3 1176 00166 6842

NASA TM-82615

NASA-TM-82615 19810016459

DOE/NASA/51040-25
NASA TM-82615

System Safety in Stirling Engine Development

H. Bankaitis
National Aeronautics and Space Administration
Lewis Research Center

Work performed for
U.S. DEPARTMENT OF ENERGY
Conservation and Solar Energy
Office of Transportation Programs

LIBRARY COPY
JUN 30 1981
LANGLEY RESEARCH CENTER
LIBRARY, NASA
HAMPTON, VIRGINIA

Prepared for
Fifth International System Safety Conference
Denver, Colorado, July 26-31, 1981

NOTICE

This report was prepared to document work sponsored by the United States Government. Neither the United States nor its agent, the United States Department of Energy, nor any Federal employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.

DOE/NASA/51040-25
NASA TM-82615

System Safety in Stirling Engine Development

H. Bankaitis
National Aeronautics and Space Administration
Lewis Research Center
Cleveland, Ohio 44135

Work performed for
U.S. DEPARTMENT OF ENERGY
Conservation and Solar Energy
Office of Transportation Programs
Washington, D.C. 20545
Under Interagency Agreement DE-AI01-77CS51040

Fifth International System Safety Conference
Denver, Colorado, July 26-31, 1981

N81-24994 #

SYSTEM SAFETY IN STIRLING ENGINE DEVELOPMENT

by H. Bankaitis

National Aeronautics and Space Administration
Lewis Research Center
Cleveland, Ohio 44135

E-867

INTRODUCTION

The Department of Energy has established a number of broad programs aimed at reducing highway fuel consumption. One of the programs addresses the Stirling engine propulsion system as a possible alternative to the conventional spark-ignition engine. The objective of this program is the development, by 1984, of a Stirling engine system having at least 30 percent improvement in fuel economy (mpg) over production vehicles powered by conventional spark-ignition engines of the same weight and performance, based on equal Btu content of fuel used.

Two aspects make this program unique. The first aspect is the Stirling cycle itself. The most pronounced characteristic of the Stirling engine is its external combustion heat source and closed-loop working gas arrangement to convert heat into work energy. Although almost any type of gas may be used as a working gas in the Stirling cycle, gaseous hydrogen, because of its heat transfer characteristics and resulting high power output, has been selected for use in the automotive Stirling engine application. The second aspect is the background of the Government-industry team implementing the program. It is a joint effort between the Government represented by a DOE-NASA team and an industry team represented by Mechanical Technology, Inc. (MTI), United Stirling of Sweden, and AM General (AMG). The engine development program is based on the extensive technological background knowledge and existing P-40 Stirling engine hardware of United Stirling of Sweden acting as a subcontractor to MTI. AMG, a wholly owned subsidiary of American Motors Corp. (AMC), is the subcontractor responsible for automotive selection and for integration and evaluation of United Stirling of Sweden-designed Stirling engines installed in passenger cars.

To demonstrate the use of Stirling engines in passenger vehicles, to assist in assessing the current state of technology, and to determine the potential problems associated with the installation and operation of Stirling engines in automobiles, it was desirable to make an early demonstration of a Stirling-engine-powered passenger vehicle. Thus an existing nonautomotive P-40 Stirling engine originally designed as a stationary, laboratory "test bench" engine for development of auxiliaries, subsystems, and components was adapted for automotive powerplant evaluation and installed in a production vehicle, the 1977 Opel Rekord 2100 Diesel sedan. The objectives of the Opel Rekord - P-40 Stirling engine integration test have been successfully met (ref. 1). In addition, to show the suitability of a Stirling engine in a U.S.-manufactured car, AMC passenger cars were selected for P-40 integration and evaluation testing. These vehicles are now undergoing testing.

The approach to the system safety aspects of this program has been two pronged. The first phase was the initial effort by the Lewis Research Center, which consisted of a top-level fault tree system safety assessment directed at one facet of the P-40 Stirling-engine-powered AMC vehicle. The second phase entails contractor's efforts during various phases of the Mod-1 and subsequent engine design work. The efforts are very preliminary and are not yet properly

structured. United Stirling of Sweden has performed a limited failure modes and effects analysis (FMEA) on the intended air-fuel system. MTI has engaged MGA Research Corp., who has reviewed automotive Stirling engine safety issues. The effort most applicable to and influential in automotive Stirling engine design is the ASE Mod-1 design and performance audit by MTI's engineering staff. In this audit system safety issues across the board are addressed by chosen experts in an FMEA fashion. In this second and more complicated phase, emphasis should be placed on recognizing differences in language, units used, materials chosen, and vendor's capabilities as well as the problem of working with both mechanical and electronic functions, hydrogen effects on metals, and the complexities of tiers of project management.

The first phase of this program is described in the remainder of this paper.

SYSTEM DESCRIPTION

The United Stirling of Sweden P-40 Stirling engine (a four-cylinder, double-acting, U-drive configuration) consists of an air preheater, a combustor, a heater, an enclosed working gas, a regenerator, a cooler and a conventional drive unit (crossheads, connecting rods, crankshaft, and drive shaft lubrication) (fig. 1). All the other auxiliaries are similar to those used in conventional spark-ignition-engine-powered vehicles. The most pronounced characteristic of the Stirling engine is its external combustion heat source and closed-loop working gas arrangement to convert heat into work energy. Combustion air and fuel are continuously burned in the combustors, and are regulated by an air-fuel control system shown in figure 2. The hot combustion gases are passed around the outside of the heater tubes and heat is transferred to the interior, enclosed working gas. The working gas moves back and forth between the top hot space of one cylinder and the cold bottom space of the next cylinder, hence the double-acting principle. Passing between the top hot space of one cylinder and the cold bottom space of the next cylinder, the working gas relinquishes some of its heat content to a regenerator, which releases the heat back into the gas upon its return from the cold space of the cylinder. A cooler is used to further cool the gas prior to compression in the cold bottom space of the cylinder. This action by the working gas provides driving force for the pistons that is converted to shaft torque and power to the wheels. Increased engine power is obtained by increasing the working gas pressure in the engine. Conversely, to decrease engine power the working gas pressure in the engine must be decreased. To accomplish these tasks three separate, yet integral, systems are arranged to act in concert. These three systems are the mean-pressure power control system, the air-fuel temperature control system, and the electronic power control unit.

The mean-pressure power control system is used to vary and control the working-gas pressure in the Stirling engine cycle for driveability characteristics very similar to those of a conventional spark-ignition engine. The power control system consists of the working gas storage tank, the control valve, and the working gas compressor. Figure 3 shows the power control system; figure 4 is a more detailed schematic of the total control system. To increase engine pressure, the working gas is allowed to flow from the storage tank through the control valve to the engine. To decrease engine pressure, working gas is allowed to flow through control valve to the compressor and is then pumped back to the storage tank. For a more rapid decrease in pressure,

the control valve short circuits the working gas between the cylinders. Thus the power control valve performs three functions:

(1) supplies working gas to the engine.
(2) removes working gas from the engine.
(3) short circuits the working gas between the cylinders.

These power demands on the engine, or pressure changes, result in a varying demand for heat in the working cycle of the engine, yet the heater temperature is kept constant. Thermocouple readings of the heater head tube temperature are converted to a signal controlling the position of the air throttle (fig. 2). A feedback signal to electronics ensures a stable throttle position. The air-fuel ratio is then controlled by a Bosch K-Jetronic unit.

The electronic power control unit is the link between the accelerator pedal and the power control system. The accelerator potentiometer signal is compared with engine speed and working gas pressure in the engine. Comparison of these signals triggers the servovalve (an integral part of the power control valve) to flow the working gas either to the engine or from the engine to the storage tank. Both engine speed and engine pressure signals are provided by transducers.

THE WORKING GAS

Although almost any type of gas can be used as the working gas in the Stirling cycle, gaseous hydrogen, because of its heat transfer characteristics and resulting high power output, has been selected for use in the automotive Stirling engine application.

Approximately 100 g (1 liter) of gaseous hydrogen at a mean pressure of 20 MPa (200 atm) is sealed within the engine while approximately 700 g (7 liters) of gaseous hydrogen at approximately 20 MPa (200 atm) is in the storage bottle (fig. 5.).

DEPLOYMENT

Six P-40 Stirling engines are used in this phase of the program. Three of the six engines are installed in demonstration vehicles: engine ASE-40-5 in the 1977 Opel Rekord, engine ASE-40-8 in the 1979 AMC Spirit and ASE-40-12 in the AMC concord. The other engines are used as stationary R&D test beds at Lewis, MTI and United Stirling of Sweden. The P-40 Stirling engine will be phased out of this program by the Mod-1 and Mod-2 automotive Stirling engines (ASE).

