; both worked nominally and the 4.1 amp 47 ms pulse was again observed through the NSI emulator.

The effort was then focused on the thermal environment. In particular, battery performance is known to degrade at low temperatures and an effort was made to establish the temperature profile during the EVA. EVA task timelines, downlink video, console logs and as flown attitudes were used to establish the temperature timeline for the SAFER unit worn by EV1. The analysis was reviewed by EV1 and his comments were incorporated. The results indicate (Figure 11) a benign environment - all SAFER components were "well within operational limits." The battery temperature at SAFER activation was 28 degrees F, well above any temperature at which performance would have been significantly degraded.

The elimination of the thermal environment as a suspect influence was also verified by a series of thermal tests conducted (11/20/97) in Chamber H, Building 33 at JSC. The suspect SAFER unit and battery, other SAFER batteries, and several NSI's similar to the NSI in the suspect SAFER unit were placed in the chamber. The avionics and battery were examined independently at 1 degree F. Both worked nominally; again, the 4.1 amp 47 ms avionics pulse was measured through the NSI emulator (measured at 0.98 ohms).

The battery and avionics were then paired together with the NSI emulator and the results were nominal.

The chamber testing also did much to nearly eliminate a battery failure mode called "voltage delay." Voltage delay is a characteristic of some battery chemistries. After a period of no usage, a battery with voltage delay will take some time (a "delay") to come up to its nominal voltage when turned on because a chemical passivation layer, which developed during the off time (a few days is all it takes), has to be broken down. If the delay occurred during the avionic's attempts to generate the NSI fire pulse, it was theorized that the pulse would be absent or undersized thereby not giving the NSI the necessary energy. The SAFER battery's chemistry, Li/MnO_2, is not known for having a voltage delay according to industry, military, and intelligence community experts. Neither battery #1008 or #1010 showed voltage delay after several dormant days. If passivation was typical of these batteries, it would have been observed in these tests.

Still at 1 degree F in the chamber, the avionics and battery were hooked to an NSI very similar (manufacturer, resistance, etc.) to the NSI which did not fire in SAFER Unit #1005. The NSI was placed in an instrumented (explosion proof) container (termed a "bomb") rather than the real pyro valve. This technique allowed NSI testing to take place without involving the pyro valve which is a single use, expensive item. **When the SAFER was activated, the NSI did not fire**. An inductive probe was then placed into the NSI circuit and the SAFER activated again. The NSI again did not fire - the current trace (Figure 13) showed that the NSI current had started at a current of 4.1 amps, but dropped immediately. The current dropped below the "all fire" NSI specified current of 3.5 amps in less than 1 ms and to approximately 2.8 amps within 3 to 4 ms. This was the first time in the SAFER design process that an NSI firing attempt had been conducted with an inductive current probe in the NSI circuit. Recalling the electrical equation V=IR (voltage = current x resistance), when assembled as an integrated system, the NSI circuit resistance was increasing, thus decreasing the current to the NSI.

Similar performances of the independent parts and the integrated system were found (11/21/97) at 20, 40 and 70 degrees F. Thermal environment appeared to have no influence on the failure.

A review of the Fault Tree (Figure 8) at this time showed that every path (ironically) had been traced successfully. Focusing on page 4 of 10 of Figure 8, the chamber testing had shown that insufficient power (current) was being sent by the Valve Drive Assembly (VDA) to the wiring harness (W/H) going to the NSI. This condition is represented at the top of page 4 of Figure 8 by Block G009. Some fault phenomenon unknown to the FRB was occurring when the system parts were integrated. The separate pieces of the design were performing as designed when tested separately.

A summary of the data at this point showed: (1) that the resistance of the NSI firing circuit was increasing (Figure 13), (2) that the success of the two NSI firings on the certification unit could have been probability/luck (Figure 10) shows a 60% probability of a firing at 2.8 amps), and (3) that the failure of the flight unit and the Chamber H firing attempts was also probability/luck.

A very experienced JSC NSI expert who was not involved in the SAFER design nor involved in the FRB's work to this point then provided the missing fact. In his experience, he had heard that an NSI's bridge wire resistance would increase (due to ohmic heating) when a current pulse was applied.

To investigate this theory, two NSI's were tested (11/24/97) with the SAFER Certification Unit. In both cases, the current trace showed the behavior seen in the Chamber H tests. The current peaked above 4 amps but then dropped within approximately 3 ms to approximately 2.4 amps indicating a rise in the NSI circuit resistance. Two more NSI's were then tested in SAFER Unit #1005 and the same behavior was observed. In all four cases "downloaded" NSI's were used. Downloaded NSI's are exactly the same as flight ready NSI's except that their propellant has been removed. The lack of propellant had minimal influence on the results yet it allowed the testing to occur in the on-site SAFER laboratory. Firing flight ready NSI's requires much more precaution, paperwork, and the work cannot take place in the SAFER lab.

The two NSI suppliers to NASA, Hi Shear and UPCO were contacted and asked about their knowledge of the resistance change phenomenon. Neither company had any data on this subject since most NSI users send a tremendous amount of energy to the NSI via capacitive discharge circuits. The NSI bridge wire fires almost explosively, immediately and no resistance change is noted or measurable.

To prove the theory that the successful and unsuccessful firings were based solely on probabilities (recall Figure 10), a simple statistical analysis was performed. The analysis showed that if 14 different NSI firings were attempted and none fired then the circuit would NEVER fire an NSI with 99.99% certainty. A test plan was drawn up to obtain 14 NSI's similar to the flight failure NSI. Each NSI firing would only be attempted once (repeated firings can "glaze" the bridge wire thus affecting its probability of firing) and the firing was in the instrumented "bombs" used previously. The flight unit and flight battery would be used. If and when an NSI fired, the test would be halted.

The first of the 14 NSI's was loaded into SAFER unit #1005 with battery #1010 (the incident SAFER unit and battery). **The SAFER unit was activated and this first NSI successfully fired**. This was the first NSI ever fired in this flight unit and the first NSI firing ever documented with an inductive current probe recording NSI current.

The current trace (Figure 14) showed the same behavior as seen in the previous tests: the current was 3.5 amps (on its way to 4 amps when the resistance change occurred), then dropped to 2.7 amps (indicating the resistance change). The current then dropped to zero when the NSI fired. The FRB concluded that the flight SAFER failure was due to the change in resistance of the NSI and the constant voltage circuit's inability to supply 3.5 amps or more to the NSI. The resistance change drove the circuit's current down to 2. 8 amps (60% probability of successful firing point), below the 3.5 amp "all fire" value. The successful firing of two NSI's in the certification unit and the failure of the NSI to fire in Unit #1005 during STS-86 were due to probabilities.

A review of the design history of the avionics was conducted. Several of the findings suggest that a more thorough design review process (including a review of the testing plan) should have been held. However, the FRB recognizes that few people are aware of the phenomenon that caused the failure and that there is a possibility even a more robust design review might not have caught the problem.

Some of the findings from the history review:

- The SAFER community did not know that the resistance of an NSI changes (due to ohmic heating) as current is applied and the NSI bridge wire temperature increases. Therefore, the design assumed that the NSI resistance, per the manufacturer's specification sheets, was 1.05 +/- 0.1 ohms and that the "all fire" current was 3.5 amps.
- Pyrotechnic personnel working with SAFER personnel assumed the new circuit could supply a constant current (of 4 amps) and they were only "vaguely aware" of the changing resistance phenomenon. Their experience was almost solely with capacitive discharge NSI circuits.
- Pyrotechnic (pyro) personnel did not review the SAFER circuit design because:
  (1) SAFER personnel did not make strong, clear requests to pyro personnel to review the design.
  (2) Pyro personnel did not take it upon themselves to review the design.
- Industry knowledge and data on the NSI phenomenon is very limited because most of their experience is with capacitive discharge circuit users. Tremendous power is supplied in these cases.
- Every test of the avionics system design used the NSI emulator, a 1 ohm (constant resistance), chosen because the NSI resistance specification was advertised as 1.05 +/- 0.1 ohms. Every current trace recorded during development did not show the real behavior of an NSI. The emulator had never been verified against a real NSI.
- The SAFER team selected the "constant voltage" approach because:
  (1) The NSI specification simply indicated a required current (3.5 amps or higher) to fire the NSI
  (2) The NSI specifications suggested the resistance was constant ("1.05 +/- 0.1 ohms")
  (3) The avionics designer <u>did not know</u> that other NSI systems (shuttle and non-shuttle) largely used the capacitive discharge circuit approach.
  (4) No technical/independent review of this "constant voltage" choice ever took place.
- The SAFER avionics "fire" circuit was changed after the Critical Design Review (CDR) due to a thermal test failure to fire an NSI which was traced to the battery's inability to supply enough energy at lower than -4 F.
- The baseline CDR design avionics likely would have fired the NSI reliably (if it had been supplied with sufficient battery power) because it used a much higher voltage source (24 volts versus 5 volts).
- <u>The SAFER project was under significant schedule pressures</u>. The thermal test NSI failure to fire occurred on May 13, 1997. Three flight units were required to be on dock at KSC only 100 days later on August 22.
- The SAFER Team chose to modify the avionics instead of the battery because of schedule and cost. Changing the battery seemed excessive. The redesign chosen required relatively minor changes to the Valve Driver Assembly Board (some rewiring, minor component change out), required no changes to the Power Supply Board, and it reduced the load on the battery 62% (160 to 60 watts). The redesigned avionics (in bread board form) was back in the thermal chamber in 8 days.
- The post-CDR circuit design was not thoroughly reviewed by a significant number of knowledgeable, technical individuals nor any independent peers.
- Pyrotechnic personnel did not know that the circuit design was being changed.

- The only Change Request circulated to the JSC community for review of the redesign only changed the requirements for the Valve Drive Assembly (VDA) Board. The design change was not presented nor was any technical justification given for the redesign selected. The VDA requirements change was buried in a lengthy "Super CR (Change Request)" and CR approval did not require the reviewers to review the circuit design.
- The technical change ("nuts and bolts of the change") to the SAFER avionics design did not go through any extensive board review or authorization process. Therefore, the change to the SAFER configuration was made without significant technical or independent review. Paragraph 3.7 "Configuration Management" of the SAFER Project Requirements Document states "After release of flight drawings, configuration changes which do not affect the requirements of this document will be subject to the approval by an Automation, Robotics, & Simulation Division (AR&SD) design review board." There are no minutes indicating that a board-type review was ever held. There is no documentation reflecting the approval of the redesign.
- Only the single SAFER Certification Unit went through the complete thermal and vacuum process during which only 2 NSI's were fired.
- Flight unit acceptance testing was limited (vibration, simple thermal, simple ops) and acceptance was based on similarity to the certification unit. NSI's were never fired in any of the flight units.
- Current traces of the NSI firing pulse were not taken during the real firing of the two NSI's. Access was difficult and it was felt that the successful firing of the NSI was sufficient data. Current traces would have shown the lower than expected current level due to the changing resistance.

Building on the observation that an independent peer type review should have been held (perhaps by carefully selecting the Critical Design Review participants), the SAFER FRB held an independent peer review on January 27, 1998. JSC experts in the fields of avionics, pyrotechnic devices, propulsion, software, and batteries were asked to review the FRB's findings, recommendations, and technical directions. None of the experts had previous experience with SAFER. The experts were:

1.	Frank Alanis	EP5	Pyrotechnics
2.	Robert Bragg	EP5	Batteries
3.	John Casey	EP5	Software
4.	William Hoffman	EP5	Pyrotechnics
5.	Darrell Kendrick	EP4	Propulsion
6.	Harold Vang	EV2	Avionics

The peer review attendees felt that the FRB's troubleshooting efforts were acceptable and that the major and contributing factors were accurately identified. Two alternative design solution concepts were presented to the peer attendees: one option (Figure 16) uses the same basic STS-86 design concept but with voltage source (increased from 5 to 9 volts) and resistance modifications. The second option (Figure 17) involves a replacement of the current avionics approach with a "capacitive discharge" circuit similar to the design found on most other NSI systems. The peer group felt that both options were worth pursuing further and that the final candidate should be chosen, in general, based on which options provides the most margin (assuming there are no other major performance, cost, and/or schedule differences).

As of this publication date, work is continuing on both options. Selection of the final circuit design will be via the normal design review process with guidance from the EVA Project Office

SECTION 5
Findings Contributing to the Failure

TECHNICAL FINDINGS

Technical Finding #1: SAFER #1005's NSI did not fire because insufficient current (2.8 amps) was provided to the NSI bridge wire.

Technical Finding #2:The NSI's resistance changed from 1.09 ohms to approximately 1.6 ohms when the "fire" current pulse from the SAFER avionics was applied to the NSI. The increased resistance caused the current to drop from 4.1 amps to 2.8 amps, well below the all fire 3.5 amp current.

Technical Finding #3: The SAFER avionics circuit could not supply more than 2.8 amps when the NSI resistance increased to approximately 1.6 ohms because of its "constant voltage" design (V=IR, voltage = current x resistance) .

Technical Finding #4: The SAFER circuit was designed using an NSI resistance spec of 1.05 +/- 0.1 ohms and an all fire current of 3.5 amps. .

Technical Finding #5: The SAFER circuit avionics design point provided little margin. The design current (4.1 amps) is near an asymptote (3.5 amps) in the NSI probability-of-firing curve. A small drop in NSI current dropped the probability of a successful firing dramatically.

Technical Finding #6: Based on a manufacturer's specification of R = 1.05 +/- 0.1 ohms for the NSI, a 1.0 ohm resistor was selected and used throughout the design process as an NSI emulator. This emulator was never verified against a real NSI during an NSI firing. An inaccurate emulator was used during the development and acceptance prrocesses.

Technical Finding #7: Several traces were recorded using the NSI emulator and each suggested a sufficient and consistent NSI fire pulse. These "successes" may have reduced the number of NSI firings deemed necessary in the certification and acceptance testing processes.

Technical Finding #8: A current trace was not taken during the firing of NSI's (2) during the certification program.

Technical Finding #9: The successful (2) NSI firings during the certification process were "luck" based on probabilities.

Technical Finding #10: Fabrication procedures for the SAFER battery do not include steps to verify the battery strings (3) are each functioning nominally. All 3 strings are required for reliable, repeatable NSI firings at the worst case cold temperatures.

Technical Finding #11: The SAFER status and fault detection software does not truly verify battery capability. There is no capability to verify all 3 battery strings are nominal. Only battery voltage, battery temperature, battery capacity remaining, and out-of-limits alerts for these parameters are reported.

Technical Finding #12: There is no verification of nitrogen pressure or temperature on the downstream side of the manual isolation valve.

Technical Finding #13: There is no thorough NSI User's guide available to potential users of the NSI.

Technical Finding #14: There is no specification available stating the energy versus dwell time for NSI users implementing a capacitive discharge firing circuit.

PROCESS FINDINGS

Process Finding #1: Personnel designing SAFER were not aware of the phenomenon of an NSI's resistance changing. Pyrotechnic experts involved in the SAFER project were only vaguely aware of the phenomenon. Industry information on the subject is non-existent. The SAFER designers assumed NSI resistance was 1.05 +/- 0.1 ohms, that the all fire current was 3.5 amps, and that the minimum pulse was 5 ms.

Process Finding #2: The decision to go with a constant voltage circuit versus a capacitive discharge circuit was never thoroughly discussed in any forum nor with independent technical experts.

Process Finding #3: The baseline avionics design was not robustly reviewed by a sufficient number of strong technical experts. The design was not reviewed by an independent peer group.

Process Finding #4: The avionics design was changed after the Critical Design Review (CDR) but there is no thorough, formal design review process in place for technical changes that take place after the CDR. The only documented process is stated in Paragraph 3.7 "Configuration Management" of the SAFER Project Requirements Document (PRD): "After release of flight drawings, configuration changes which do not affect the requirements of this document will be subject to the approval by an Automation, Robotics, & Simulation Division (AR&SD) design review board."

The SAFER PRD allowed changes to be made to the SAFER flight configuration without a thorough, independent review of the design change, technical reasoning, or planned testing. No one outside of the AR&SD was required to review the redesign. There is no documentation showing what review process and/or meetings were held to approve the redesign and the test plan. No one besides the circuit designer reviewed the technical details of the redesign.

Process Finding #5: The post-CDR effort was likely rushed by the tremendous schedule pressure for the STS-86 SAFER units.

Process Finding #6: The acceptance plan for each flight SAFER unit did not include an NSI firing. The (inaccurate) NSI emulator was used instead.

SECTION 6
Recommendations

Listed below are the recommendations from the SAFER Failure Review Board. In each case, the recommendation is followed by an explanation and/or comment. The JSC Automation, Robotics, and Simulation Division has been asked to guarantee that these recommendations are incorporated into future development projects, including the redesign effort for SAFER. Project management will be performed by the EVA Project Office.

Recommendation #1: *Redesign the SAFER avionics circuit which generates the NSI firing pulse. The redesign effort should consider swapping the circuit from a constant voltage circuit to a capacitive discharge circuit.*

Modification of the NSI fire circuit will resolve the technical cause of the STS-86 failure. The capacitive discharge alternative should be considered because it is the more common technique to fire an NSI and these circuits typically supply high power and therefore can provide increased margin.

Recommendation #2: *The redesigned SAFER avionics circuit should provide increased margin over the as-flown design.*

The design point, 4 amps, was very near the all-fire (100% probability) NSI current of 3.5 amps. Below 3.5 amps, the probability of successful firing dropped quickly and significantly (see Figure 10). This provided little margin when the current to the NSI did not meet the design value due to the NSI resistance change.

Recommendation #3: *JSC organizations responsible for in-house generated projects must thoroughly review JSC guidelines on product development and project management in order to guarantee proper and thorough development procedures (especially relating to review board membership and conduct) are implemented.*

Although the recommendation is formal in its reference to the JSC documents, the FRB notes that even without reference to the documents the developing organizations should have by the nature of the business identified the required expertise and individuals for the review process. And active participation should then have been mandated to meet the objective that the product was thoroughly review

The JSC Systems Level Procedure 4.4 and The Project Management Guide (JSC 61100) outline specifically how design review boards should be selected and conducted. The organizations developing SAFER did not robustly and fully follow these guidelines.