SYSTEM SAFETY REQUIREMENTS

The NASA Stirling Engine Project Ofice has required that contractors make safety considerations an integral part of all phases of the Stirling engine program. However, regarding the P-40 Stirling engine, total implementation of the requirements was not feasible because the engine had been designed by United Stirling of Sweden with their own funding and no further refinements or redesigns had been contemplated as part of this program. This is not to imply that the engine is unsafe, prone to catastrophic failures, or poorly designed. On the contrary, it seems to be a well-designed piece of hardware that is being adapted for applications originally not anticipated by the designers. This particular application of the P-40 Stirling engine points to

the need for assessment of the engine's safety aspect. In addition, the initial P-40 system safety assessment will provide insight into the extent and type of system safety analysis that will be necessary during ASE Mod-1 and Mod-2 engine design phases.

SAFETY ASSESSMENT - APPROACH, LIMITATIONS, AND ANALYSIS

Approach

Fault tree analysis (top level), which has been developed as a tool for system safety analysis, is designed to ferret out circumstances that a system may not have been designed to handle and for which some additions or modifications are needed to minimize risks of serious accident. The major advantage in using this particular technique is that the analysis can begin at any point (level) and can be extended as far as knowledge permits or suspended upon reaching a point of diminishing returns. By then a good basis for singling out the basic failure modes that deserve special attention should have been identified. At the single-component level this analysis technique is not distinguishable from reliability analysis. This may be used to calculate the probability of functional failure under circumstances not envisioned by the designer and to indicate design modifications necessary to minimize risks of hardware failure.

Top-level fault tree system saftety assessment was employed in a highly qualitative effort directed at one facet of the total P-40 Stirling-engine-powered AMC vehicles, namely the enclosed gas system. In the presented analysis, the probability of functional failure cannot be calculated because of the lack of component durability history. These data are now being accumulated and will be considered as an input into a more complete system safety analysis in the future. Top-level fault trees or other system safety analysis techniques must also be employed when assessing future Stirling engines, major systems, subsystems, and components during their respective design phases.

Definition of Top-Level Undesirable Effect

As described earlier the P-40 Stirling engine is an external combustion engine using gaseous hydrogen at high pressure and temperature as a working fluid to yield propulsive energy to a vehicle. The engine must function with the gaseous hydrogen working fluid contained within the system hardware designed for the purpose and be responsive to the operator's commands without endangering the well being of the operator, passengers, bystanders, or hardware. Thus the most undesired event for this segment of the P-40/Spirit system safety assessment is defined as follows:

"Explosion and/or fire due to unprogrammed, nonpredictable loss of the gaseous hydrogen working fluid."

Top-Level fault tree logic

Thus a fault tree (fig. 6 - displays 1-3) has been constructed by logically relating possible sequences of events that, if they occur, could result in the undesired event.

Limitations of analysis

It is important at this point to emphasize the limitations of this analysis. These limitations stem from the fact that the current P-40 engine is a stationary, bench-type experimental engine. Because of its highly experimental nature, NASA, MTI, and United Stirling of Sweden do not have all the necessary data or information pertaining to the engine. Furthermore some of the information about the P-40 engine is considered proprietary by United Stirling of Sweden and not available to the analyst. Therefore this analysis is limited by

(1) Consideration of the enclosed working gas system only
(2) Lack of operating and maintenance procedures, manuals, or instructions
(3) Very limited information on design specifications, test specifications, and component characteristics, materials, qualifications, etc.
(4) Unknown changes being made by United Stirling of Sweden in components, configuration, and materials
(5) Lack of direct contact with the systems and equipment designers responsible for the product
(6) Lack of a complete, comprehensive, and accurate set of system drawings
(7) Exclusion of human error in maintenance or operation of the engine

The basis source of information for this segment of the safety assessment consists of

(1) United Stirling of Sweden schematic of the Stirling engine
(2) Figures and descriptions in MTI progress and topical reports (ref. 1)
(3) Existing failure reports (refs. 2 to 5)
(4) Private communications with Lewis, MTI, and United Stirling of Sweden project and test engineering personnel
(5) Information regarding Stirling engine hydrogen safety tests performed by Stanford Research Institute and sponsored by Ford Motor Company (refs. 6 and 7)

Analysis of Displays

Display 1 (fig. 6). - The most undesired event may manifest itself either internally or externally to the engine. The events can take place when the engine is in the normal operating state (event R-2) including startup and shutdown sequences or when the engine is dormant (event R-3). Aside from the stresses induced by the normal operating cycle of the engine on its materials, parts, and components, an unevaluated source of additional stress is involvement of the vehicle in a collision or submitting it to unduly harsh road conditions or other vibrational environments (event D-1). The effects of a collision or an unusual vibration-shock environment cannot be fully assessed at this time because sufficient data are not yet available. The same is true for events D-2 and D-3. Further studies should be performed to properly evaluate the impact of events D-1, D-2, and D-3 on the system.

Considering event R-3, which takes place while the engine is in the nonoperating condition, event R-3.1 can only occur if catastrophic failure X-1 or X-2 takes place. However, some type of timely and proper-magnitude ignition source (F_1) would be necessary to cause the undesired event to occur. The

individual designation (F_1, F_2, F_3, etc.) of the conditions is based on the differences in probability of an ignition source occurring at the proper time with respect to gaseous hydrogen concentration. The ignition source cannot be specifically identified but could range from a cigarette or open flame to an activation of a sparking relay switch or even static charge produced by high-pressure gaseous hydrogen rushing over a sharp metallic point or edge.

Considering the event designated by R-2, which takes place during the operating mode, it appears that the most undesired event may manifest itself either internally to the engine (event R-4) or externally to the engine (event R-5). These events are represented in more detail in subsequent subdisplays.

Display 2 (fig. 6). - The most undesirable R-1 event internal to the engine (event R-4) may take place in the combustor (R-4.1), crankcase (R-4.2), or cooling system (R-4.3). An event in R-4.3 (D-4) is deferred to further study. Occurrence of R-4.3 seems possible if interface bolt and seal failure can occur. The extent of overpressurization of the cooling system to yield a pressure burst was not evaluated. This event might be a good candidate for further study and assessment. However, porosity in the cooling water jacket (failure X-4) and subsequent release of hydrogen gas into the cooling water system has been experienced. Occurrence of this event emphasizes the need to carefully select and closely control the manufacturing process as well as to use proper and effective nondestructive testing methods to facilitate acceptance of the parts.

Seal system failure, X-3, would have to occur to allow hydrogen gas to enter the crankcase. A schematic of the seal system is presented in figure 7. Although rotating machinery is present, its lubricating fluid most likely would prevent the occurrence of a friction spark or other type (including hot surface) of ignition. In operational failures of this type experienced to date, leakage through this seal resulted in an unacceptable loss of either engine power or maintainability of the required working gas pressure, thus leading to an orderly engine shutdown by the operator. Prolonged operation at that condition most likely would lead to degradation of the lubricating fluid through hydrogenation and to gaseous hydrogen being vented from the crankcase to either the engine compartment or the immediate surroundings of the vehicle.

In event R-4.1, gaseous hydrogen release may occur during the startup sequence (event R-4.1), during the engine operating sequence (event R-4.1.2), or even during the engine shutdown sequence (event R-4.1.3) when residual heat in the engine is still prominent. These events are detailed in displays 2A, 2B, and 2C, respectively. Most frequent causes for such occurrences would be material failures, improper workmanship, or maintenance inattention. Effects of the gaseous hydrogen containment-wall failures during the startup sequence would depend on the extent of failure. If a slow leak is taking place, it is conceivable that the system could be pressurized to attempt a start, but then it would be necessary for the purging cycle to fail (F_7) to produce undesired event R-1. A large, sudden leak prior to activating the igniter in the combustor would most likely cause an automatic abort because of pressure drop. Still it is likely that some rotating blower, switch spark, or static discharge could cause detonation in the combustor.

With respect to failure X-8, the reportedly seamless heater head tubes containing gaseous hydrogen are not really seamless. These tubes are manufactured by rolling plate material into a tube, welding the seam, and then drawing the tube to the desired diameter, thus obliterating the seam weld.

Display 3 (fig. 6). - This display exhibits events leading to the presence of unrestrained gaseous hydrogen external to the engine (event R-5). The event may occur in the engine compartment only (event R-5.1), in the passenger compartment (event R-5.2), and in the external perimeter of the vehicle (event R-5.3).

Failures leading to event R-5.1 are of catastrophic nature, with the exception of D-7. Location of the crankcase vent is determined by the designer, and its contribution to event R-5.1 depends on the aforementioned seal system failure (X-3). This can vary for different engine designs. Failures X-12 and X-13 have not been experienced to date. Failure X-14 has been experienced quite often and damages, failure modes, and effects are well documented in reference 3 and in routine failure notice reports (form NASA-C-591).