The FRB recognizes that a more robust design review may not have averted the failure. On the other hand, we will never know because there was not a robust design review. Most important, future products will benefit from implementing this recommendation.

Both referenced documents note specifically how review board members should be chosen. However, neither the baseline nor the revised SAFER avionics circuit designs were ever reviewed at the circuit design level by any qualified, "current" avionics experts outside of the designing organization. Although the baseline design may have been presented at the Critical Design Review forum, most if not all attendees and Board members had expertise and/or responsibility in other technical or process/management areas. The development organization should have guaranteed that other technical experts other than the designer reviewed the circuit.

The design review process placed all technical performance evaluation on the testing performed rather than preceding the testing with a more thorough technical review. Unfortunately, the testing process was flawed by the use of an inaccurate NSI emulator (see Technical Finding 6), probabilities (see Technical Findings 5 and 9), and limited NSI test firings (see Recommendations 9 and 10).

Recommendation #4: *Modify the JSC design review documents so that they clearly state the need for independent peer expertise participation.*

The JSC Systems Level Procedure 4.4 contains no reference to independent peer participation in the review process and The Project Management Guide (JSC 61100) makes only a short reference to this need. For in house generated products, this independent participation is crucial.

Neither the baseline nor the revised SAFER avionics circuit designs were ever reviewed at the circuit design level by independent avionics experts. Equipment developed outside NASA for the government has a natural peer review process built in when the contractor must present their product design to the government. The reviewing organization (the government) is independent of the designing/developing organization (the contractor).

Products developed in house at NASA do not have a built in peer review. Thus, development organizations within NASA must make an effort to obtain outside evaluators. This technique was employed and worked well for the JSC NASA developed SPIFEX product where independent JSC organizations chaired the Critical Design Review (CDR) and the developing organization guaranteed that independent experts in every field participated in the CDR.

The SAFER FRB held a mini peer review, as described in Method of Investigation, which agreed with the recovery plan and the general circuit layouts being considered . The Automation, Robotics, and Simulation Division should continue this approach with SAFER (and other in house developed products) during its redesign process.

Recommendation #5: *Modify the design change process in order to guarantee technical changes are thoroughly and independently reviewed and approved. The review process should include a review of test plans to verify the change. The results of the design change process should be documented.*

The SAFER avionics design was modified after the CDR due to the May 1997 failure to fire an NSI due to the battery. The redesigned circuit was never reviewed by anyone outside of the development organization. The redesigned circuit was never reviewed at a technical level by anyone except the designer. No paperwork such as a Change Request was ever generated for the redesign technical details. No independent board or technical body was ever educated on the design change or the philosophy behind the design change solution.

The only paper trail related to this change was a Change Request that noted the requirements change to the Valve Driver Assembly. This was a multi-page CR (a "Super CR") in which this requirements change was buried. Reviewers of any requirements change CR are not obligated to review technical details behind the requirements change. Additionally, these reviewers are not the appropriate personnel to perform a technical review. Some reviewers assumed that the design specifics would be reviewed in a technical forum.

Recommendation #6: *Review policy that gives configuration ownership and design change approval to the AR&SD.*

Not all of the SAFER FRB members felt that the AR&SD should have configuration ownership and design change approval responsibility. Thus, the policy should be reviewed.

All other tools used for EVA's are under the control of the EVA Project Office at JSC (Code XA). Technical changes to these tools are presented at a formal board (The EVA Hardware Board) which includes members from independent organizations. The EVA Hardware Board verifies the appropriate technical work has been accomplished (including testing or testing plans) before approving configuration changes via Change Requests. Meeting minutes are published.

Changes to the EVA space suit, the Extravehicular Mobility Unit (EMU), pass through a similar board, the EMU Board which is also chaired by The EVA Project Office. Configuration changes are presented along with the technical work and testing to support the change. Minutes are published. The Board consists of members from several organizations and Change Requests are the vehicle used to gain and document concurrence.

Recommendation #7: *An accurate NSI emulator (or process) should be developed and verified by test for use in the development process.*

Based on the NSI manufacturer's specification of R = 1.05 +/- 0.1 ohms, an inaccurate NSI emulator, a 1 ohm resistor, was selected and used throughout the design process. This lead to a false conclusion on several tests that the avionics circuitry (which produced a clean 4 amp, 47 ms pulse with the emulator) would always supply 4 amps to an NSI.

These false test findings likely also supported and/or lead to the test philosophy that only a limited number of NSI firings (two) had to be conducted to certify the design (see Recommendations 9 and 10).

If an accurate NSI emulator cannot be developed then an emulator process should be developed such as the use of a series of different resistors, used one at a time, over a series of tests.

Recommendation #8: *All NSI firings conducted as part of development tests, certification or acceptance tests should be conducted with an inductive probe in place to record the NSI current.*

When an NSI firing was attempted during the development and certification processes, the NSI current was not measured. A current trace during these tests would have shown the NSI current dropping from 4 amps to the mid to high 2 amp range (as the trace taken during the investigation shows in Figure 14). Such traces would have alerted the team to the resistance changes and driven a design change.

Recording NSI firings in the future will provide valuable certification and acceptance data.

Recommendation #9: *Modify the SAFER certification testing process to include a statistically significant number of NSI firings in order to certify the redesigned SAFER.*

Only two NSI firings were conducted in the original certification process. This limited number coupled with the probabilities involved with the reduced NSI firing current allowed the design to be certified with the design that failed.

A statistical analysis should be used to determine the optimum number of NSI firings. These NSI firings may take place in an explosion-proof container (a "bomb") so that there is negligible wear on the SAFER unit (no pyro valve replacement required after each NSI firing) while still proving the NSI will be reliably fired.

Recommendation #10: *Modify the SAFER flight unit acceptance testing process to include NSI firing(s) on each SAFER flight unit.*

NSI firings were never conducted on any flight SAFER units. Since SAFER is a piece of emergency equipment, a test of its operation before deploying the unit for flight is a highly desirable goal. In addition, the "cost" of such a test is low. With a low cost and a high return, the firing of NSI's in each flight unit should be part of the acceptance plans.

Recommendation #11: *The redesigned avionics should not be modified to allow for checkout of the entire NSI firing circuit during the SAFER self test.*

The current self test performs a simple continuity check of the NSI circuit to verify that the NSI is present and unused. The circuit which generates the firing pulse is not checked for operation and continuity. However, the dynamic parts off this circuit are redundant.

Recommendation #12: *The battery fabrication and acceptance processes should be modified to include*:

(1) *A more thorough cell screening effort, via destructive sampling/testing, to include cell load tests at -4F.*
(2) *A load test of each 4- and 10-cell bundle before they are assembled into a string.*
(3) *A load test of each flight battery (a string check is listed in Recommendation #13)*

The FRB found that the battery had worked well on STS-86 and in the post flight trouble shooting. However, risks at the cell, bundle and string levels can be reduced via some fabrication process changes and a minor battery design change.

A battery is made of three 14-cell strings. Each string is made up a two bundles, a 4-cell bundle and a 10-cell bundle.

In the current fabrication process, cells are screened with a simple voltage check (10 seconds). By adding much more thorough destructive lot sampling involving capacity discharge and pulse discharge tests, the probability of using only acceptable cells in the fabrication of a SAFER battery is increased.

Bundles are currently not load tested. Adding load tests at the bundle level will increase the probability of using operational bundles in the fabrication of the SAFER battery.

Battery voltage during acceptance is currently measured under minimal load. In order to increase the probability of accepting nominal, capable batteries, a three-part load test (1 amp, 2 amp,, and maximum load) should be added to the acceptance testing.

Recommendation #13: *Modify the battery fabrication ground support equipment (GSE) and the battery to allow a check of each of the three battery strings independently after battery brick assembly.*

All three of the battery's strings must be functional for the NSI to fire reliably yet there is currently no insight into the status of each string. The three strings are connected in parallel and the only data point is the (common) voltage across the ganged, parallel strings. Therefore, the failure of one or two strings cannot be detected in the current design.

Changes to the GSE and the battery will allow a check of the voltage of each of the three strings. There will be much more insight into the health of the battery.

Recommendation #14: *Modify the battery to allow a check of each of the three battery strings independently in flight before SAFER is donned for an EVA.*

All three of the battery's strings must be functional for the NSI to fire reliably yet there is currently no insight into the status of each string. The three strings are connected in parallel and the only data point is the (common) voltage across the ganged, parallel strings. Therefore, the failure of one or two strings during pre-launch handling, launch or extended on-orbit time cannot be detected in the current design.

Changes to the battery will allow a check of the voltage of each of the three strings which would guarantee the battery is acceptable for use.

Recommendation #15: *Modify the SAFER out-of-limits (software) criteria for the battery voltage from 28 volts to 35 volts.*

Changing the criteria for the battery voltage will result in the capturing of two potential failures; one dead cell on each string or two failed 10-cell bundles. With these failures, the ability of the battery (especially at cold temperatures) to reliably fire the NSI is reduced.

Recommendation #16: *The JSC pyrotechnics group, EP5, should conduct a series of "constant voltage" tests on the NSI.*

There is currently very limited data on the use of an NSI in a constant voltage circuit. The data will allow future NSI users to confidently consider a constant voltage NSI firing circuit (see Recommendation #17 also).

Recommendation #17: *The JSC pyrotechnics group, EP5, should produce a "users guide" for the NSI.*

No "users guide" currently exists for NSI users. A users guide will be a valuable asset to NSI users and it will increase the probability of success of future systems using the NSI.

Corporate knowledge will also be documented and reliably passed to future generations.

Recommendation #18: *Do not incorporate any design changes addressing voltage delay.*

There is no voltage delay phenomenon in the SAFER battery cells.

Recommendation #19: *Do not incorporate any design changes which would allow a signal to be sent to the crew member if the NSI did not fire or gas was not being delivered to the thrusters.*

Addition of an alert for these failures (there is currently no sensors for nitrogen pressure or flow downstream of the manual isolation valve) is not considered useful or cost effective. Crew members only have one option if the NSI does not fire and/or if the thrusters are not receiving propellant: power cycle. Crew members have and will be trained extensively on this scenario as all SAFER crew members previously have been trained. EV1 on STS86 did not know the failure had occurred because he was in a foot restraint.

Implementation would also have been expensive for a relatively small return.

Recommendation #20: *Change the hand controller message for the absence of a good NSI bridge wire from "NSI Failure" to the more descriptive "NSI CIRCUIT OPEN."*

The current message for this condition, "NSI FAILURE," does not accurately and completely describe the condition of the NSI.

This is a software change and is therefore relatively inexpensive.

Recommendation #21: *A flight test of the redesigned SAFER unit should be conducted as soon as possible.*

A **flight test** for the redesigned SAFER should be manifested at the first opportunity. SAFER is an emergency piece of equipment that will be used for many, many years during hundreds of hours of EVA's. A simple flight test would be relatively inexpensive and low risk yet the return would be high: complete verification of the design. This low cost, high return flight test will compliment the extensive ground testing for the redesigned SAFER.

Discussions have commenced on this topic with the EVA Project Office (XA), the Automation, Robotics and Simulation Division (ER), the Mission Operations Directorate (DF and DA), and the Flight Crew Operations Directorate (CB).

FIGURES

Title	Page

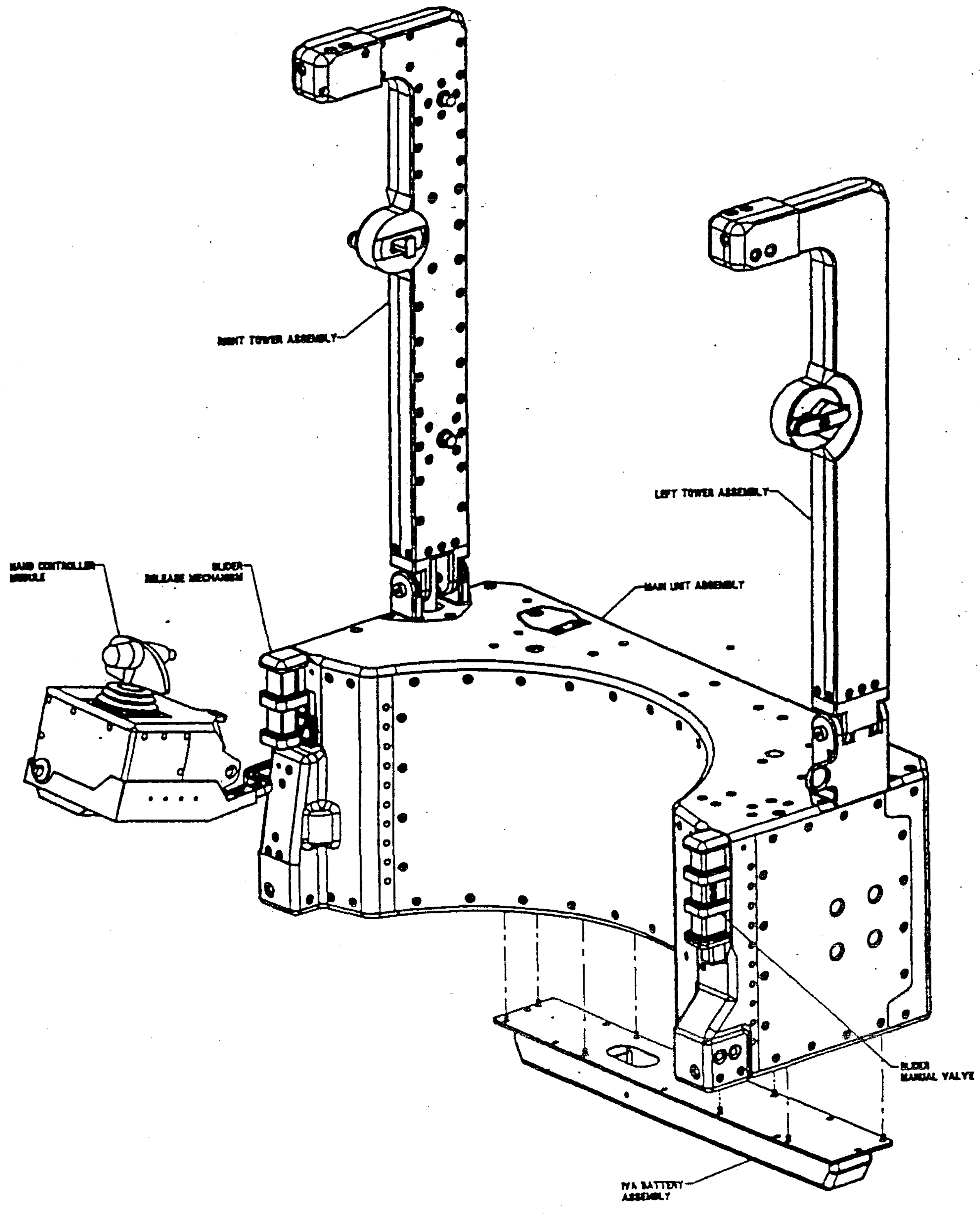


Figure 1: USA SAFER overview (page 1 of 2)

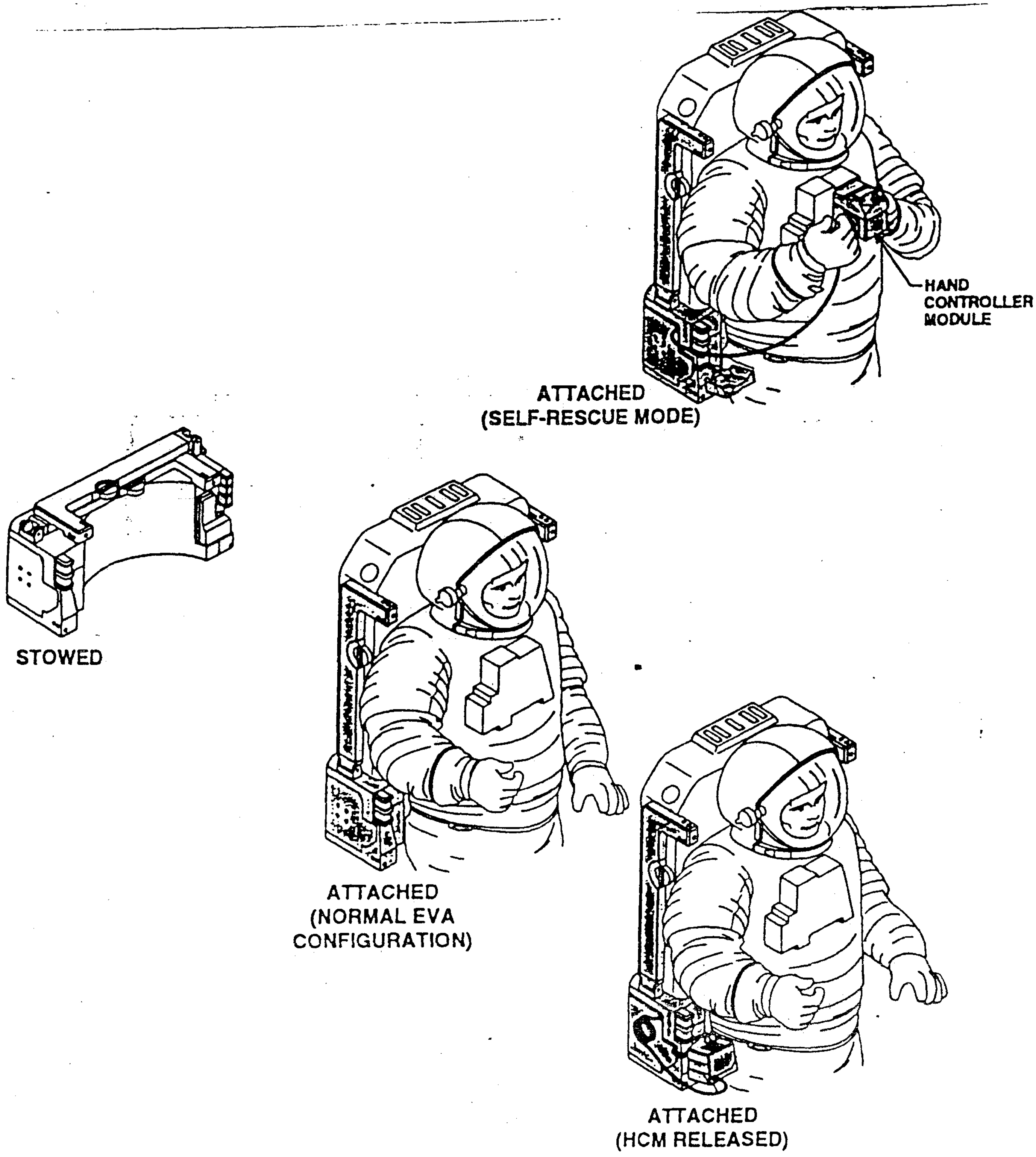


Figure 1: USA SAFER overview (page 2 of 2)