Fire and detonation experienced with an X-14 failure have been easily contained by the engine compartment enclosures. However, NASA test engine experience clearly shows that check-valve failures result in metallic check-valve parts being lodged in various valve seats, regenerators, and line filters, causing these components to work improperly or to fail completely.

Event R-5.2 is cause for concern because gaseous hydrogen cannot be detected by smell or sight, thus its presence of 4 percent in the air mixture presents a real danger to the operator and the passengers. This problem is further compounded if smoking is permitted inside the demonstrator vehicle.

For the P-40/Spirit the most likely cause of event R-5.3 is failure X-19. As shown in figure 8 the gaseous hydrogen storage bottle with its associated fittings and supply line is located in the left front wheel well of the vehicle. Neither the high-pressure hydrogen storage bottle nor the fittings and line have any protection against debris impact. This situation if not corrected could lead to catastrophic failure of the fitting or line by impact, thus releasing approximately 7 liters of high-pressure gaseous hydrogen. Even if no other ignition source was present, static discharge over sharp points would most certainly cause fire (event R-1).

The X-19 and X-2 failures in event R-5.3.1 can also be caused by the failure of storage bottle holding mounts. This would allow the storage bottle to drop onto the wheel, possibly rupturing the bottle but most certainly breaking the high-pressure line.

Failures X-17 and X-18 would occur only if the valve packing or valve body catastrophically failed, thus instantaneously releasing the whole storage content. A combination of high gas pressure and sharp edges of failed valve body or packing could provide an electrostatic ignition source, thus resulting in the most undesired event (R-1).

Accidental dumping of gaseous hydrogen by untimely activation of dump valve (failures X-15 and X-16, event R-5.3.1) may be caused by a combination of electronic signal occurrences.

Evaluation of Fault Tree

The constructed fault tree as presented (fig. 6) is only a qualitative safety assessment of one facet of a Stirling engine system. Quantitative measurement can only be obtained through experimental data that reveal component failure rate. The qualitative results include the critical paths of the fault tree and the qualitative importances of the component failures on the fault tree. The critical paths are defined as the combinations of component failures that will cause system failure. The qualitative importance gives a ranking to each component with regard to its contribution to system failure.

To facilitate analysis of the fault tree critical paths, a set of Boolean equations can be derived for each of the failure modes:

$$R_1 = R_2 + R_3 \quad (1)$$

$$R_2 = R_4 + R_5 + F_1 \cdot D_1 + F_2 \cdot D_2 + F_3 \cdot D_3 \quad (2)$$

$$R_3 = F_4 \cdot (R_{3.1} + D_1 + D_2) \quad (3a)$$

$$R_{3.1} = X_1 + X_2 \quad (3b)$$

$$R_3 = F_4 \cdot (X_1 + X_2 + D_1 + D_2) \quad (4)$$

$$R_4 = R_{4.1} + R_{4.2} + R_{4.3} \quad (5a)$$

$$R_{4.1} = R_{4.1.1} + R_{4.1.2} + R_{4.1.3} \quad (5b)$$

$$R_{4.1.1} = I_1 \cdot F_7 \cdot (X_5 + R_{4.1.1.1}) \quad (5c)$$

$$R_{4.1.1.1} = X_6 + X_7 + X_8 \quad (5d)$$

$$R_{4.1.1} = I_1 \cdot F_7 \cdot (X_5 + X_6 + X_7 + X_8) \quad (5e)$$

$$R_{4.1.2} = I_1 \cdot (X_9 + X_{10} + X_5 + X_{11} + X_6 + X_7 + X_8) \quad (5f)$$

$$R_{4.1.3} = I_2 \cdot (D_5 + D_6 + R_{4.1.3.1}) \quad (5g)$$

$$R_{4.1.3.1} = X_9 + X_{10} + X_5 + X_{11} + R_{4.1.3.1.1} \quad (5h)$$

$$R_{4.1.3.1.1} = X_6 + X_7 + X_8 \quad (5i)$$

$$R_{4.1.3} = I_2 \cdot (D_5 + D_6 + X_9 + X_{10} + X_5 + X_{11} + X_6 + X_7 + X_8) \quad (5j)$$

$$R_{4.1} = [I_1 \cdot F_7 (X_5 + X_6 + X_7 + X_8) + I_1 \cdot (X_9 + X_{10} + X_{11} + X_5 + X_6 + X_7 + X_8) + I_2 \cdot (D_5 + D_6 + X_9 + X_{10} + X_5 + X_{11} + X_6 + X_7 + X_8)] \quad (6)$$

$$R_{4.2} = F_5 \cdot (X_3) \quad (7)$$

$$R_{4.3} = F_6 \cdot (D_4 + X_4) \quad (8)$$

Substituting equations (6) to (8) into equation (5a) yields

$$R_4 = [I_1 \cdot F_7 \cdot (X_5 + X_6 + X_7 + X_8) + I_1 \cdot (X_9 + X_{10} + X_5 + X_{11} + X_6 + X_7 + X_8) + I_2 \cdot (D_5 + D_6 + X_9 + X_{10} + X_5 + X_{11} + X_6 + X_7 + X_8) + F_5 \cdot (X_3) + F_6 \cdot (D_4 + X_4)] \quad (9)$$

Also one can obtain

$$R_5 = R_{5.1} + R_{5.2} + R_{5.3} \quad (10a)$$

$$R_{5.1} = I_3 \cdot F_8 \cdot (D_7 + X_{12} + X_{13} + X_{14}) \quad (10b)$$

$$R_{5.2} = I_4 \cdot R_{5.2.1} \quad (10c)$$

$$R_{5.2.1} = D_8 + D_9 \quad (10d)$$

$$R_{5.2} = I_4 \cdot (D_8 + D_9) \quad (10e)$$

$$R_{5.3} = F_9 \cdot (X_{21} + X_2 + X_{20} + X_{18} + X_{19} + X_{17} + R_{5.3.1.1}) \quad (10f)$$

$$R_{5.3.1.1} = X_{15} + X_{16} + I_5 \cdot D_{10} \quad (10g)$$

$$R_{5.3} = \{(F_9 \cdot [(X_{21} + X_2 + X_{20} + X_{18} + X_{19} + X_{17}) + X_{15} + X_{16} + I_5 \cdot D_{10}]\} \quad (10h)$$

$$R_5 = \{(I_3 \cdot F_8 \cdot (D_7 + X_{12} + X_{13} + X_{14}) + I_4 \cdot (D_8 + D_9) + F_9 \cdot [(X_{21} + X_2 + X_{20} + X_{18} + X_{19} + X_{17}) + X_{15} + X_{16} + I_5 \cdot D_{10}]\} \quad (11)$$

Then substituting equations (9) and (11) into equation (2) yields

$$R_2 = \{I_1 \cdot F_7 \cdot (X_5 + X_6 + X_7 + X_8) + I_1 \cdot (X_9 + X_{10} + X_5 + X_{11} + X_6 + X_7 + X_8) + I_2 \cdot (D_5 + D_6 + X_9 + X_{10} + X_5 + X_6 + X_{11} + X_7 + X_8) + F_5 \cdot (X_3) + F_6 \cdot (D_4 + X_4) + I_3 \cdot F_8 \cdot (D_7 + X_{12} + X_{13} + X_{14}) + I_4 \cdot (D_8 + D_9) + F_9 \cdot [X_{21} + X_2 + X_{20} + X_{18} + X_{19} + X_{17} + X_{15} + X_{16} + I_5 \cdot D_{10}] + F_1 \cdot D_1 + F_2 \cdot D_2 + F_3 \cdot D_3)\} \quad (12)$$

Substituting equation (12) for R_2 and equation (4) for R_3 in equation (1) gives the final equation for R_1:

$$R_1 = \{I_1 \cdot F_7 \cdot (X_5 + X_6 + X_7 + X_8) + I_1 \cdot (X_9 + X_{10} + X_5 + X_{11} + X_6 + X_7 + X_8) + I_2 \cdot (D_5 + D_6 + X_9 + X_{10} + X_5 + X_6 + X_{11} + X_7 + X_8) + F_5 \cdot (X_3) + F_6 \cdot (D_4 + X_4) + I_3 \cdot F_8 \cdot (D_7 + X_{12} + X_{13} + X_{14}) + I_4 \cdot (D_8 + D_9) + F_9 \cdot [X_{21} + X_2 + X_{20} + X_{18} + X_{19} + \quad (13)$$

$X_{17} + X_{15} + X_{16} + (I_5 \cdot D_{10})] + F_1 \cdot D_1 + F_2 \cdot D_2 +$

$F_3 \cdot D_3 + F_4 \cdot (X_1 + X_2 + D_1 + D_2)\}$

From equation (13) for the final event R_1, minimal cut sets or critical paths can be established within the set of all possible failures. A minimal cut set or critical path is the smallest combination of basic events that must occur to cause the top event to develop. These cut sets can be ranked in terms of most likely failure modes once component failures within them are known. Thus the likelihood of event R_1 occurring by a particular cut set or critical path can be established. This is given by the sum of the cut-set probabilities. A listing of the events that comprise a particular cut set leading to event R_1 is presented as follows:

(1) F_1 with D_1

(2) F_2 with D_2

(3) F_3 with D_3

(4) F_4 with X_1, X_2, D_1, D_2

(5) F_5 with X_3

(6) F_6 with D_4 X_4

(7) I_1 and F_7 with X_5, X_6, X_7, X_8

(8) I_1 with X_9, X_{10}, X_5, X_{11}, X_6, X_7, X_8

(9) I_2 with D_5, X_9, X_{10}, X_5, X_{11}, X_6, X_7, X_8, D_6

(10) I_3 and F_8 with D_7, X_{12}, X_{13}, X_{14}

(11) I_4 with D_8, D_9

(12) F_9 with X_{21}, X_2, X_{20}, X_{18}, X_{19}, X_{17}, X_{15}, X_{16}

(13) I_5 and F_9 with D_{10}

By applying engineering judgment to the likelihood of the occurrence of both a basic failure mode and an ignition source as discussed previously, events within each listing can be ranked from most to least likely as follows:

(1) I_1 in combination with X_5, X_6, X_7, X_8, X_9, X_{10}, X_{11}

(2) I_2 in combination with X_5, X_6, X_7, X_8, X_9, X_{10}, X_{11}, D_5, D_6

(3) I_4 in combination with D_8, D_9

(4) F_9 in combination with X_{19}, X_{17}, X_{21}, X_{18}, X_{10}, X_2, X_{20}, X_{16}, X_{15}

(5) F_4 in combination with X_1, X_2, D_1, D_2

(6) F_1 in combination with D_1

(7) F_2 in combination with D_2

(8) F_6 in combination with X_4, D_4

(9) F_5 in combination with X_3

(10) F_3 in combination with D_3

(11) $I_1 \cdot F_7$ in combination with X_5, X_6, X_7, X_8

(12) $I_3 \cdot F_8$ in combination with X_{14}, X_{13}, X_{12}, D_7

(13) $F_9 \cdot I_5$ in combination with D_{10}

Further evaluation of the significance of these events would include consideration of the mode of their occurrence. An internal event may be undesirable, but because it occurs internally to the system and limits damage only to hardware, it may be judged less significant. An event that occurs externally to the system and may involve injury to personnel may be considered very significant and be submitted to a much more rigorous evaluation.

DISCUSSION and RECOMMENDATIONS

The P-40 Stirling engines installed in AMC vehicles are almost identical to the P-40 engine used to power the Opel Rekord as described in MTI topical report (Ref. 1). From this analysis and the experience with P-40 Stirling engines the following conclusions were drawn:

- The P-40 engine is not prone to structural catastrophic failures even when it is enduring drastic changes of operating conditions or component malfunction.

- The engine functions are closely monitored by strategically located sensors.

- The electronic control unit is designed to interpret loss of any sensor signal as a command for a normal shutdown.

- The check valves used in the initial versions of the P-40 engines have failed due to breakage of spring, disk retaining cages and O-rings. Recently, United Stirling of Sweden redesigned the check valves, and limited experience indicates that such failures are less likely to occur.

- The hazards of hydrogen fire or detonation cannot be overemphasized and are described in numerous publications such as reference 8. The inherent danger of fire is much greater when the engine is running and the engine compartment hood is raised to facilitate engine inspection during public demonstrations. To minimize the risk of hydrogen fire injury to the observers, an interlock between the engine compartment hood and the ignition key in the passenger compartment has been installed in the demon-

stration vehicles. This interlock prohibits engine operation with the hood raised. However, it must be pointed out that the lockout can be circumvented while performing engine maintenance. Thus, in public demonstrations of the vehicle the operator must strictly adhere to the prescribed operating procedure.

Installation of the hydrogen storage bottle and supply line unprotected from the environment in the left front wheel well of the vehicles is very poor

a. Because the storage bottle, fitting, and supply line are subjected to corrosion and possible impact damage from road debris. The fitting and supply line are especially vulnerable and are thus highly prone to catastrophic failure. The environment to which these components are exposed enhances the risk of catastrophic structural failure.

b. Because failure of the straps anchoring the storage bottle would cause the bottle to drop and most certainly rupture the high-pressure supply line, causing sudden discharge of high-pressure gaseous hydrogen. The escaping hydrogen can be ignited or detonated by a spark or by heat generated by rupture.

c. In case of collision the structural integrity of the mounts and the storage bottle itself may be compromised, but most likely the structural integrity of the fitting and the high-pressure line would be compromised, leading to a rapid release of the storage bottle content.

Experience to date with the hydrogen storage bottle and their structural characteristics appear to be very favorable. The hydrogen storage bottle at 15^{0} C and 300-atm pressure has a bottle wall stress of 77 ksi. On the basis of yield strength of 140 ksi, a safety factor of 1.8 exists. On the basis of proof pressure of 450 atm and the resulting 116-ksi stress in the bottle wall, a safety factor of 1.2 is still provided. These factors were verified by Lewis in a single rupture test of the Opel Rekord hydrogen storage bottle after about 18 months of continuous use in the vehicle.

Stanford Research Institute (SRI), sponsored by the Ford Motor Co., in 1973 and 1976 conducted an independent study of hydrogen safety of Stirling engines (refs. 6 and 7). Although the quantities of hydrogen gas used in SRI tests may not be the same as that used in the P-40 engine, the behavior of hydrogen-air mixtures, their ignition and detonation characteristics, and damage to the hardware experienced with P-40 engines parallels closely the observations by SRI. The SRI studies (refs. 6 and 7) clearly state that

. Hydrogen fires within the engine proper in many cases may be considered nonhazardous.

. Significant hazard of fire or explosion occurs only as a result of a very rapid release of gaseous hydrogen.

. Occurrence of fire or explosion for such a massive hydrogen release depends entirely on the timing and location of ignition sources.

. With a standard hood significant explosive effects were limited to tests with the ignition source under the hood. Maximum pressure of 4.58 psi was recorded outside the vehicle.

. With a louvered hood somewhat lower maximum shock overpressures were observed for ignition beneath the hood.

Although the quantity of hydrogen used in the Stirling cycle is considerably (possibly 2000 times) less than the quantity of gasoline, the following is still recommended for the Stirling engine vehicles:

. To minimize ignition sources under the hood, no electrical component should be capable of igniting the gas mixture surrounding the equipment.

. The hydrogen storage bottle should be caged, possibly with antishrapnel net, and anchored so that it does not propel into the passenger compartment or outside vehicle envelope in case of catastrophic failure of the fitting.

. For hydrogen bottle installations in vehicle wheel wells the hard supply line should be replaced with a suitable flexible line and caged to protect it from road debris impact.

. Smoking in the passenger compartment or in the immediate vicinity of the demonstration vehicle should not be allowed.

. Vehicle demonstration rides should be limited to closely controlled, sparsely traveled traffic areas. This recommendation might be withdrawn if the behavior of the vehicle during involvement in an accident is clearly defined and the recommendations on the storage bottle and supply line are implemented.

. The operator should brief the passengers on how to quickly exit from the demonstration vehicle in case an emergency arises.

. The contractor should generate maintenance procedures for the Stirling engine and ensure that these procedures are not violated.

In the future it is advisable that the following actions be taken:

. Perform detailed system safety analysis using the fault tree technique, failure modes and effects analysis, or other appropriate techniques of all new designs (Mod-1, Mod-2, reference engine) and any design modifications. These studies should be continuously updated and form the basis for hardware manufacture and buildup and maintenance and operation, inspection, and acceptance procedures. This is to be accomplished by personnel capable and experienced in system safety analysis.

. Perform suitable system safety analyses of the existing hardware modifications prior to accomplishing them.

. Investigate the feasibility of using metal-lined, fiberglass-filament-wound bottles for storage of the gaseous hydrogen. Lewis has been investigating use of such bottles for a variety of applications and has accumulated a wealth of

useful data. In addition, use of such bottles would minimize shrapnel in the event of catastrophic structural failure.