Ron Cook, S&MA

11/21/97

SAFER Flight Configuration Block Diagram (NSI, HCM, Avionics, Battery)

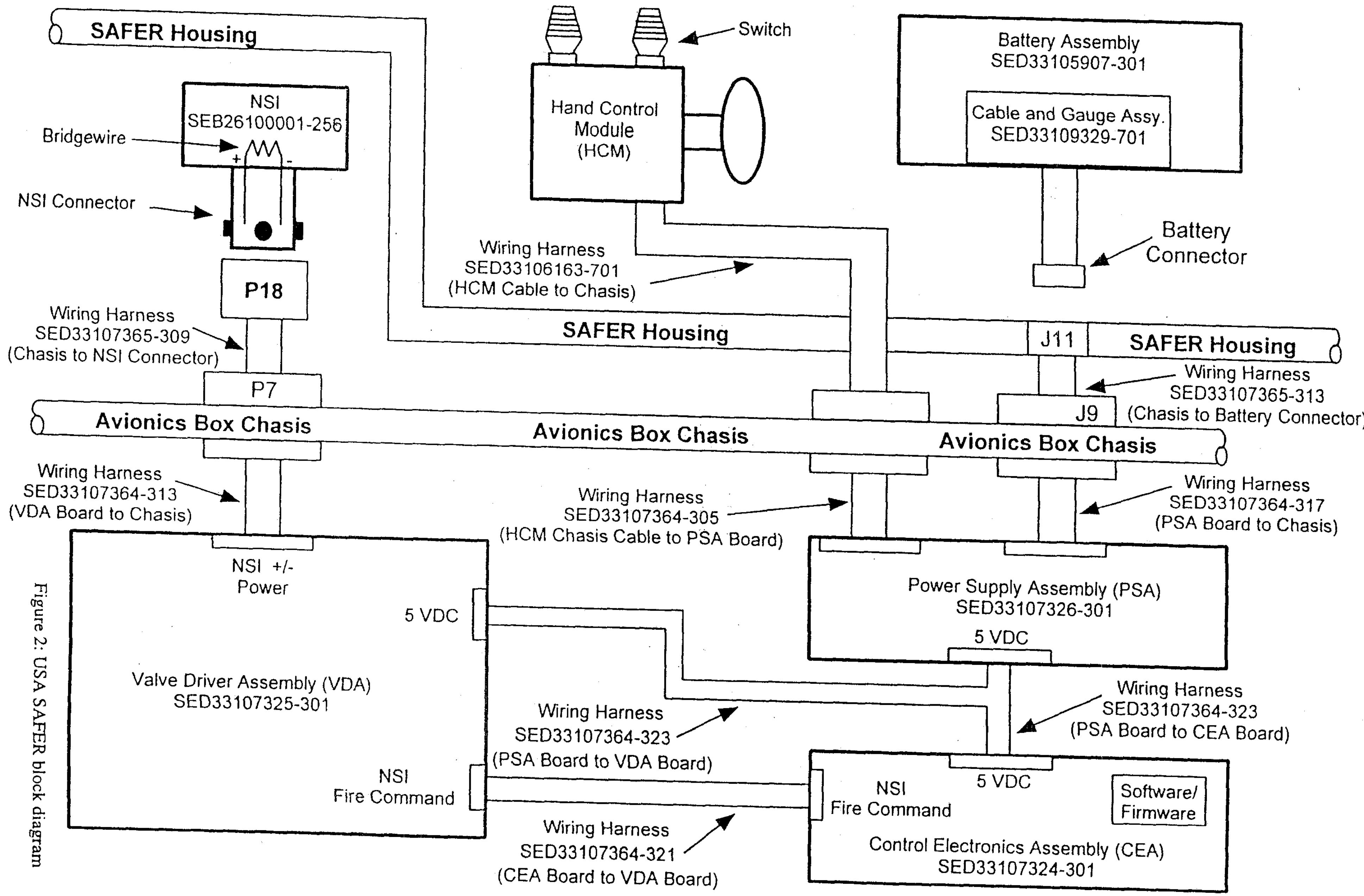
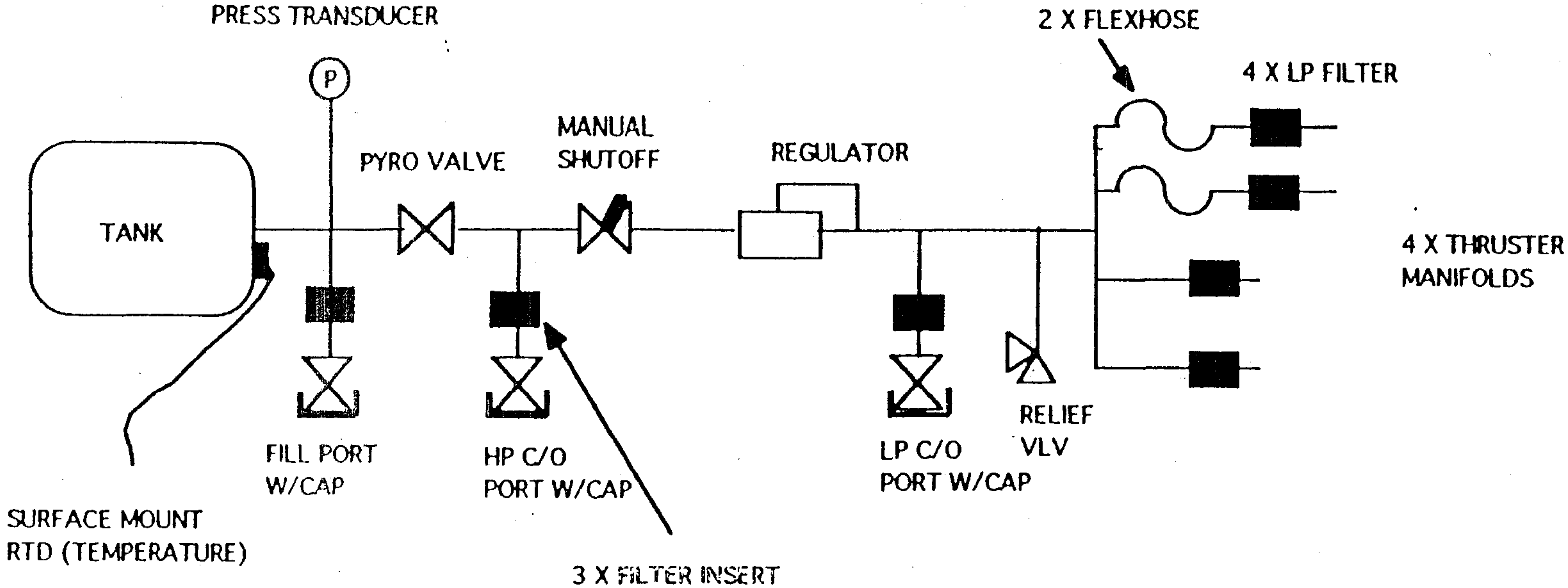


Figure 2: USA SAFER block diagram

SAFER SCHEMATIC



PART	VENDOR	PART NUMBER
TANK	ARDE	D4616
RTD	RDF CORP	24123
HP XDCR	EATON	41SG624-1
FILTER INSERT	BRUNSWICK	11267-509
PYRO VALVE	PAC SCI	2-502030-1
MAN VALVE	BUTECH	B-2570-01
REGULATOR	TESCOM	269-530-PL3VE
RELIEF VALVE	CIRCLE SEAL	5159T1-6T-L-300
FLEXHOSE	AIRPRO	1/4 X 15" AND 25"
LP FILTER	BRUNSWICK	12267-556
THRUSTER	MOOG	B84138-1

Figure 3: USA SAFER propulsion system

1. REF. DOCUMENT NO. TS9720292	DISCREPANCY REPORT/MATERIAL REVIEW RECORD NASA-LYNDON B. JOHNSON SPACE CENTER		PAGE ____ OF ____
			RECORD NUMBER
2. Name Top Assy: SAFER	3. Drawing/Part No.: SED33105900-301	4. Serial/Lot Number: [illegible] 1005	5. IDR: N/A
6. Name Sub Assy	7. Drawing/Part No.	8. Serial/Lot Number	9. DR/MRR: TS9730085
10. Name Component	11. Drawing/Part No.	12. Serial/Lot Number	13. STUPAK

DISCREPANCY

NSI should have been fired during flight.
Self test does not ~~[illegible]~~ indicate NSI Fired.
Should read "NSI Failure" actually read "Go for EVA."

T1. Resp. Org.	T2. Hw. Type	T3. Prev. Cond.	T4. Fail. Mode	T5. Defect	T6. Disposition	T7. Cause	T8. Recur. Cntrl	T9.	T10.
ER	FH							ER	

14. Initiator's Signature	15. Stamp Number	16. Organization and Location of Initiator	17. Date
[signature]	30	ND365	11/4/97

DISPOSITION

18. MR Action Required	19. MRB Decision		20. Removed P/N	21. Replacement P/N
☐ Yes ☐ No	☐ USE "AS IS" ☐ REPAIR	☐ CLASS CHG ☐ WAIVER ☐ SCRAP	20A. Removed S/N	21A. Replacement S/N

22. FIAR Number	INSTRUCTIONS	TECH	QC STAMP CONT.	NA
	INT #1			
	1. verify no prop used, record results: no prop used: 7681 @ 70°F ⇒ no prop used.	B.S.	11/4/97	S
	2. verify no prop downstream of manual vlv by cycling open/closed, repeat turn-on w/ inhibit plug installed, record results: NO GAS VENTED	B.S.	11/4/97	SAIC 30
	3. Depressurize unit and remove battery per TPS TS9720292 for return to JSC for troubleshooting.	B.S.	11/4/97	SAIC 30
[signature] 11/4/97	23. DATE	FINAL ACCEPTANCE		

[signature] 11-4-97

MRB APPROVAL SIGNATURES

24. Stress Engineer (NASA)	DATE	25. Materials Engineer (NASA)	DATE
26. System Engineer (Contractor)	DATE	29. System Engineer (NASA)	DATE
27. Quality Control Rep (Contractor)		SA)	DATE
28. Program Office Rep (NASA)			DATE

Figure 4: STS-86 USA SAFER Discrepancy Report

SHUTTLE PREFERRED PYROTECHNIC ITEMS LIST

1. SPPIL NO: G-1
DATE: NOVEMBER 1975

2. NOMENCLATURE: NASA STANDARD INITIATOR, Type 1 (NSI-1)
SCD/PERFORMANCE SPEC: NASA SLB 26100052/SKB 26100066

3.

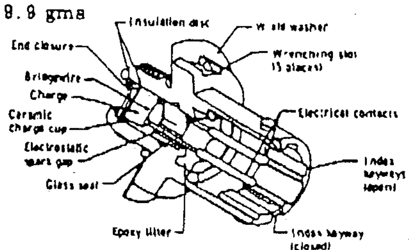
PART NUMBER	AGENCY
SEB26100001-XXX	NASA/JSC
S01-10197-XXX	Space Ordnance Systems
PC 23(939641)	Hi-Shear Corp.

4. APPROVED SUPPLIERS
Space Ordnance Systems, TransTechnology Corp.
Hi-Shear Corp.

5. PHYSICAL DATA

WEIGHT: 0.022 lb
9.9 gms

BODY MAT'L: Inconel 718



Thread: 3/8 x 24 UNF-3A
JSC Part Number: SEB 26100001-xxx
Nominal Dimensions
Length: 0.873 in.
Washer Dia: 0.800 in. (OD)
Torque Sect Dia: 0.706 in. Dia

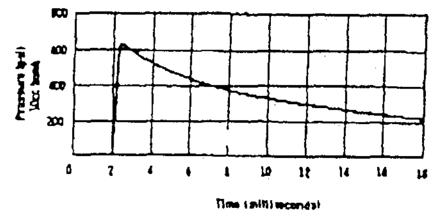
FOR CONTROLLED INSTALLATION:
USE SPANNER WRENCH,
SOS P/N T11 ... PWR:
OR EQUIVALENT:

CIRCUIT DIAGRAM
.96 to 1.15Ω

6. PERFORMANCE DATA

INPUT: Recommended firing current: 5 amps
OUTPUT: All-fire: 3.5 amps
Pressure: 650 ± 125 psi (10 cc)
Calories: 150 minimum

PRESSURE-TIME CHARACTERISTICS
Typical Lot Acceptance
(3.5 Amp firing current)



T_0 = Application of fire signal

7. PYROTECHNIC DATA

SOS: 114 milligrams of SO108 (Nom)
H/S: 114 milligrams of 939321-003 (Nom)

8. ENVIRONMENTAL CAPABILITIES

OP Temp Range	-260°F to +300°F
Temp-Humidity	+165°F, 95% RH, 10 days
Temp-Altitude	-260°F, +300°F, 10^{-6} mmHg
Storage Temp	0 to 105°F
Temp Cycle	-260°F, 300°F 20 cycles
Leakage (seal)	1×10^{-6} scc/sec He at 1 atm

Drop (6-ft)	MIL-STD-331, Test 103
Shock	100 g, 11 msec rise time
Vibration	Random -260°F & 300°F
Stor/SVC Life	7 years
Electro-static	25 KV from 500 pfd capacitor (PINS to CASE)
No-Fire	1A and 1W thru bridgewire for 5 min. (-260°F and +165°F)

Note: Also qualified to environments of higher assemblies in which the NSI is an integral component (e.g., Detonator ME453-0021-0007)

QUALIFICATION REPORT: SOS TR 6068; H/S TR2-323

9. APPLICATION: Standard EED in Apollo, Skylab, Apollo-Soyuz and Space Shuttle programs.

SAFETY/DOT CLASS: Class "C" When fired by a 1000 microfarad capacitor charged to 20 volts the pressure-time curve shifts to start at 0.3 ms; the curve shape remains the same.

REMARKS: Current life - 10 years

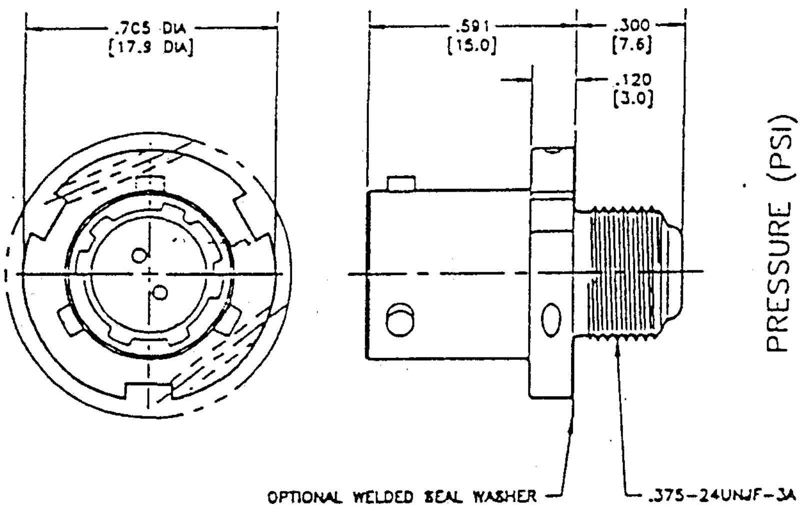
Figure 5: NASA Standard Initiator (NSI) overview

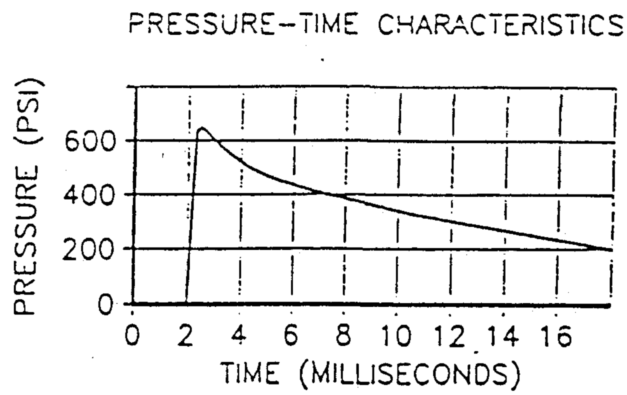
PACIFIC SCIENTIFIC

ENERGY DYNAMICS DIVISION

PRODUCT DATA SHEET

STANDARD SPACE INITIATOR
PART NO. 2-101600-1 and 2-101600-2





DESCRIPTION

The PS/EDD Standard Space Initiator has been developed and is currently under contract for qualification with National Aeronautics and Space Administration (NASA). This initiator is designed to meet the requirements of NASA Standard Initiator (NSI) which has a proven reliability through test and flight history. Lot acceptance testing is the same as for the NSI except the testing at -420°F is not performed.

MATERIAL DATA

Body: Inconel 718 Per AMS5662

SEALING PROPERTIES

Leak Rate:	$< 1x10^{-6}$ cc/sec Helium
Pressure:	Withstands 40,000 psi

EXPLOSIVE MATERIALS

Ignition/Output: 114 mg

OPERATING TEMPERATURE

-260°F to 300°F

ELECTRICAL PROPERTIES/INTERFACE

Connector:	MIL-C-26482, Series 1, No. 8, 2 Pin
Bridgewire Resistance:	1.05 ± .10 Ohm
Insulation Resistance:	2 Megohms min. @ 250 VDC for 15 seconds
Dielectric Strength:	500 Microamps max. @ 200 VRMS for 60 seconds

FIRING CHARACTERISTICS

No-Fire Current:	1.0 amp/1.0 watt for 5 min.
All-Fire Current:	3.5 amps DC minimum 10 ms

OUTPUT PERFORMANCE

Output Pressure:	650 ± 125 PSI in 10cc Closed Bomb

THE DATA PRESENTED ABOVE IS FOR INFORMATION PURPOSES ONLY

Figure 6: NSI Product Data Shee

7073 W. WILLIS DR., BOX 5002 • CHANDLER, AZ 85226-511
(602) 796-1100 • FAX (602) 796-0754

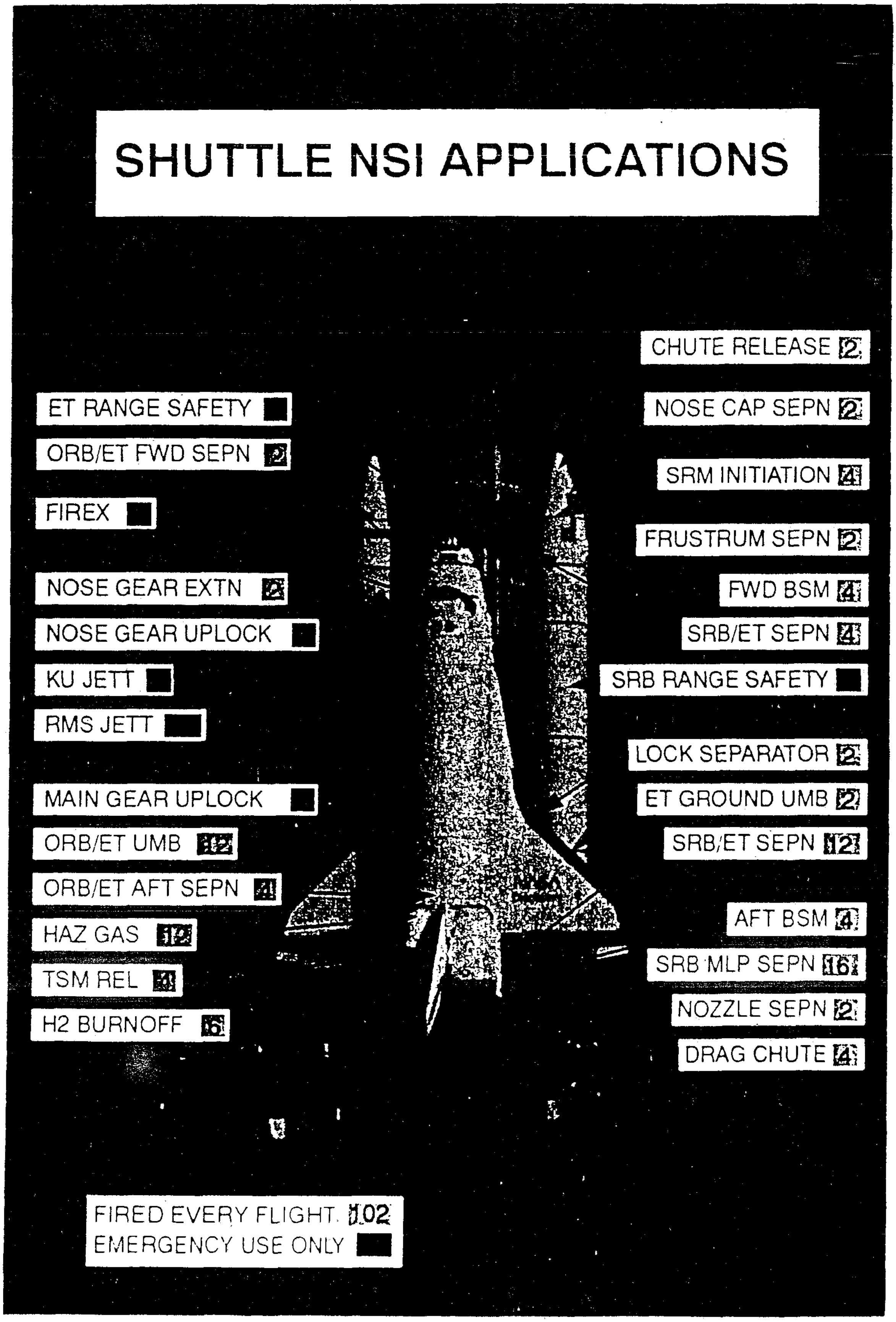


Figure 7: Shuttle NSI Applications

GROUND RULES FOR FAULT TREE ANALYSIS

The following is a list of ground rules and assumptions used during the development of the USA SAFER Failure Investigation Fault Tree.

1) Fault tree was developed assuming specific hardware/component failure or failures.

2) System design was adequate to perform intended function.

3) SAFER hardware met all design requirements.

4) Crew members and technicians operated equipment correctly.

Figure 8: USA SAFER Fault Tree (page 1 of 10)

SAFER Failure Investigation Fault Tree

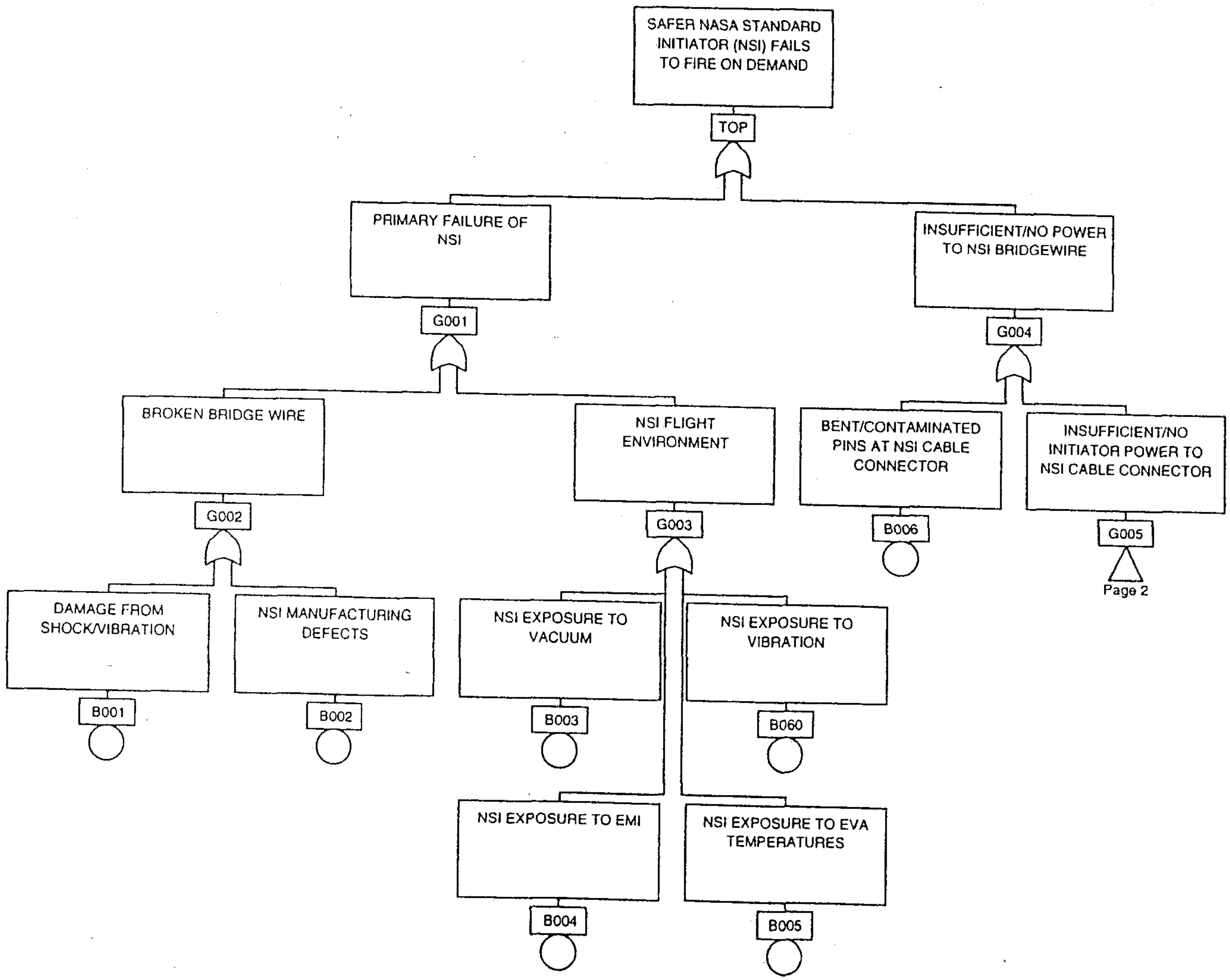
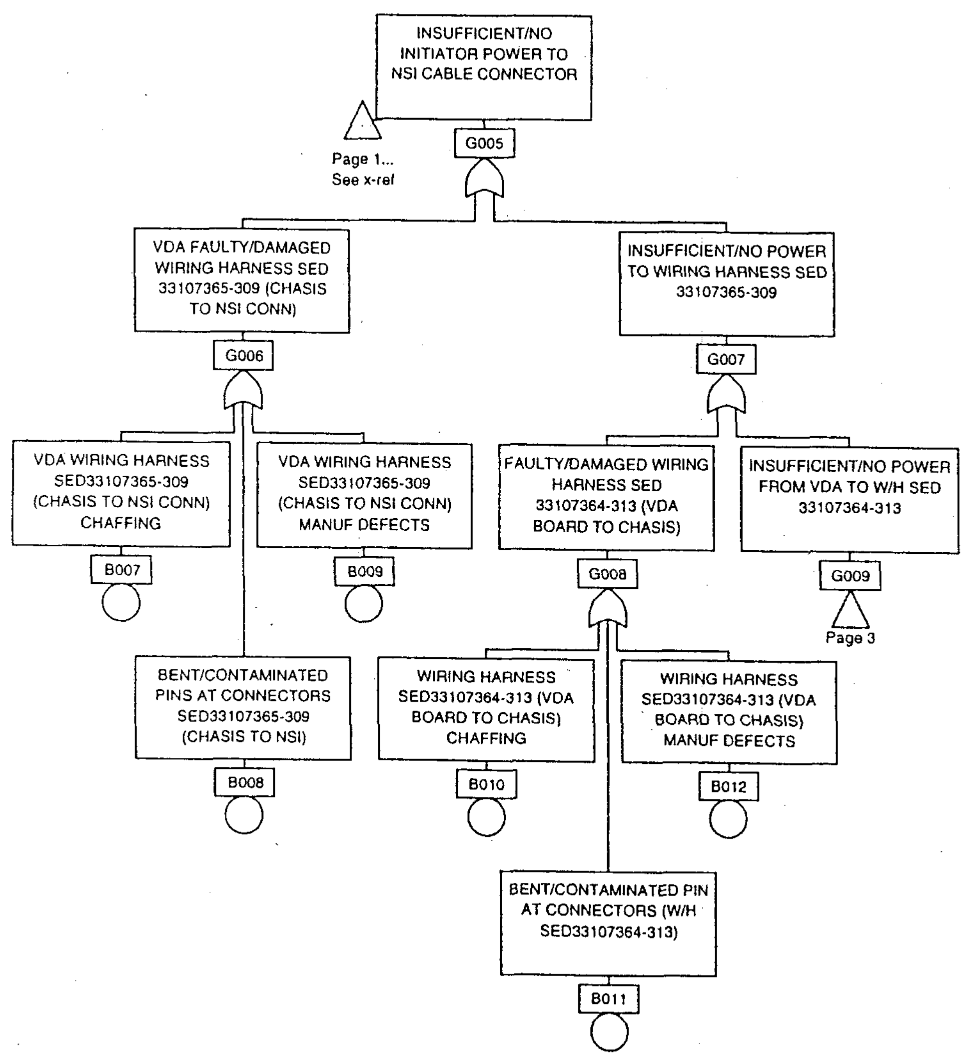


Figure 8: USA SAFER Fault Tree (page 2 of 10)

SAFER Failure Investigation Fault Tree



Safety & Mission Assurance 12/10/97 Page 3 of 10

Figure 8: USA SAFER Fault Tree (page 3 of 10)

SAFER Failure Investigation Fault Tree

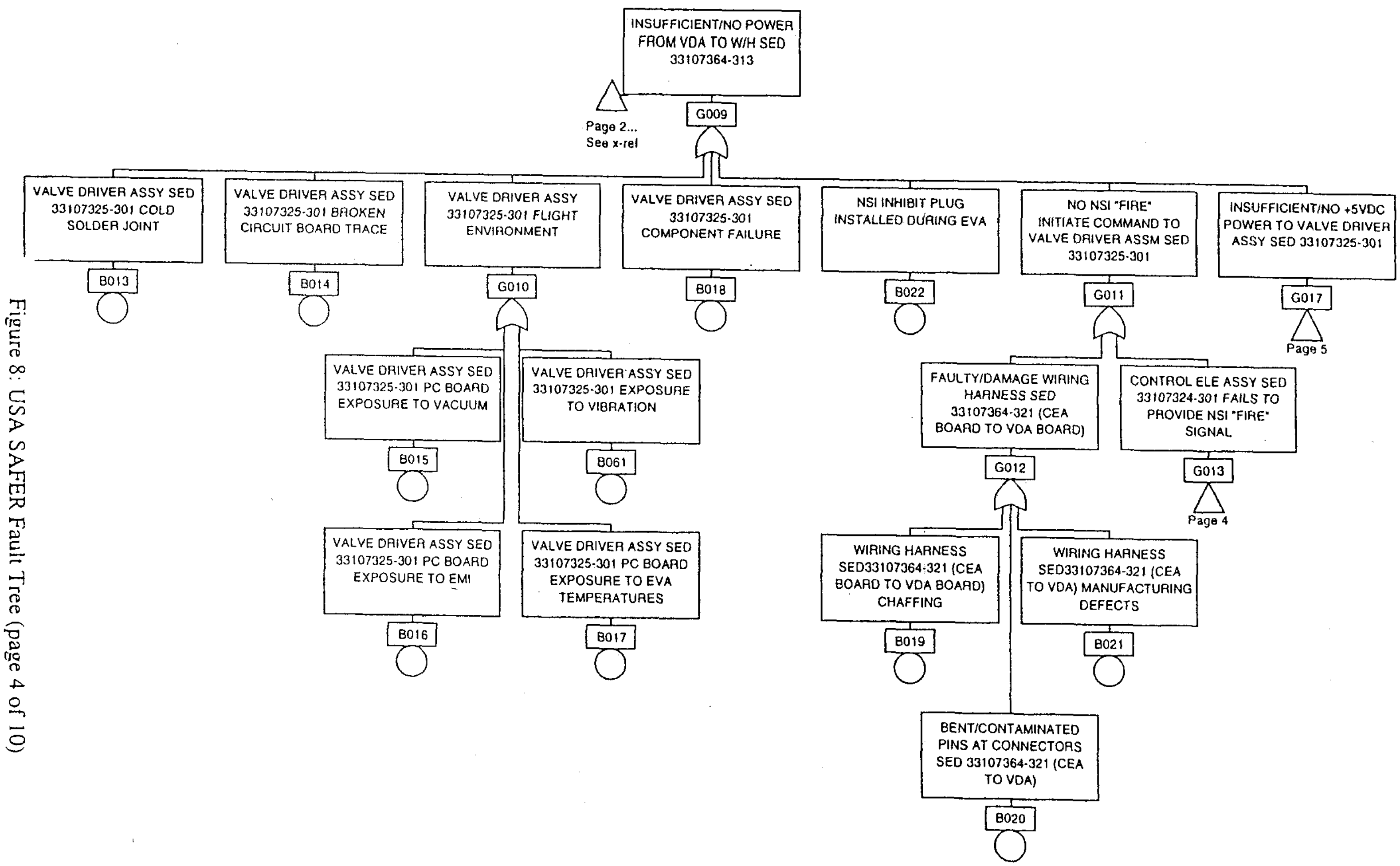


Figure 8: USA SAFER Fault Tree (page 4 of 10)