. Design the shape of the storage bottle and locate it in the vehicle envelope such that in the event of catastrophic failure of the fitting the bottle, if propelled, would be ejected downward into the shrapnel retaining net or in the worst case into the pavement within the vehicle envelope but not near the passenger compartment.

. Eliminate all possible fittings, connections, or external hydrogen supply lines that surround the current P-40 engines.

. Investigate the possibility of odorizing the hydrogen gas used in the Stirling cycle. This will alert persons handling Stirling-engine-powered vehicles of potential hydrogen gas problems in a manner that gasoline or fuel odor alerts us in present internal combustion engine cars.

. Determine the immediate and induced effects exerted on the Stirling-engine-powered vehicle system by a wide range of catastrophic collision energies.

The aforementioned potential problems are real and cannot be treated lightly. They have been experienced with P-40 engines and were also independently evaluated for SRI tests under highly controlled conditions. From experience it is evident that the P-40 engine is structurally capable of powering an automobile. Hydrogen leakages internal to the engine do not seem to present serious danger to hardware, facilities, or personnel. Hydrogen leakage external to the engine does present a certain amount of hazard to hardware and more of a hazard to personnel. The hazard to hardware on the basis of experience to date is minimal and quite acceptable. The hazard to personnel is difficult to accurately assess, in general, and therefore, preliminary qualitative system safety considerations obviously can only be approximated.

The analysis presented in this report covers only one facet of the total Stirling engine system. In addition to hydrogen-failure-mode fault tree analysis, similar analyses are necessary on such subsystems as the pressurized cooling jacket, electronic circuitry, and power control valves. Fault tree analysis combined with failure modes and effects analysis and failure rate data can provide a proper reliability assessment of the Stirling engine system.

The primary challenge for the designer of automotive Stirling engines is the production of a reliable, environmentally acceptable operational engine system that meets the program objectives. In meeting this challenge, the designer is faced with multiple design requirements that must be satisfied during the design process. In view of the potential safety problems that can be presented by hydrogen used as the working gas and the electronic control systems and multiplicity of acceptable practices as perceived by the team members implementing the program, the designer must be keenly aware of the importance of system safety. From the outset of the program the designer must address, in a formal and disciplined way, the issues associated with safety of hardware, safety of the environment, and above all safety of the public. The DOE-NASA Stirling Engine Project Office has required that contractors make safety considerations an integral part of all phases of the Stirling engine development program. As an integral part of each engine design subtask, analyses are being evolved to determine possible modes of failure. The accepted system safety analysis techniques (fault tree, FMEA, hazards analysis, etc.)

are being applied in various degrees of extent at the system, subsystem, and component levels. The primary objectives are to identify critical failure areas, to enable removal of susceptibility to such failures or their effects from the system, and to minimize risk.

Even though the design and concept verification is in its infancy, applying system safety techniques has already resulted in successfully identifying areas of concern. Subsequent reevaluation of design yielded changes improving the hardware and defined procedures assuring personnel safety. These analyses will be updated as the development program progresses.

REFERENCES

1. "Topical Report: Pre-Developmental Demonstration of a Stirling Powered Vehicle, Genesis-1 (The P-40/Opel.)," Mechanical Technology, Inc., Latham, NY, Report No. 79ASE33T01, January 15, 1979.

2. "Equipment Failure Report: P-40 No. 5 in the Opel," Mechanical Technology, Inc., Latham, NY, Report No. 78ASE22PA2, August 14, 1978.

3. "Equipment Failure Report: P-40 No. 5 in the Opel," Mechancial Technology, Inc., Latham, NY, Report No. 79ASE50PA4, March 5, 1979.

4. "Equipment Failure Report: P-40 No. 8 for the Spirit Vehicle," Mechanical Technology, Inc., Latham, NY, Report No. 79ASE64PA5, May 5, 1979.

5. "Equipment Failure Report: P-40 No. 8 for the Spirit Vehicle," Mechanical Technology, Inc., Latham, NY, Report Pending.

6. "Hydrogen Safety Tests of the Stirling Engine," T. C. Goodale, Stanford Research Institute, Menlo Park, CA, Report Project PYC-2696, December 1973.

7. "Hydrogen Safety Tests of the Stirling Engine - II," T. C. Goodale and D. Walter, Stanford Research Institute, Menlo Park, CA, Report Project PYC-2696, September 1976.

8. "Handling Hazardous Materials," D. R. Cloyd and W. J. Murphy, eds., NASA SP-5032, September 1965.

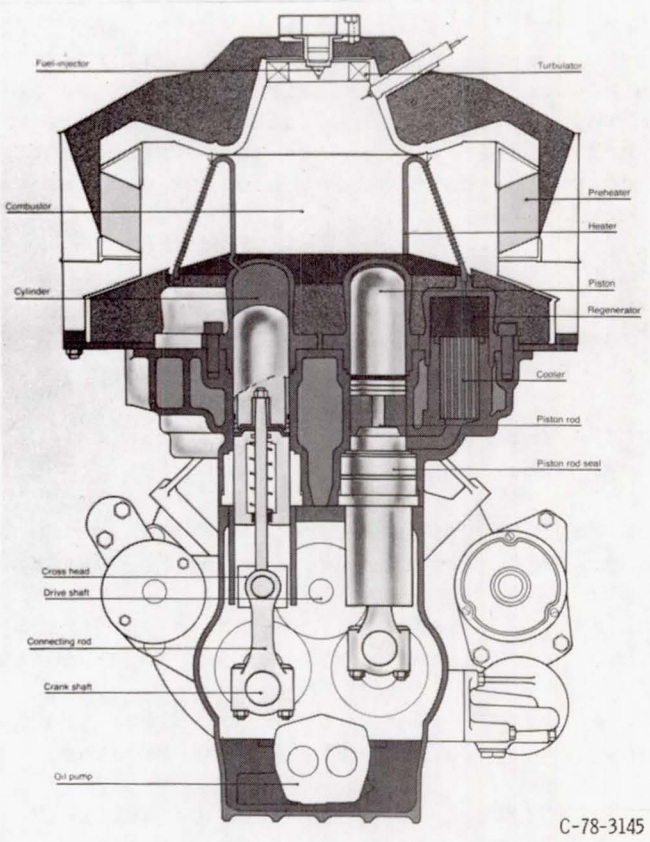


Figure 1. - Cross-sectional schematic of P-40 Stirling engine.

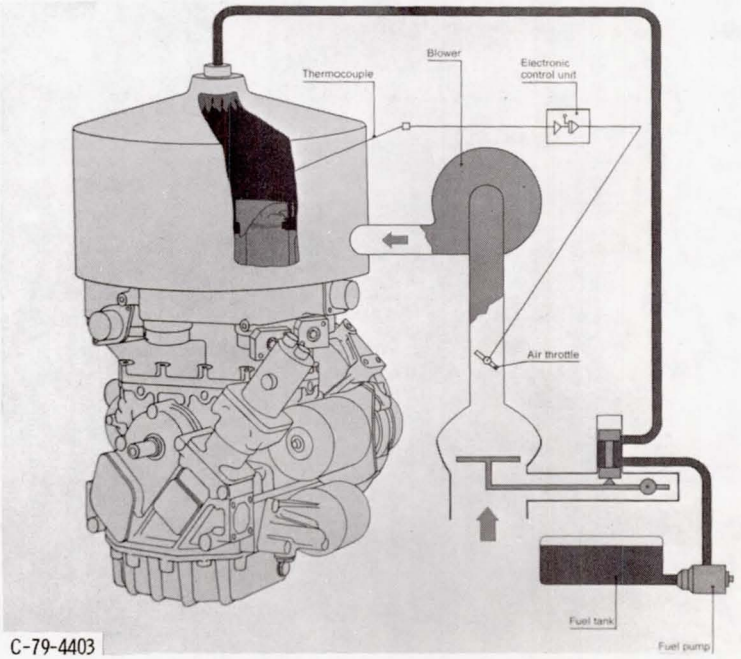


Figure 2. - Schematic of Stirling engine combustor and air-fuel control system.