SAFER Failure Investigation Fault Tree

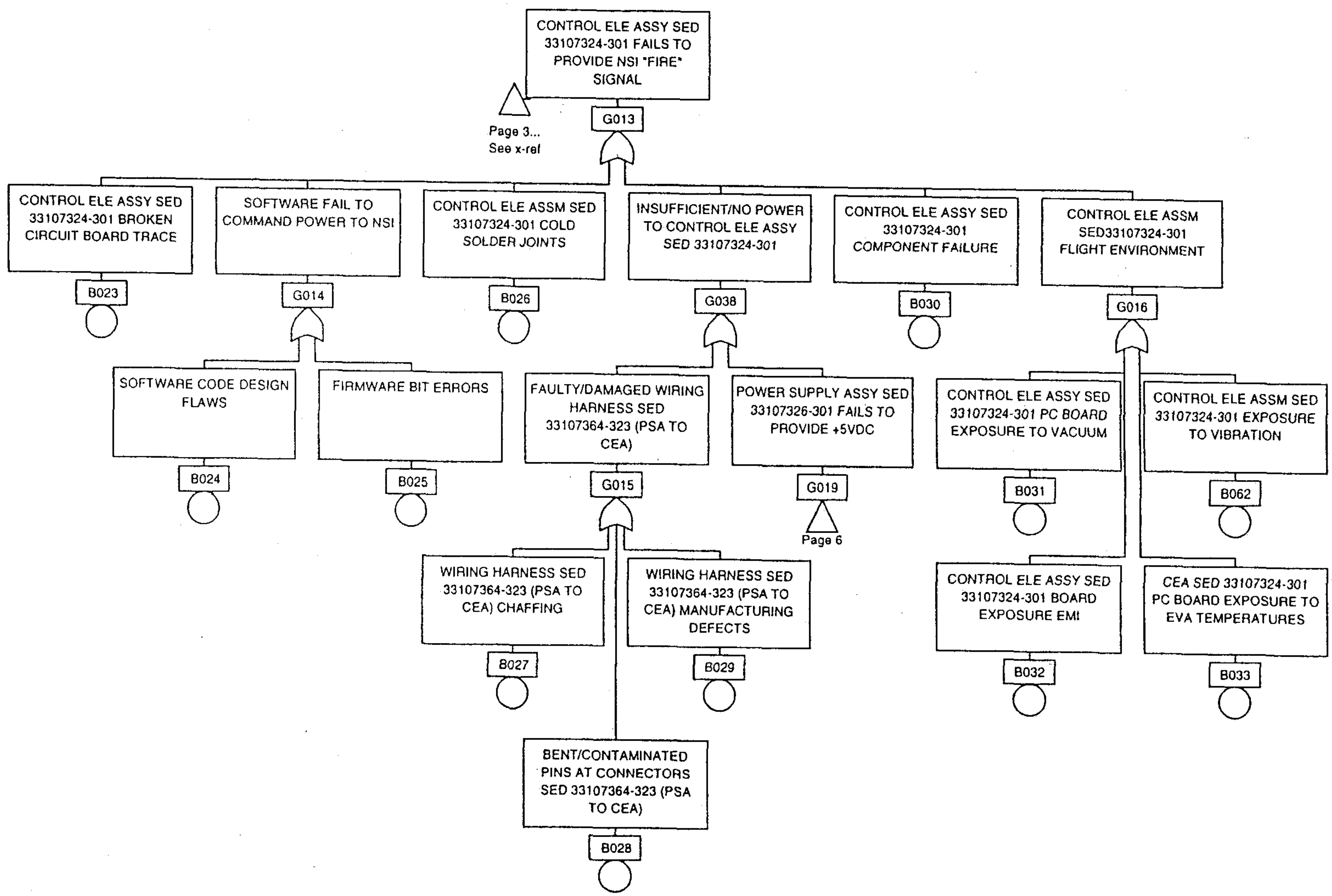
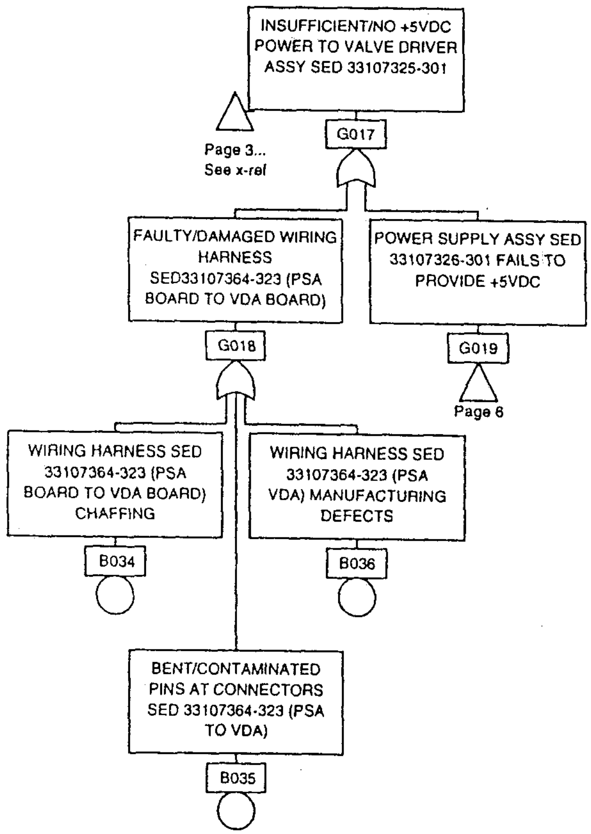


Figure 8: USA SAFER Fault Tree (page 5 of 10)

SAFER Failure Investigation Fault Tree



Safety & Mission Assurance 12/10/97 Page 6 of 10

Figure 8: USA SAFER Fault Tree (page 6 of 10)

SAFER Failure Investigation Fault Tree

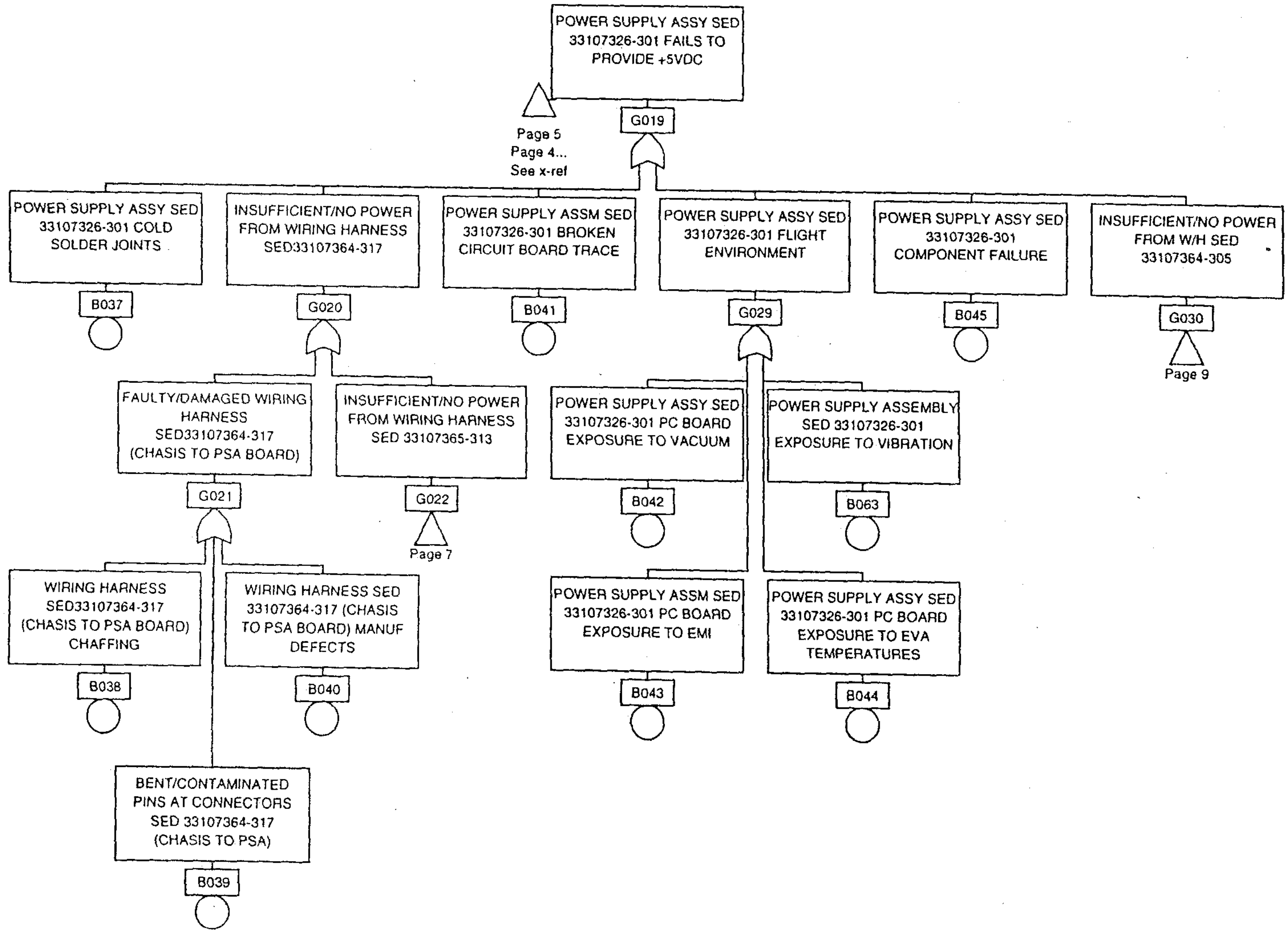
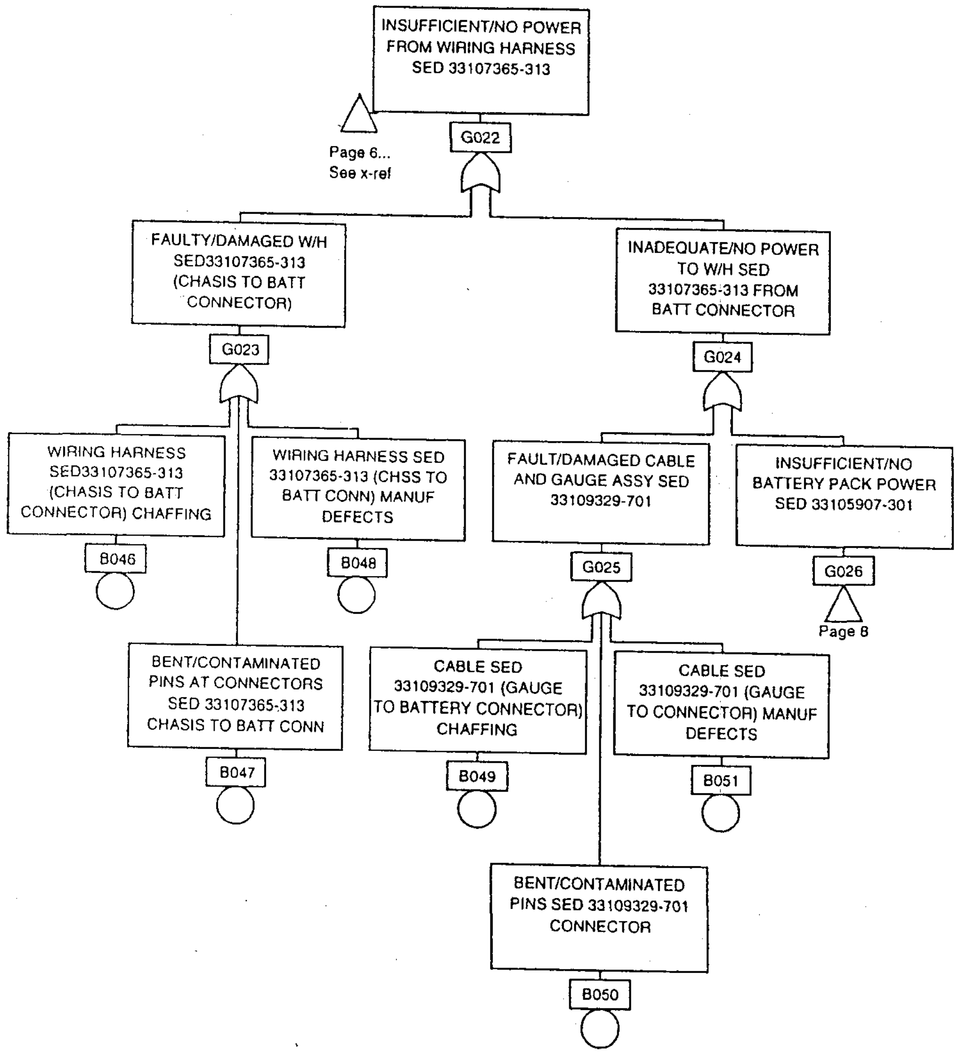


Figure 8: USA SAFER Fault Tree (page 7 of 10)

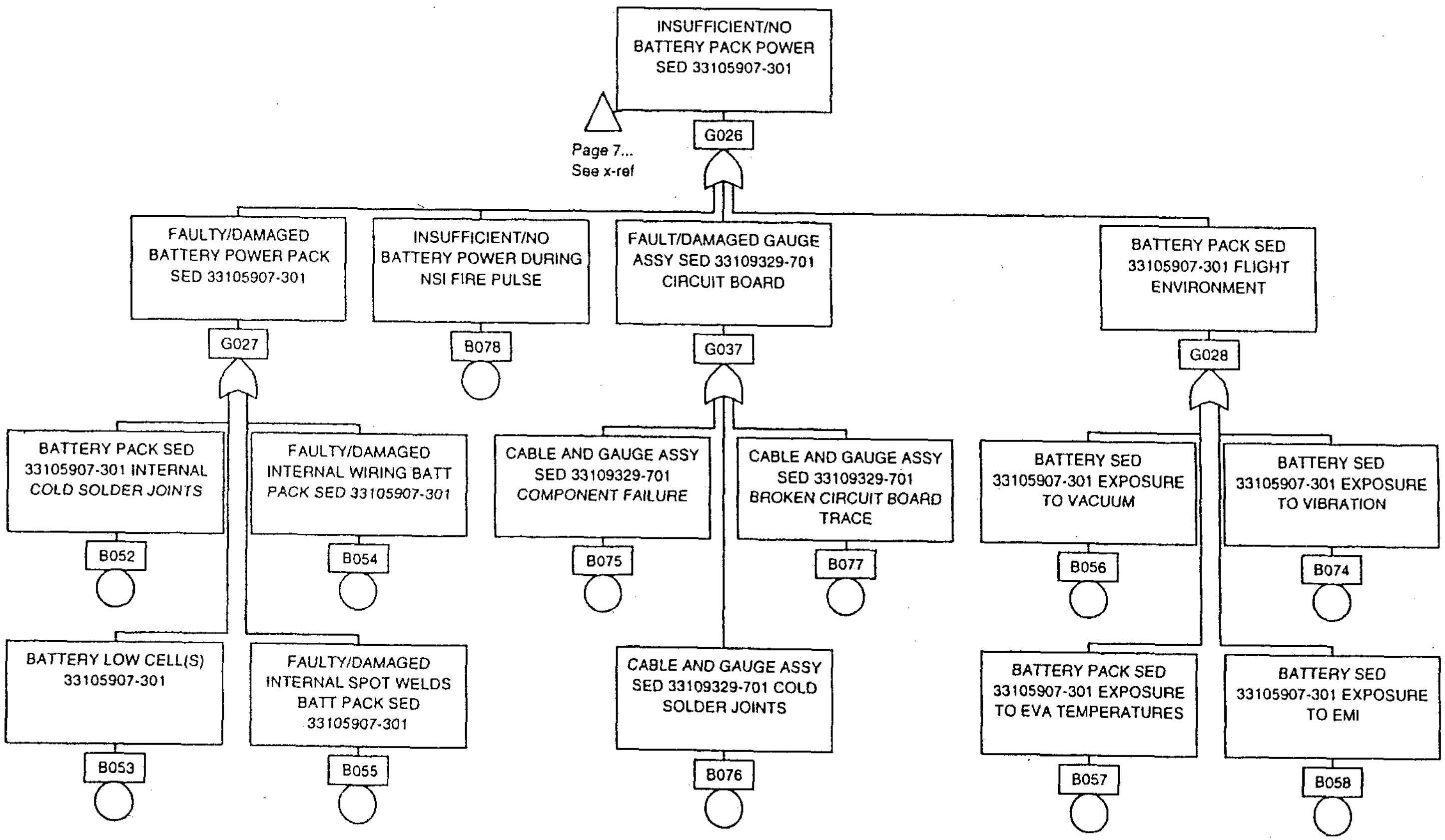
39

Figure 8: USA SAFER Fault Tree (page 8 of 10)

SAFER Failure Investigation Fault Tree



SAFER Failure Investigation Fault Tree



Safety & Mission Assurance 12/10/97 Page 9 of 10

Figure 8: USA SAFER Fault Tree (page 9 of 10)

SAFER Failure Investigation Fault Tree

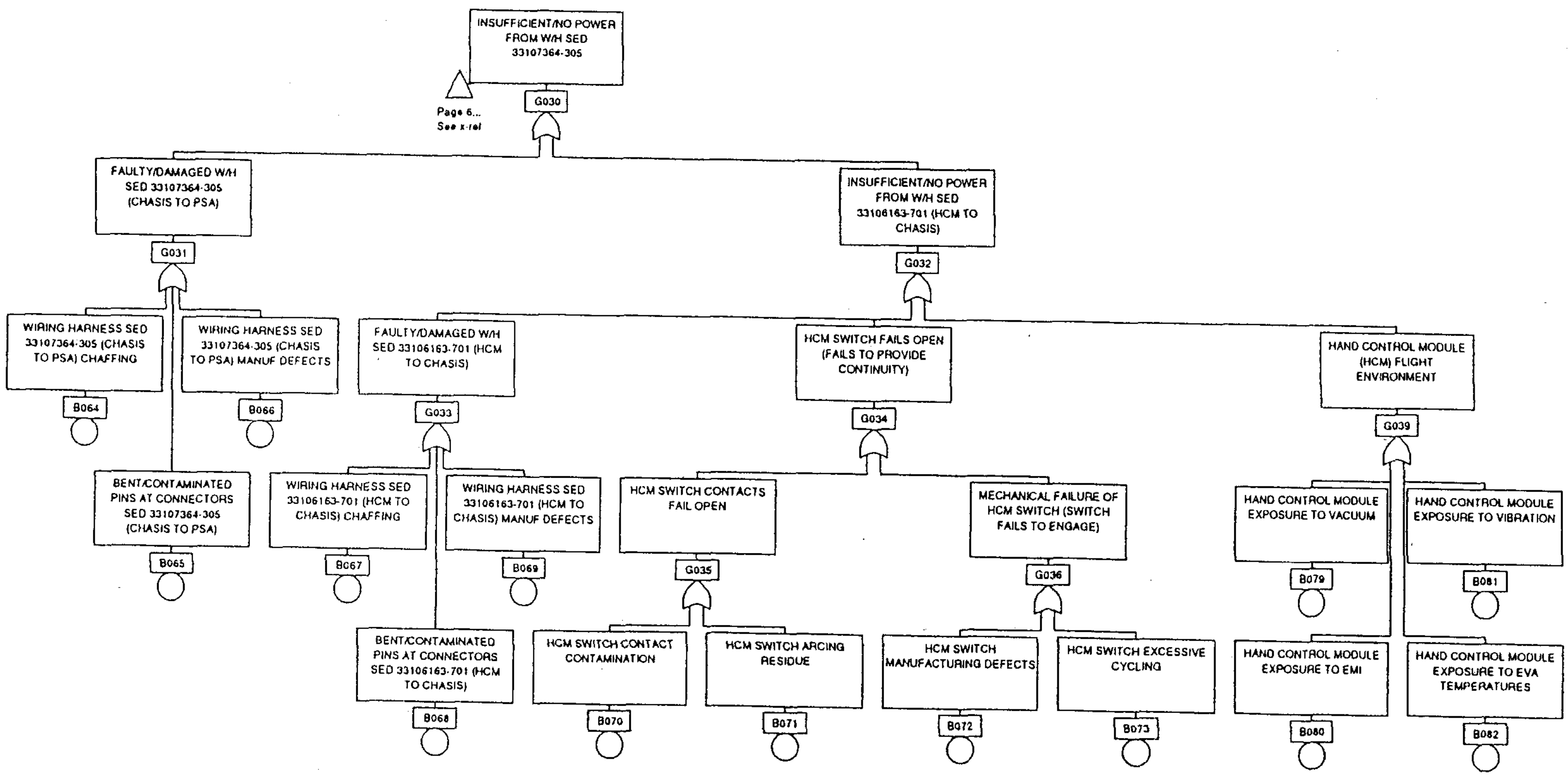


Figure 8: USA SAFER Fault Tree (page 10 of 10)