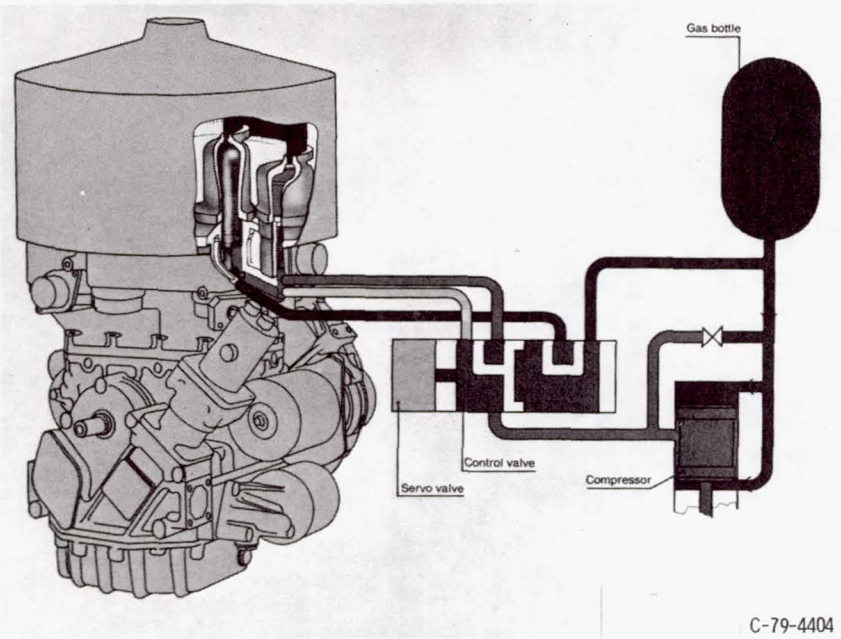
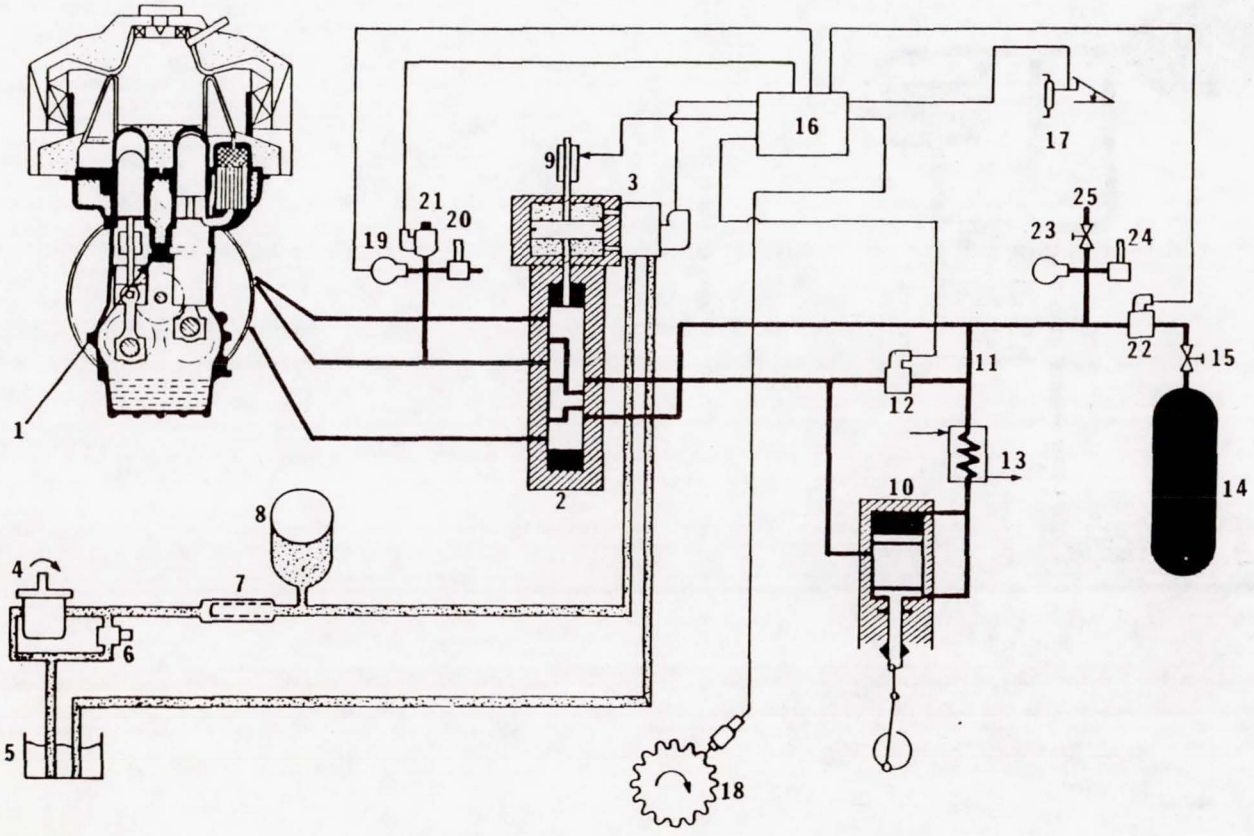


Figure 3. - Schematic of Stirling engine power control system.



1 TIMED SUPPLY SYSTEM
2 SUPPLY, DUMP AND SHORT-CIRCUIT VALVE BLOCK
3 MOOG ELECTRO-HYDRAULIC SERVOVALVE
4 OIL PUMP
5 OIL TANK
6 RELIEF VALVE (CONSTANT PRESSURE VALVE)
7 OIL FILTER
8 NITROGEN FILLED ACCUMULATOR
9 FEEDBACK POTENTIOMETER
10 HYDROGEN COMPRESSOR
11 CHECK VALVES
12 COMPRESSOR SHORT-CIRCUIT VALVE
13 GAS COOLER
14 HYDROGEN STORAGE VESSEL
15 SHUTOFF VALVE
16 ELECTRONIC CONTROL UNIT
17 ACCELERATOR WITH POTENTIOMETER
18 SPEED TRANSDUCER
19 PRESSURE TRANSDUCER (MAXIMUM PRESSURE)
20 SAFETY VALVE (MAXIMUM PRESSURE)
21 EMERGENCY VALVE AND EXTERNAL DUMPING VALVE
22 EMERGENCY VALVE
23 PRESSURE TRANSDUCER (TANK PRESSURE)
24 SAFETY VALVE (TANK PRESSURE)
25 GAS REFILLING VALVE

Figure 4. - Detailed schematic of Stirling engine power control system.

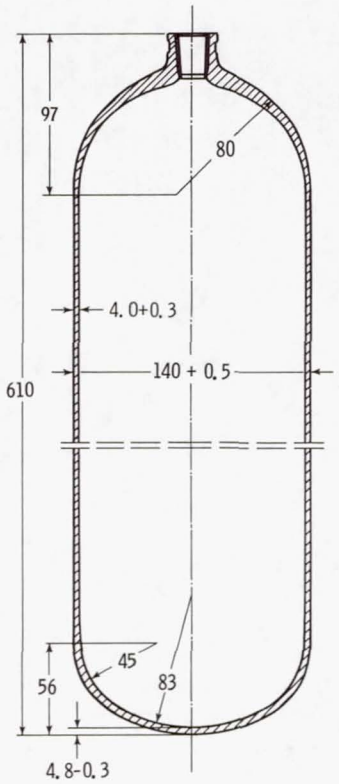


Figure 5. - Hydrogen storage bottle. Capacity, 7.0 to 7.3 liters; operating pressure, 300 atm; proof pressure, 450 atm. (Dimensions are in centimeters.)