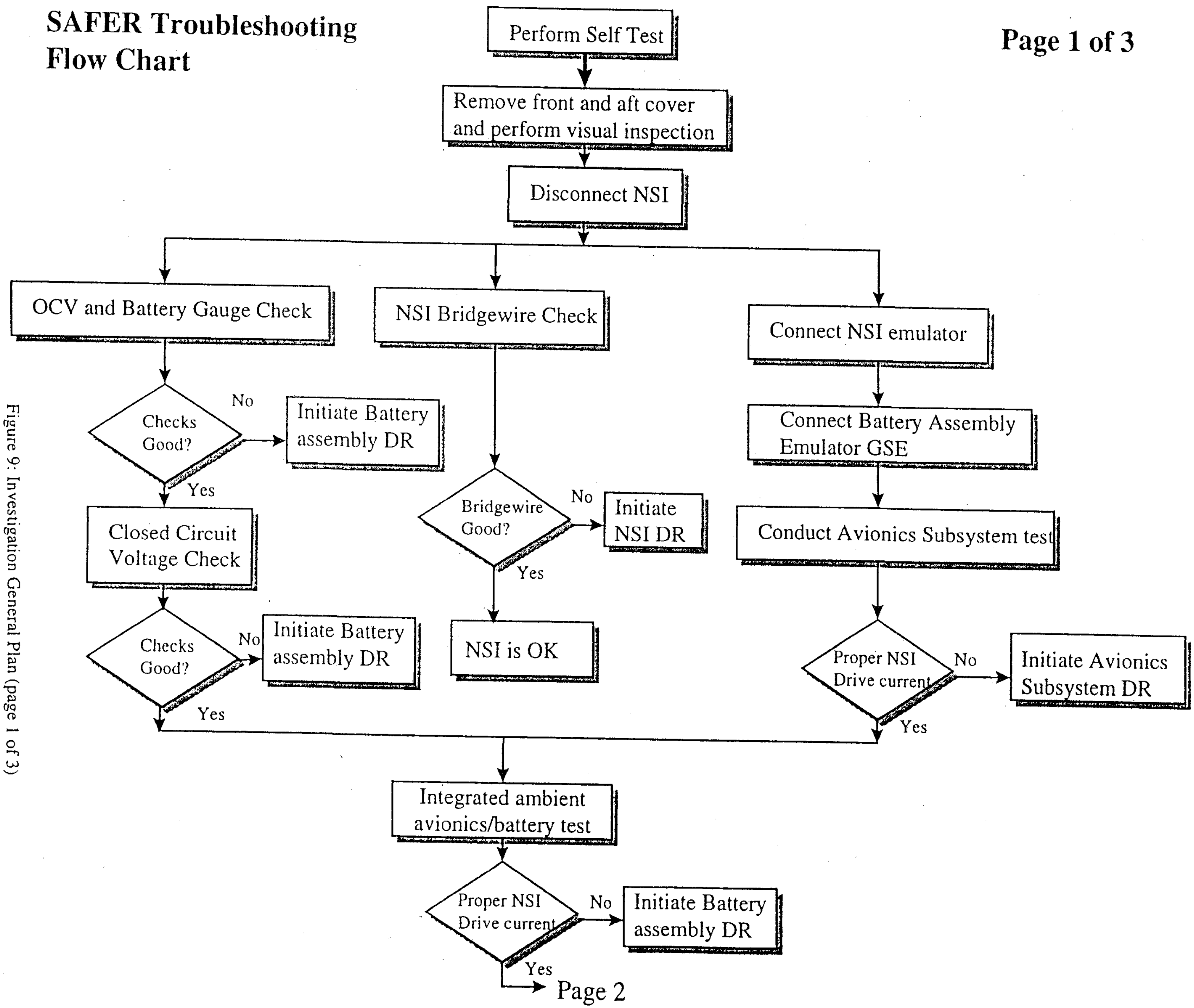


Figure 9: Investigation General Plan (page 1 of 3)

SAFER Troubleshooting Flow Chart

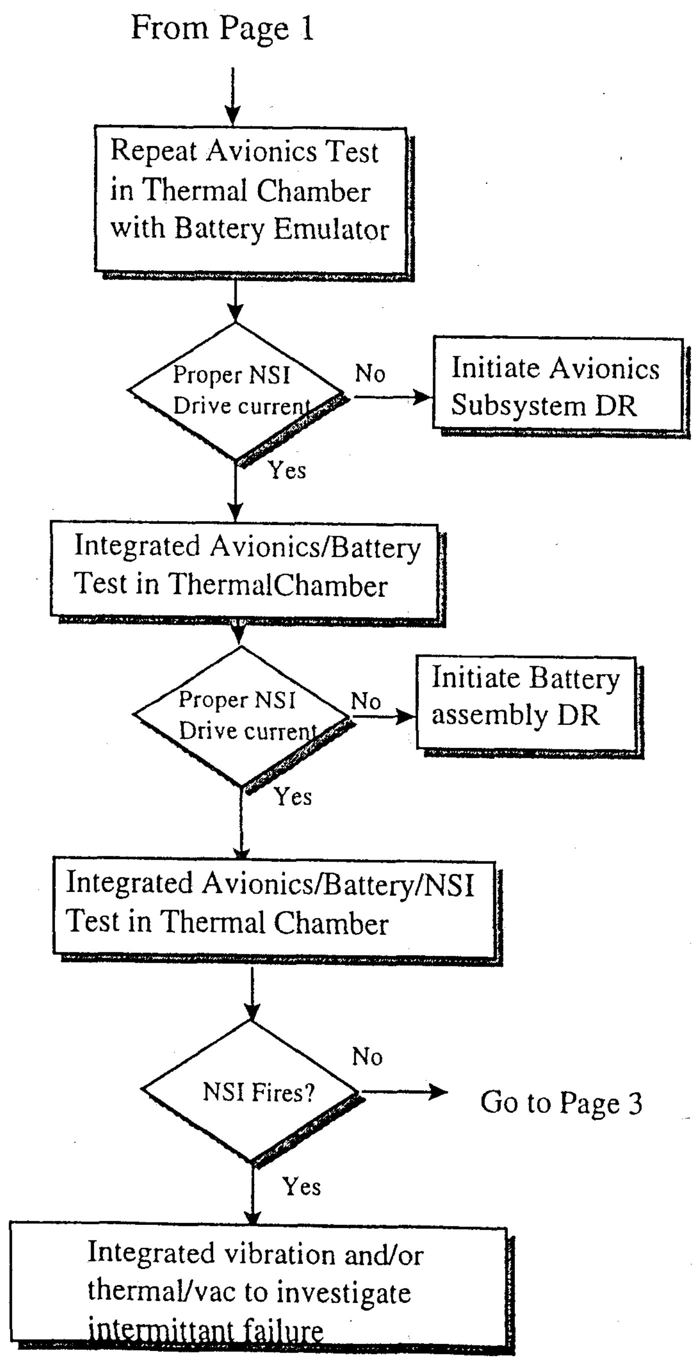


Figure 9: Investigation General Plan (page 2 of 3)

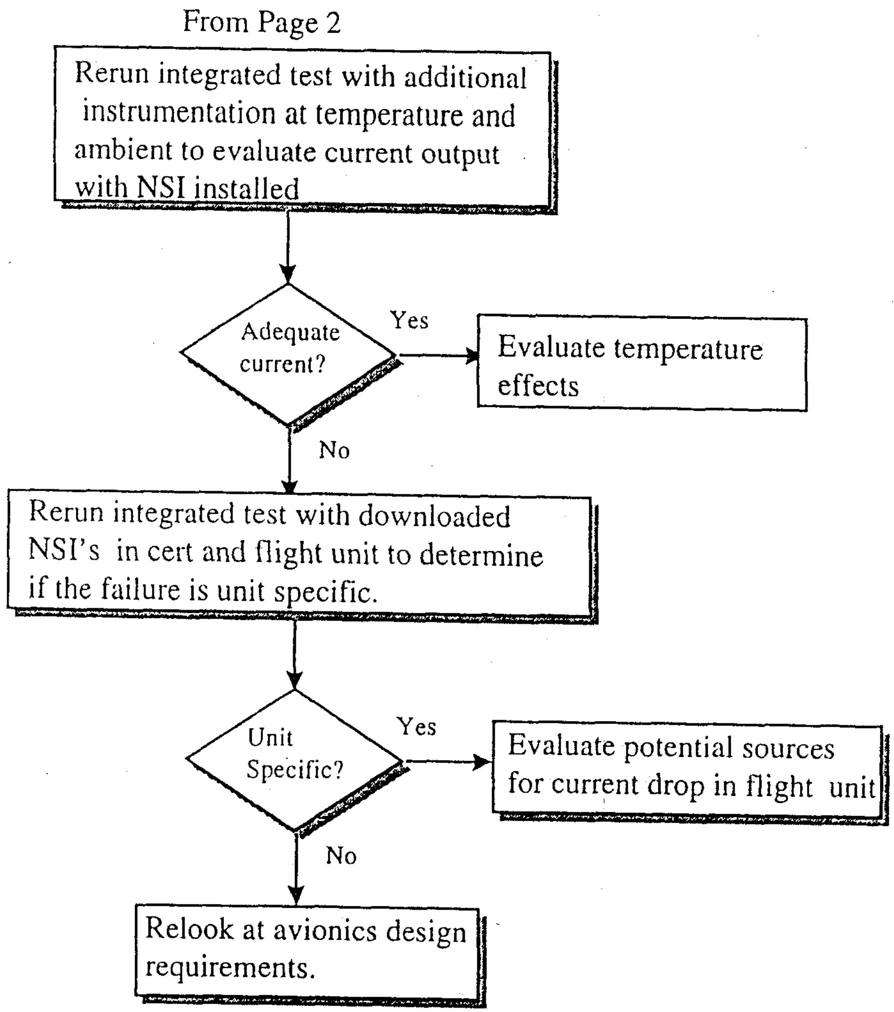


Figure 9: Investigation General Plan (page 3 of 3)

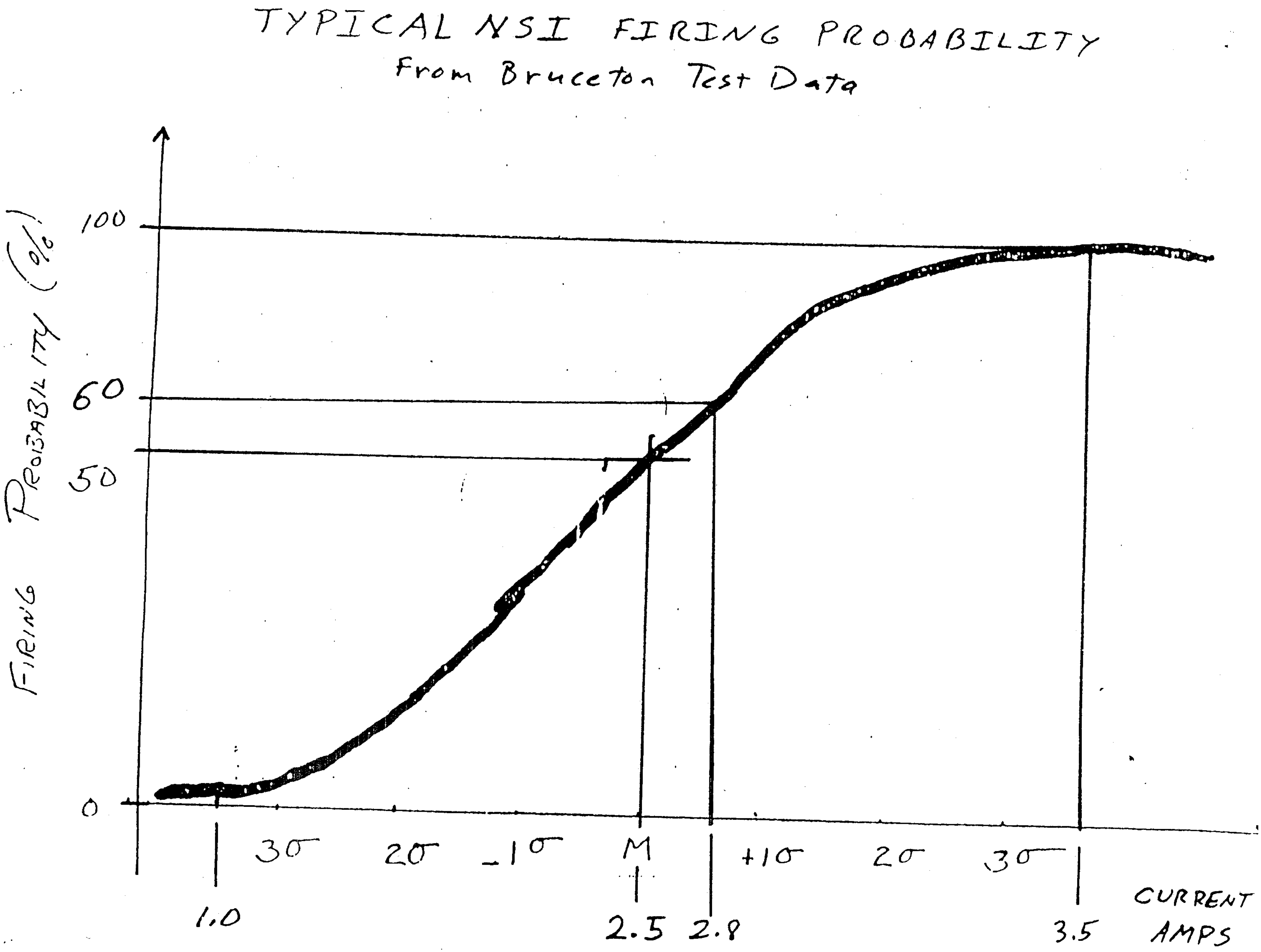


Figure 10: NSI current versus Probability of firing

Lockheed Martin Space Mission Systems & Services
Science. Engineering. Analysis. and Test
2400 NASA Road 1. P.O. Box 58561 Houston. TX 77258-8561
Telephone (281) 333-5411

LOCKHEED MARTIN

February 4, 1998
Contract: NAS9-19100
Subtask Order: HELEC2Y1
HDID-A44B-837

TO:	M. K. Ewert	/ JSC /	EC2
VIA:	A. H. Milliken	/ LM /	C70
	B. C. Conger	/ LM /	C70
FROM:	J. M. Lepore	/ LM /	C70

SUBJECT: **U. S. SAFER STS-86 Postflight Thermal Analysis**

Postflight analysis of the U.S. SAFER for STS-86 was completed using EVA task timelines, downlink video, console logs, and as-flown attitudes. Analysis results indicate that all U. S. SAFER components were well within operational limits during the entire EVA. Component temperature predictions are summarized in Table 1.

The as-flown EVA attitude is designated IO 5.1+141 / +142 (Sun R233 P155) at a sun beta angle of 48 degrees and an altitude of 213 nautical miles. Thermal radiation environments were obtained at 14 possible EVA locations using flux cubes, as shown in Figures 1 and 2. EMU six-direction average sink temperatures for each location are summarized in Table 2.

EVA task timelines, downlink video, and console logs were used to determine EV1's (U. S. SAFER s/n 1005) approximate location during the entire EVA. The location timeline was reviewed by Scott Parazynski (EV1), and his comments were incorporated. EV1 locations were mapped to appropriate flux cube locations to determine a U. S. SAFER environment timeline. Corresponding EMU sink temperatures, including flux cube location numbers, are shown in Figure 3.

It was assumed that the temperature of all SAFER components was 51°F when EV1 egressed. This assumption was based on tunnel adapter temperatures (Figure 4) near the external airlock just prior to egress. The SAFER was powered on 4.1 hours into the approximately 4.7 hour EVA (egress to ingress).