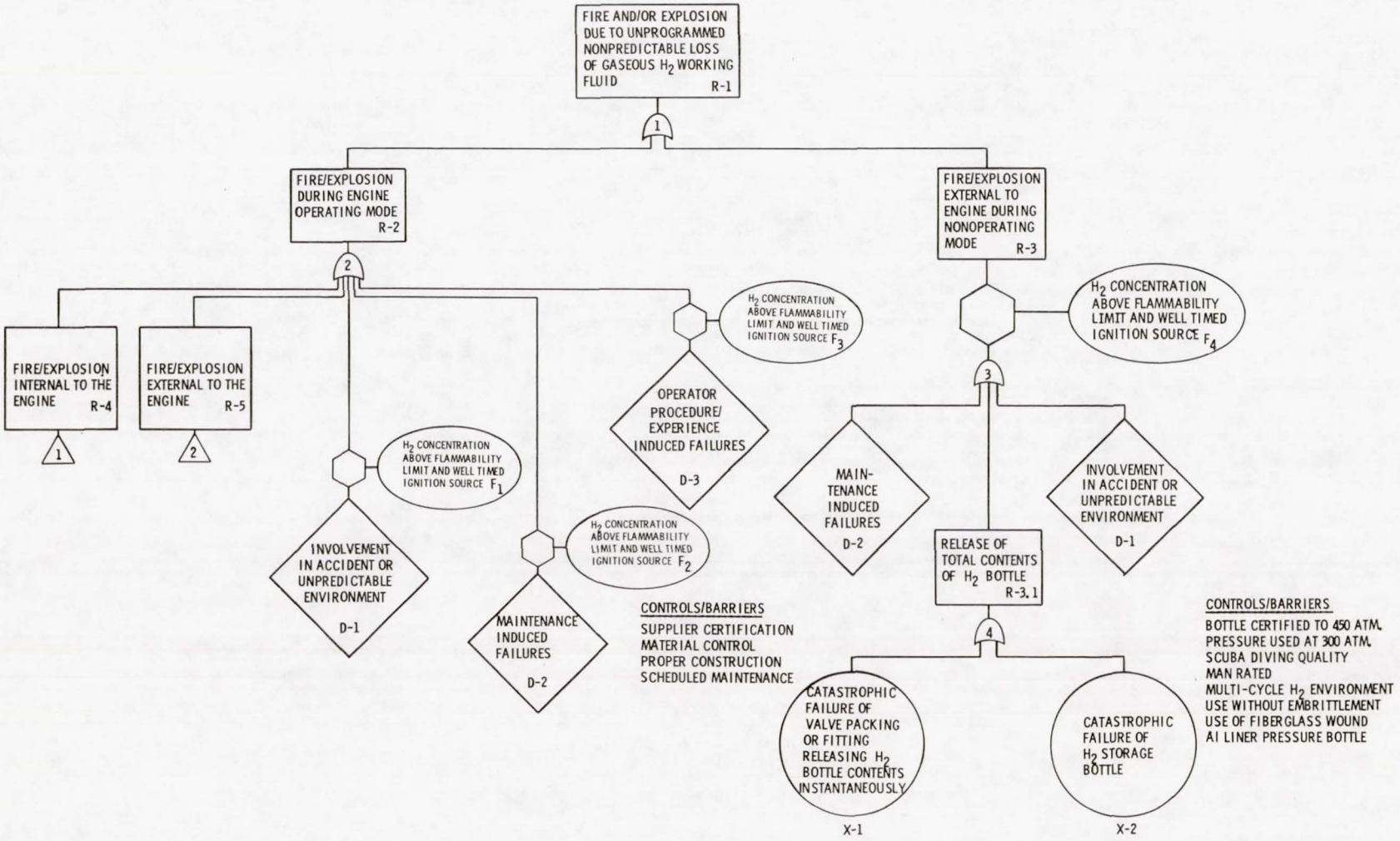


Figure 6. - Fault tree logic display.

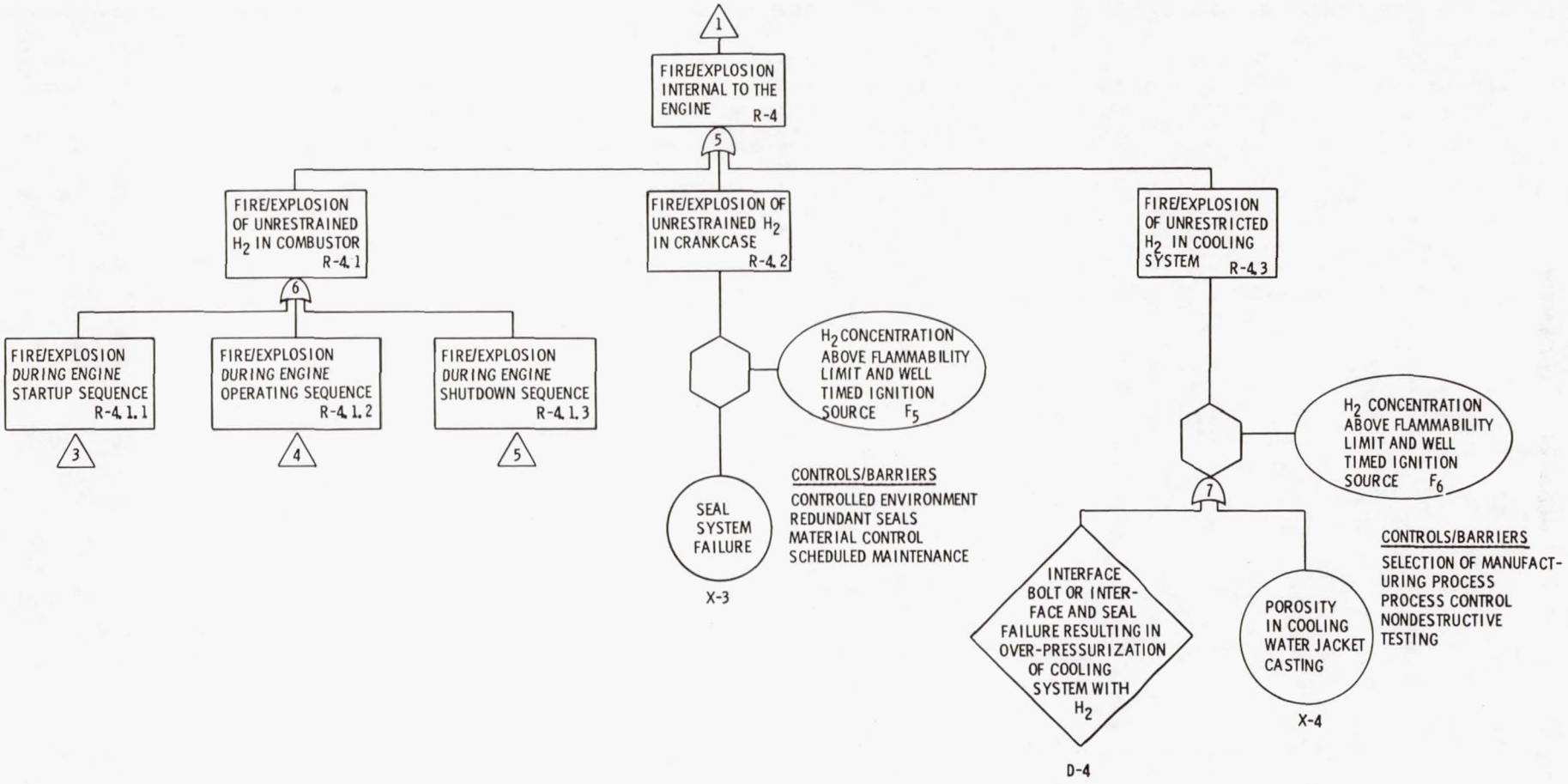


Figure 6. - Continued.

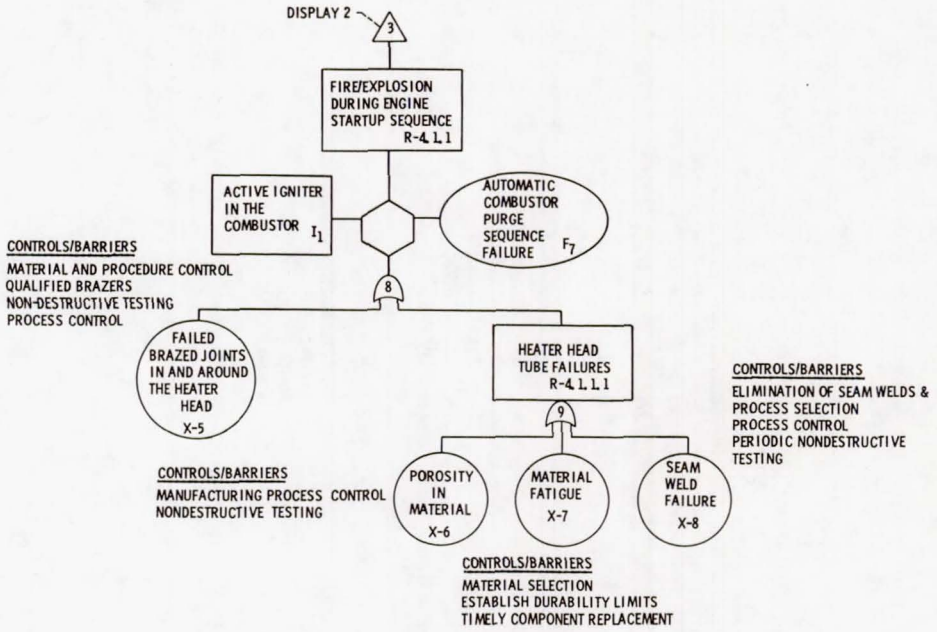


Figure 6. - Continued.