J.M. Lepore
EVA Systems Analysis Group
Thermal and Fluid Process Analysis Project

Figure 11: STS-86 thermal findings (page 1 of 2)

Table 1
U. S. SAFER STS-86 Post-flight Analysis
Component Temperature Predictions

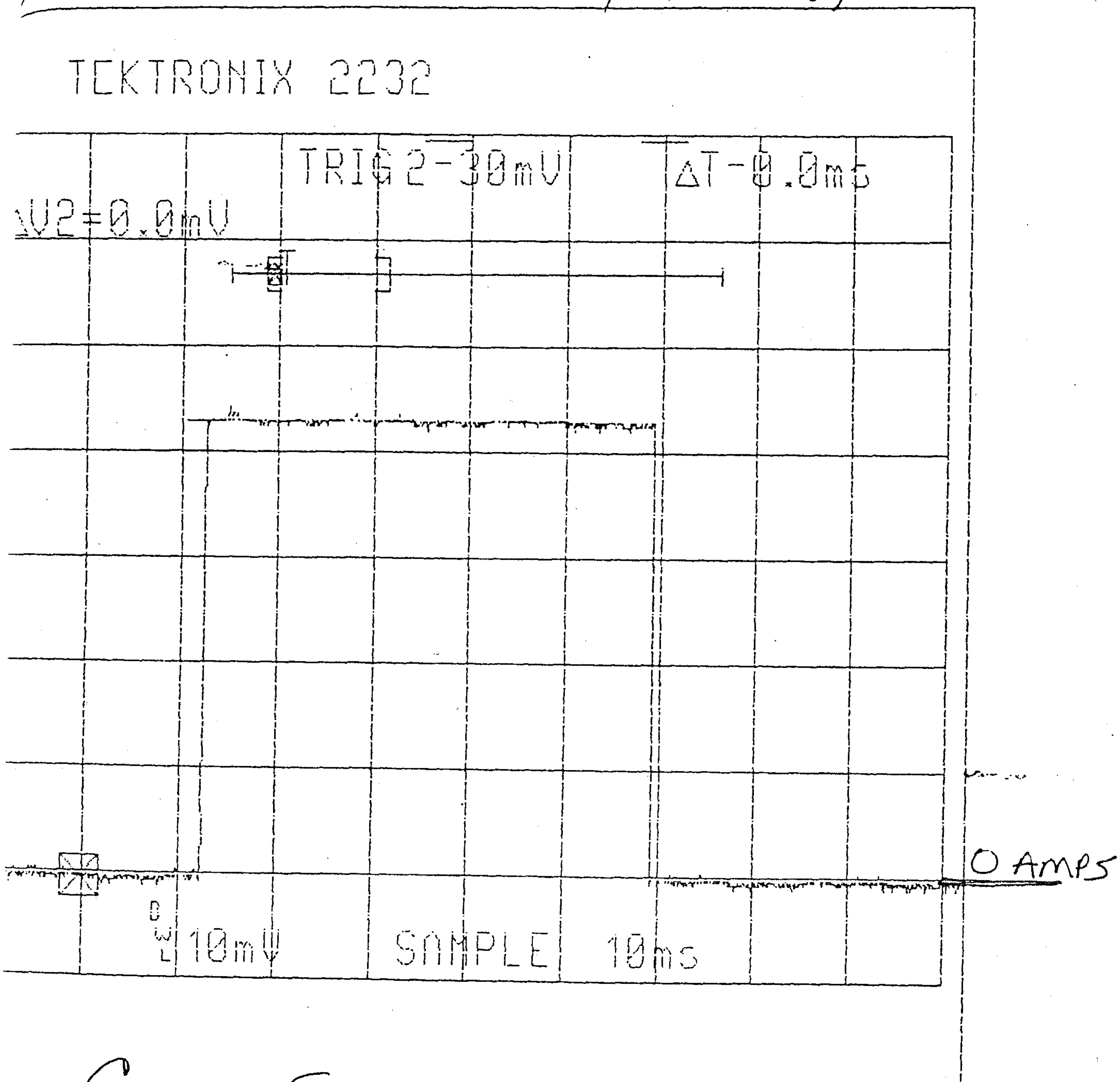
Component	Temperature (F)
Tower Housing	8
Tower Thruster	10
Prop. Module Housing (avg)	18
Avionics	31
GN2 Tank	27
Pressure Regulator	19
Rate Sensor	19
Battery	28
HCM LCD	26
HCM Electronics	28
HCM knob Switch	29
HCM Gimbal Switch	35

Notes: (1) All temperatures are after 4.1 hours exposure
(2) Initial SAFER temperature is 51 °F (tunnel adapter)
(3) As-flown attitude used (IO 5.1 +141/142, Sun R 233 P 155)
(4) EVA timeline used to determine appropriate flux cube locations (environment) for transient analysis

Figure 11: STS-86 thermal findings (page 2 of 2)

TS 9720313
Step 11
SAIC 63

NSI CURRENT (BATTERY S/N 1008)



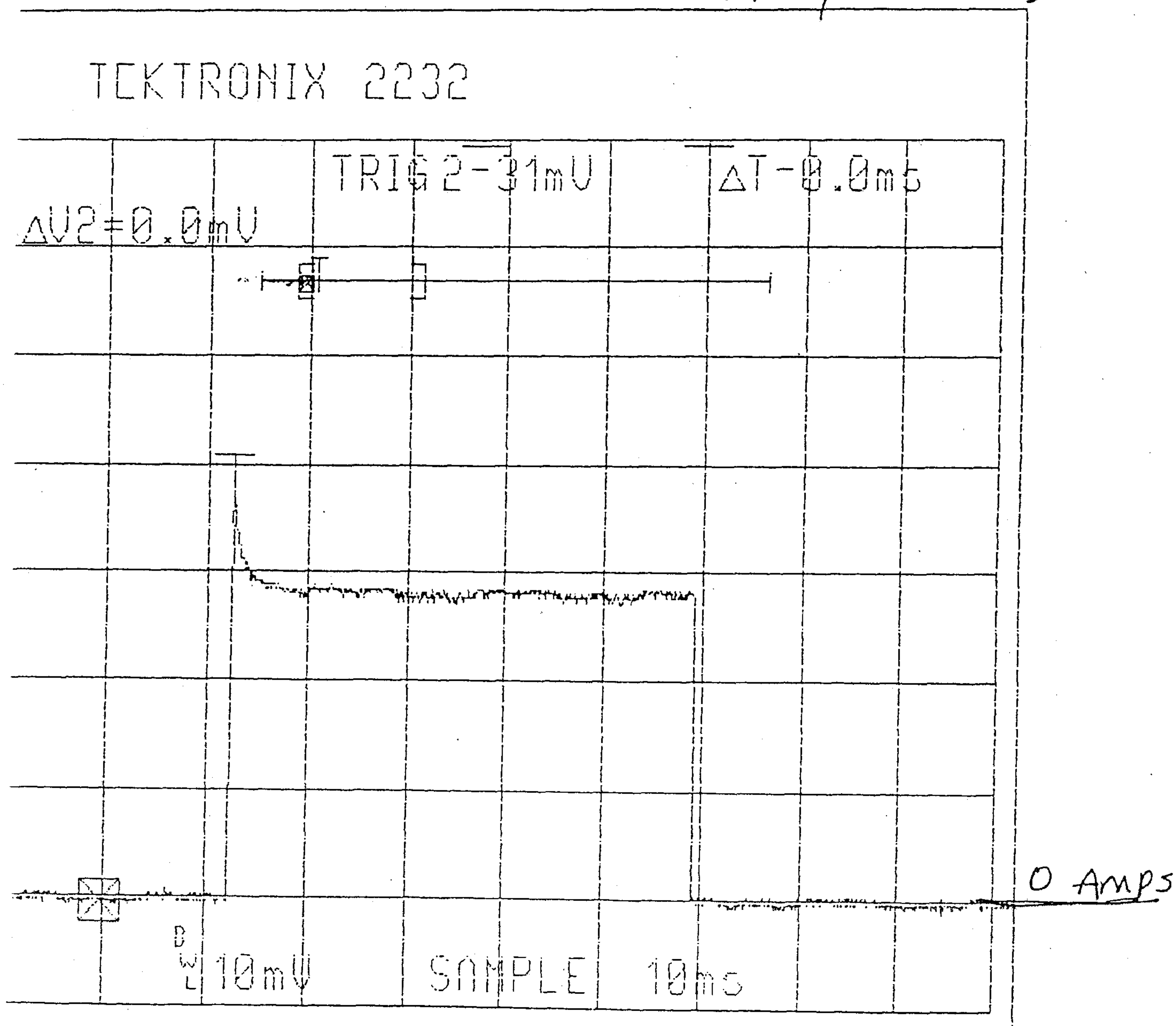
CURRENT SCALE - 1.0 AMP/DIVISION
TIME SCALE - 10 msec/DIVISION

Figure 12: Nominal/design NSI fire current pulse

ATTACHMENT 11-20-4
SAIC 63

TP972031
Step 14

NSI CURRENT (BATTERY S/N 1010)

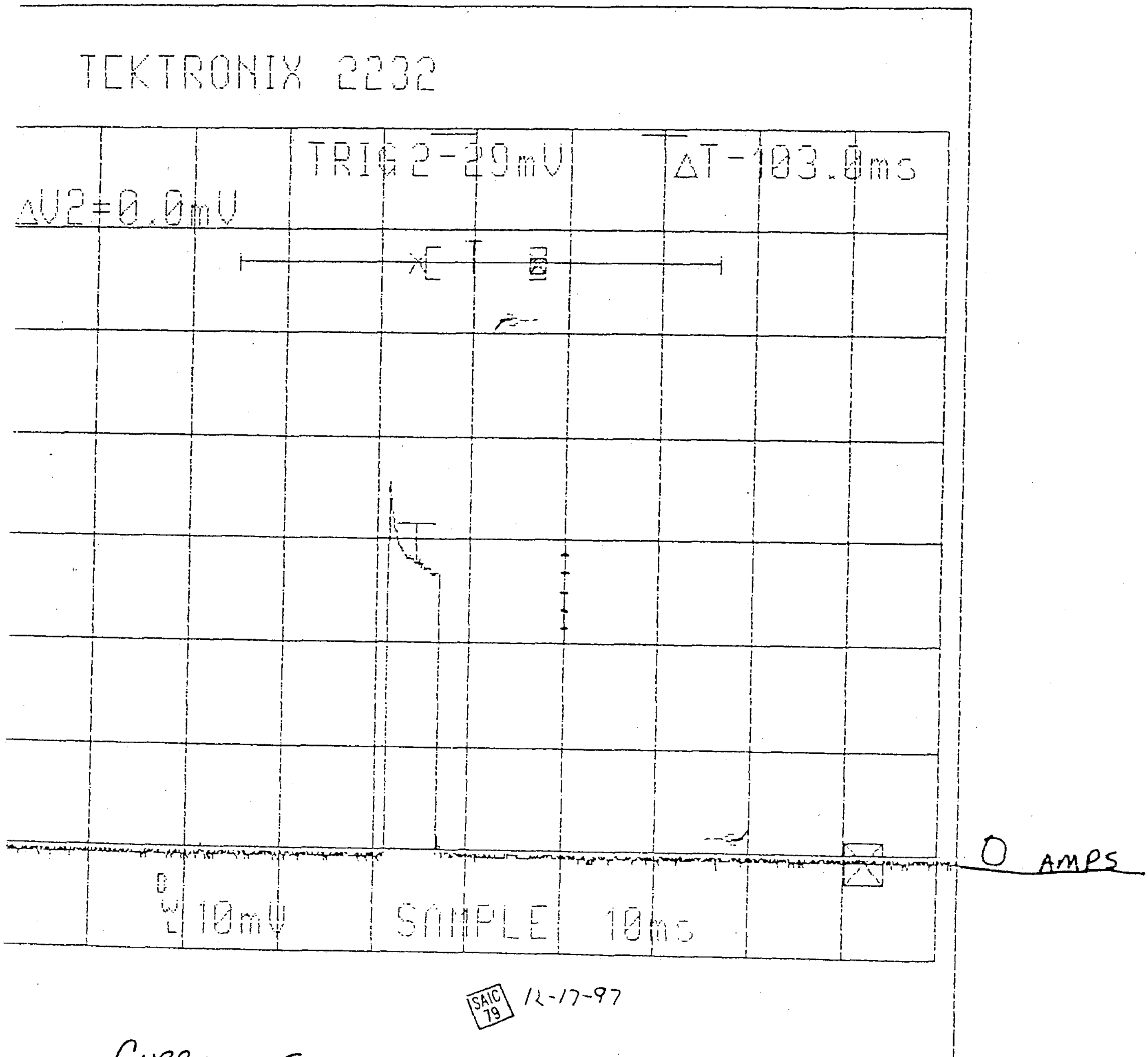


CURRENT SCALE — 1.0 AMP/DIVISION
TIME SCALE — 10 msec/DIVISION

Figure 13: Off nominal NSI fire current pulse

IS 9720327
Run #1

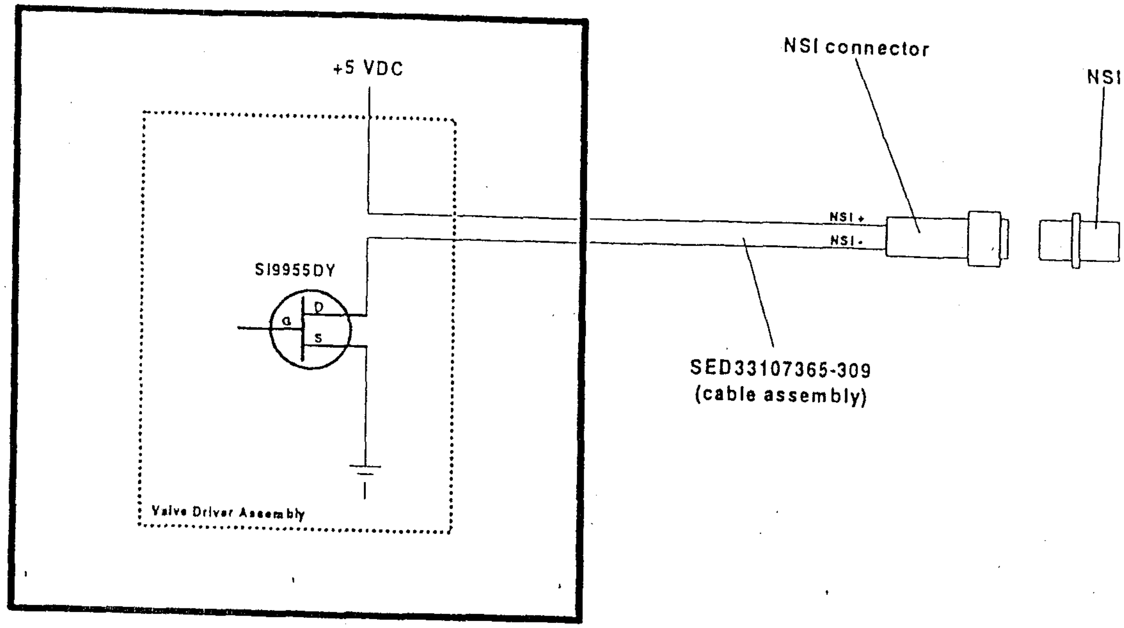
NSI CURRENT VS TIME (BATTERY S/N 1010)



CURRENT SCALE — 1.0 AMP/DIVISION
TIME SCALE — 10 msec/DIVISION

Figure 14: Successful NSI fire current pulse

NSI DRIVE CIRCUIT DESIGN (POST CDR BASELINE)



- SAFER NSI DRIVE CIRCUIT CDR BASELINE WAS MODIFIED TO PROVIDE NSI CURRENT FROM A 5 VDC 30 WATT SWITCHING REGULATOR USED IN THE AVIONICS DESIGN.. THE CIRCUIT PROVIDES 4.1 AMPS NOMINAL CURRENT FOR A NSI RESISTANCE OF 1.05 ohms +/- .10 ohms.**
- FOR 4.1 AMP NSI CURRENT, THE BATTERY ASSEMBLY MUST PROVIDE ~26 WATTS TO THE AVIONICS SUBSYSTEM TO FIRE NSI IN ADDITION TO THE BASELINE AVIONICS SUBSYSTEM CURRENT.
- DURING CERTIFICATION UNIT TESTING, ALL NSI FIRING ATTEMPTS WERE SUCCESSFUL.
- POST STS-86 FLIGHT ANOMALY TESTING HAS DETERMINED THAT THE NSI RESISTANCE INCREASES TO ~1.63 ohms DUE TO BRIDGEWIRE HEATING. FOR A NSI RESISTANCE OF 1.63 ohms, THE NSI CURRENT PROVIDED IS ~2.7 AMPS.**

** NSI BRIDGEWIRE SPECIFICATION IS 1.05 ohms +/- .10 ohms. THE ALL-FIRE CURRENT IS 3.5 AMPS.

Figure 15: STS-86 NSI circuit design (page 1 of 2)

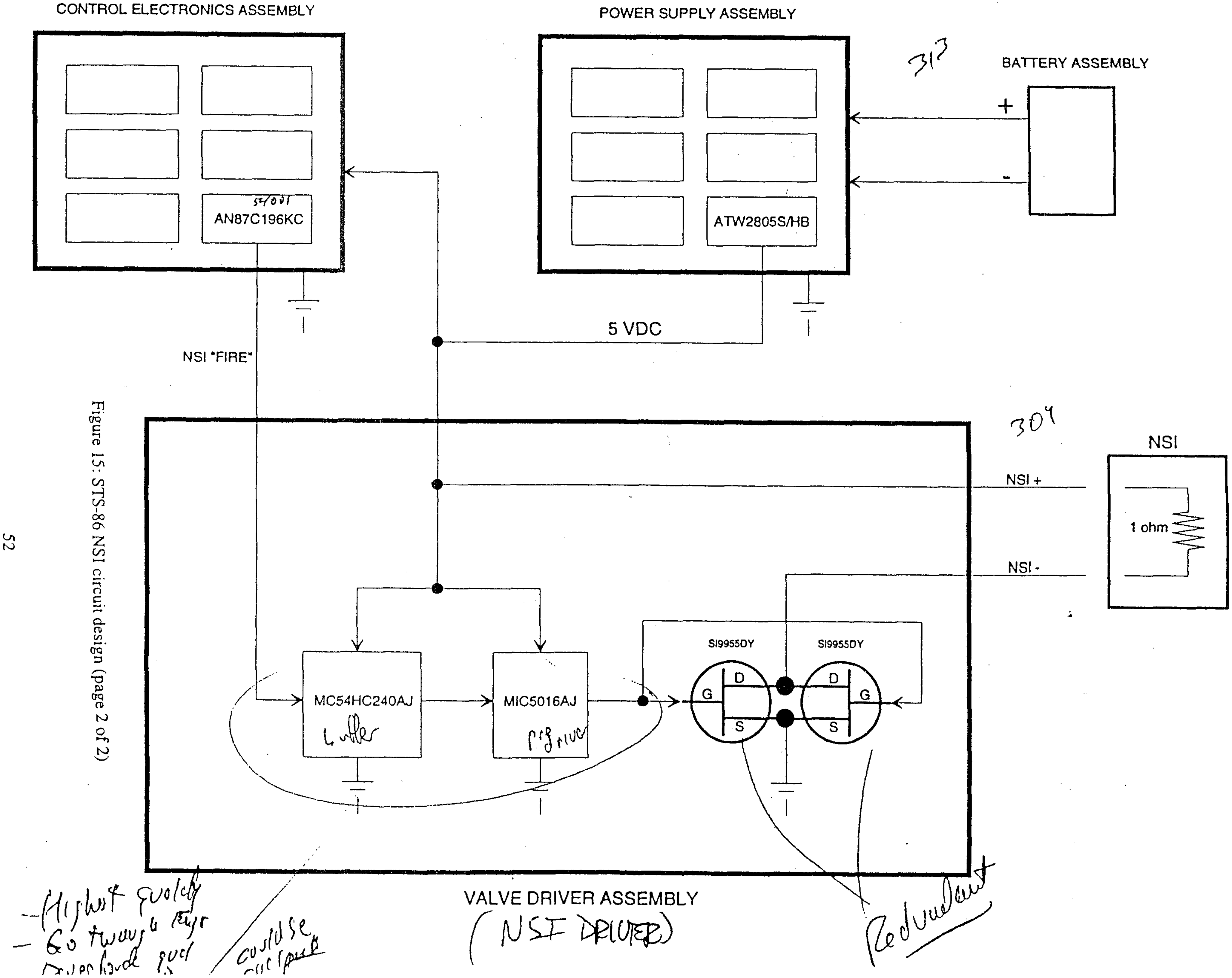
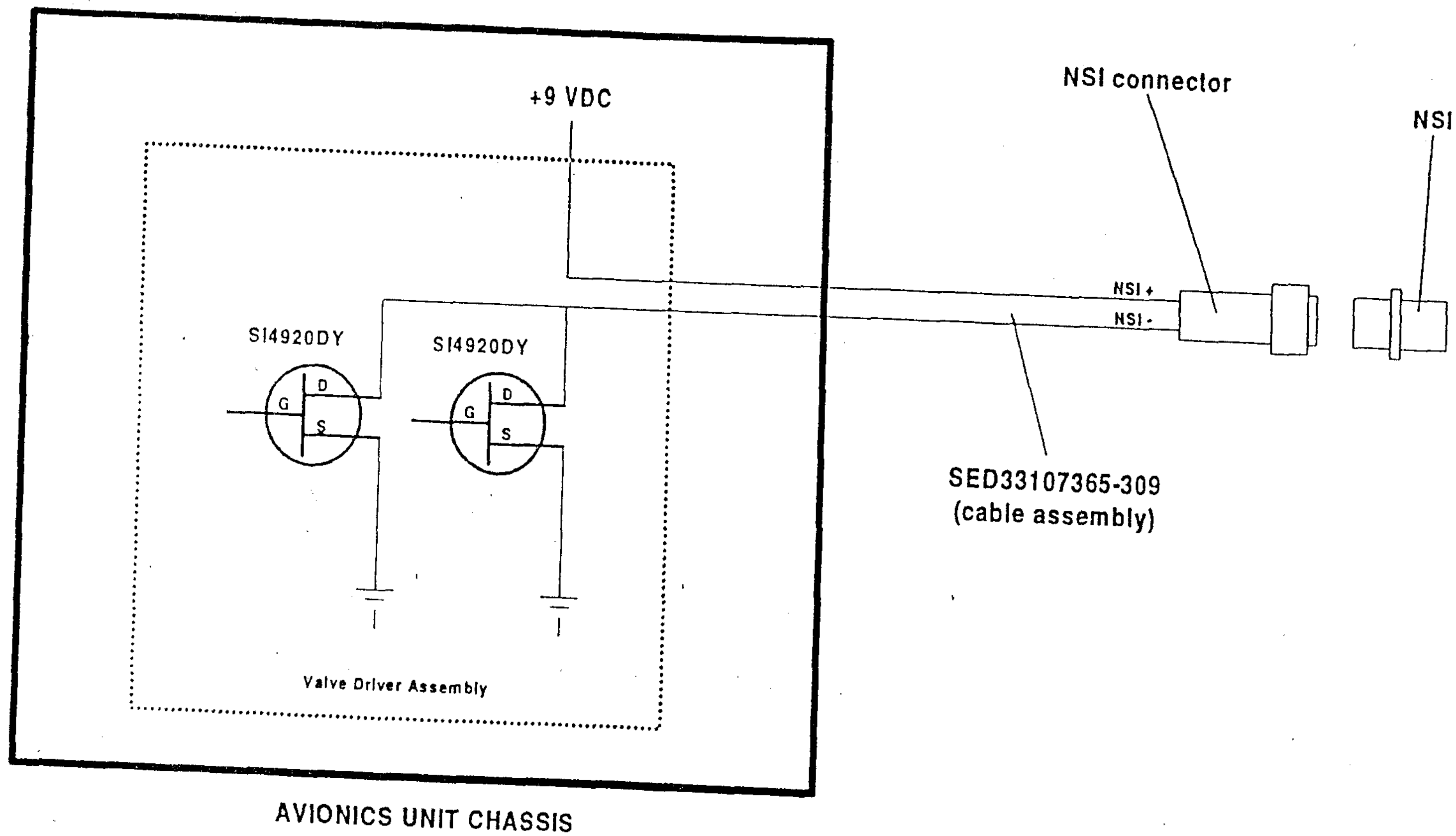


Figure 15: STS-86 NSI circuit design (page 2 of 2)

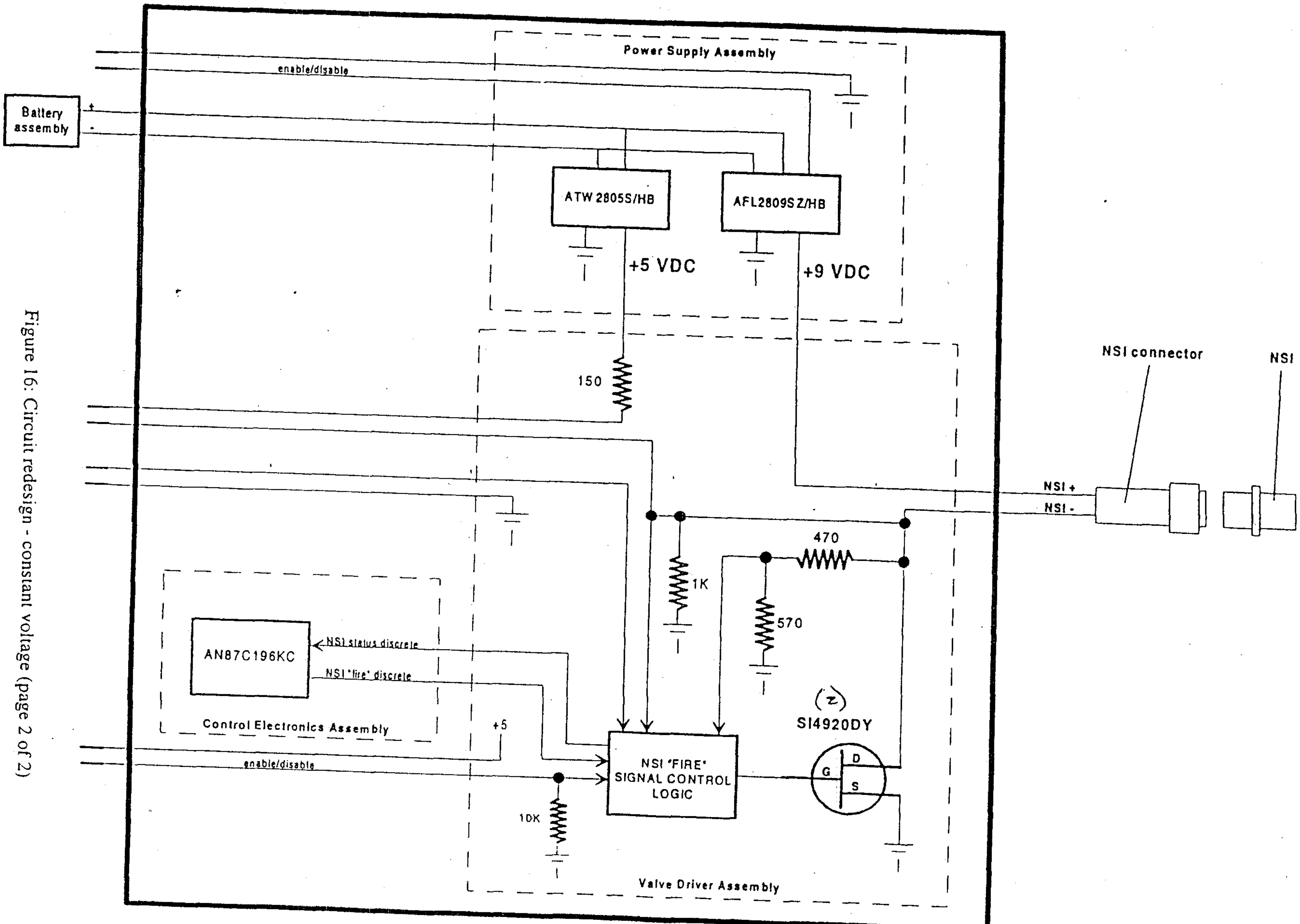
RECOMMENDED NSI DRIVE CIRCUIT DESIGN CHANGE (OPTION 1)



- SAFER AVIONICS SUBSYSTEM WILL BE MODIFIED TO PROVIDE NSI DRIVE CURRENT FROM A 9 VDC 90 WATT SWITCHING REGULATOR ADDED TO THE AVIONICS DESIGN..
- NSI DRIVE CIRCUIT WILL BE DESIGNED TO PROVIDE ~ 7.0 AMPS NOMINAL NSI CURRENT FOR ~47 MSEC. FOR NSI RESISTANCE OF 1.05 ohm +/- 0.1 ohm. THE DRIVE CIRCUIT WILL PROVIDE ~ 5.0 AMP NSI CURRENT FOR NSI RESISTANCE OF 1.5 ohm AND ~ 4.0 AMP NSI CURRENT FOR NSI RESISTANCE OF 2.0 ohm.
- NSI DRIVE CIRCUIT WILL BE DESIGNED TO BE DUAL-REDUNDANT.

Figure 16: Circuit redesign - constant voltage (page 1 of 2)

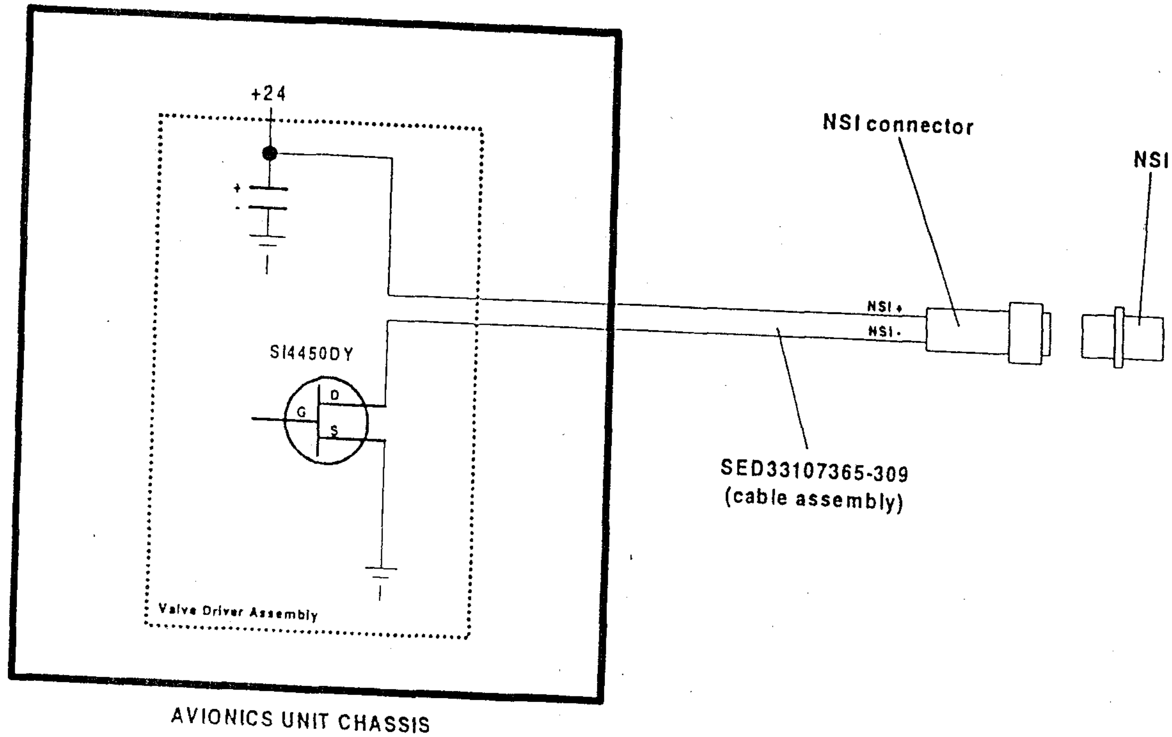
PROPOSED SAFER NSI DRIVE CIRCUIT FLIGHT CONFIGURATION - OPTION #1



AVIONICS UNIT CHASSIS

Figure 16: Circuit redesign - constant voltage (page 2 of 2)

RECOMMENDED NSI DRIVE CIRCUIT DESIGN CHANGE (OPTION 2)



- SAFER AVIONICS SUBSYSTEM WILL BE MODIFIED TO PROVIDE NSI DRIVE CURRENT FROM THE ENERGY STORED IN A 1320 uF CAPACITOR.
- THE AVIONICS SUBSYSTEM WILL PROVIDE NO LESS THAN 110 MILLIJOULES OF ENERGY TO THE NSI IN 5.0 MILLISECONDS.
- 1320 uF CAPACITOR WILL BE CHARGED TO +24 VOLTS WHEN AVIONICS IS POWERED ON.
- THE BATTERY ASSEMBLY DOES NOT HAVE TO PROVIDE ADDITIONAL POWER TO THE AVIONICS SUBSYSTEM IN ADDITION TO THE BASELINE AVIONICS SUBSYSTEM CURRENT DURING THE TIME THE NSI IS FIRED.

Figure 17: Circuit redesign - capacitive discharge (page 1 of 2)

PROPOSED SAFER NSI DRIVE CIRCUIT FLIGHT CONFIGURATION - OPTION #2

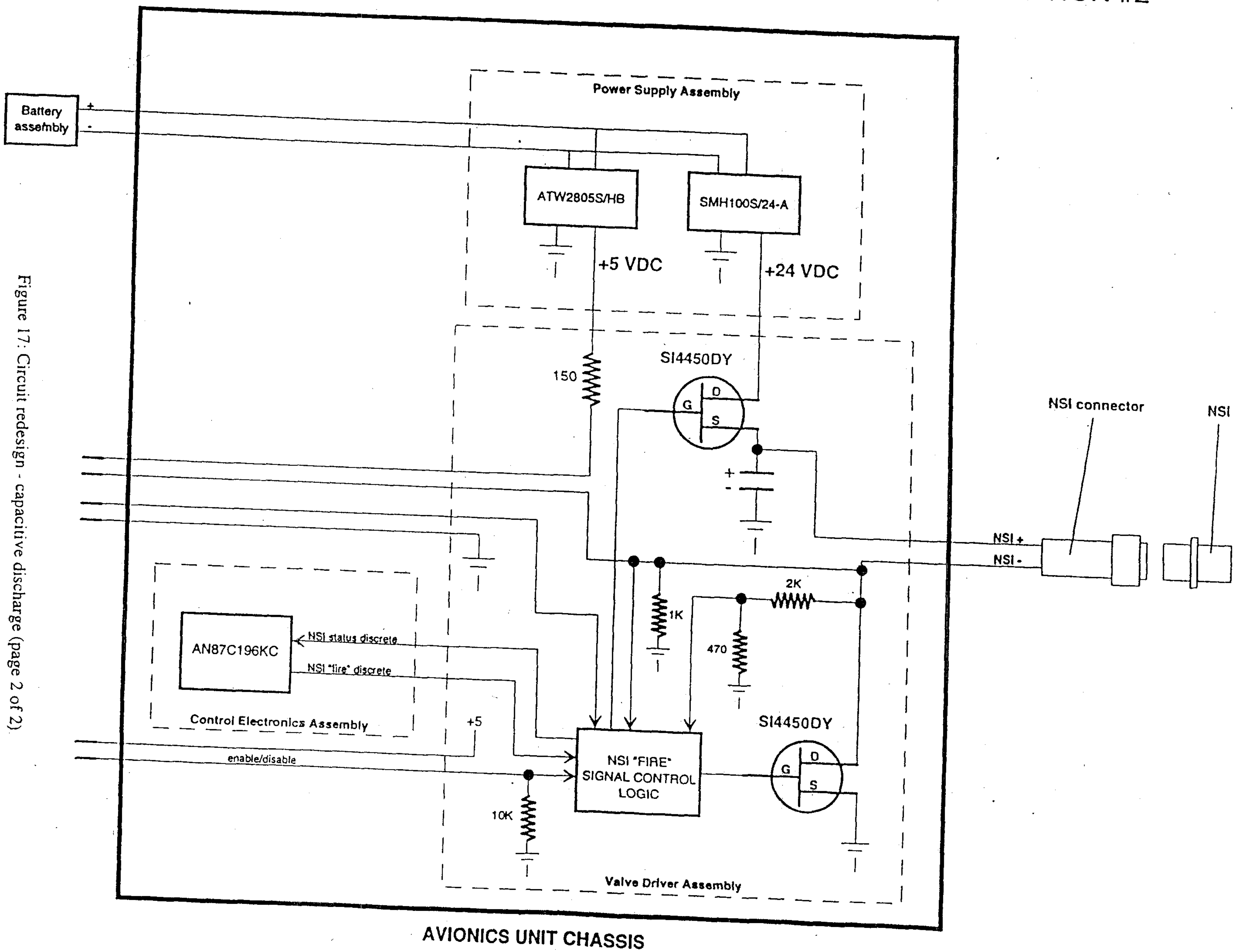


Figure 17: Circuit redesign - capacitive discharge (page 2 of 2)