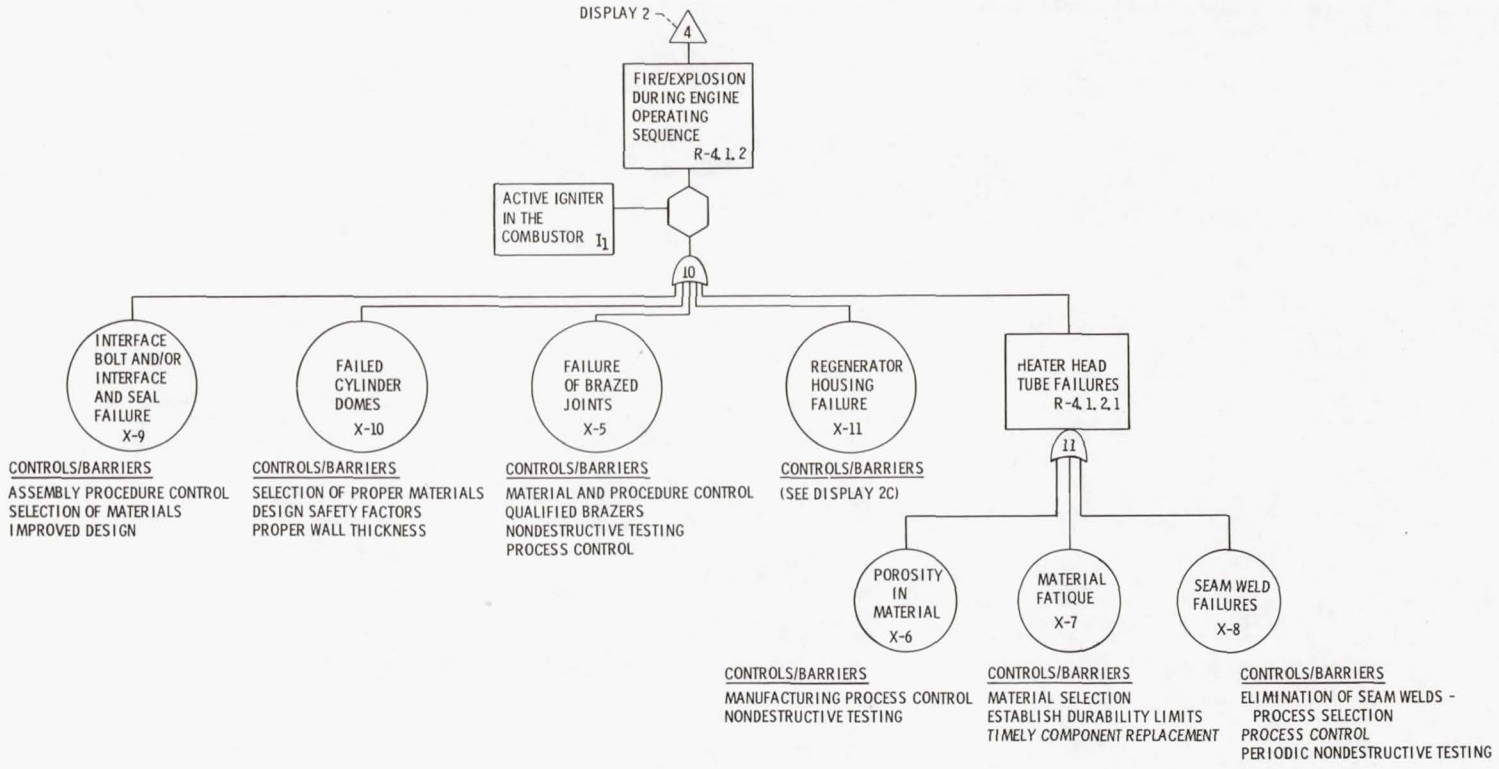


Figure 6. - Continued.

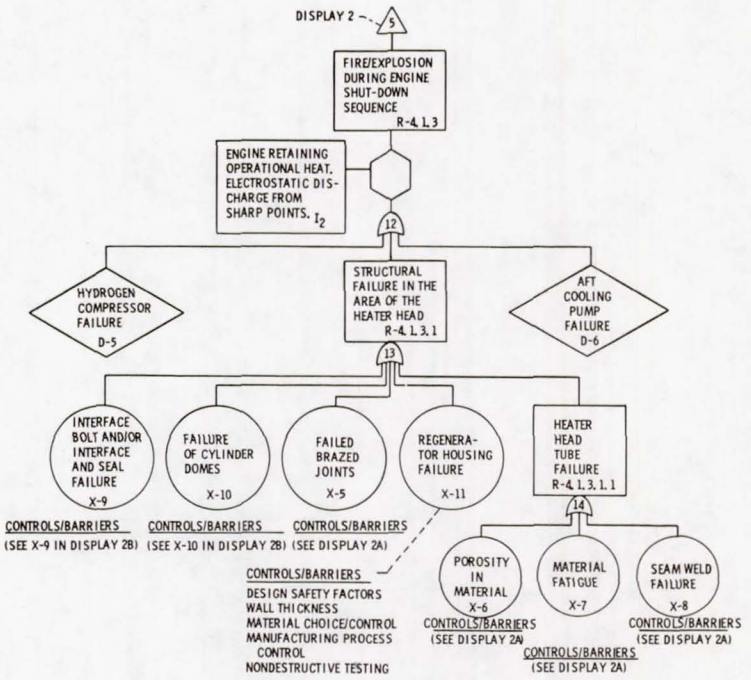


Figure 6. - Continued.

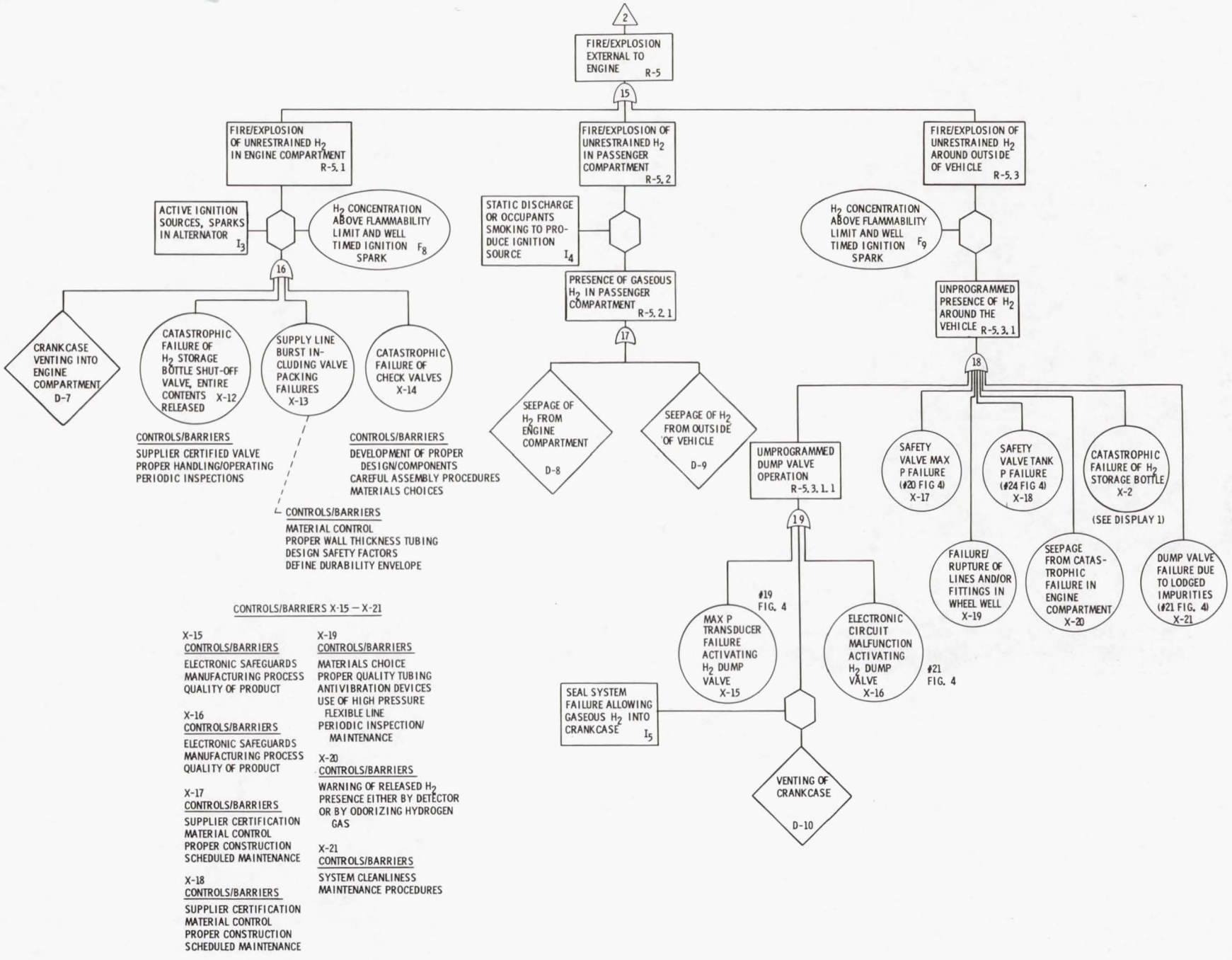


Figure 6. - Concluded.

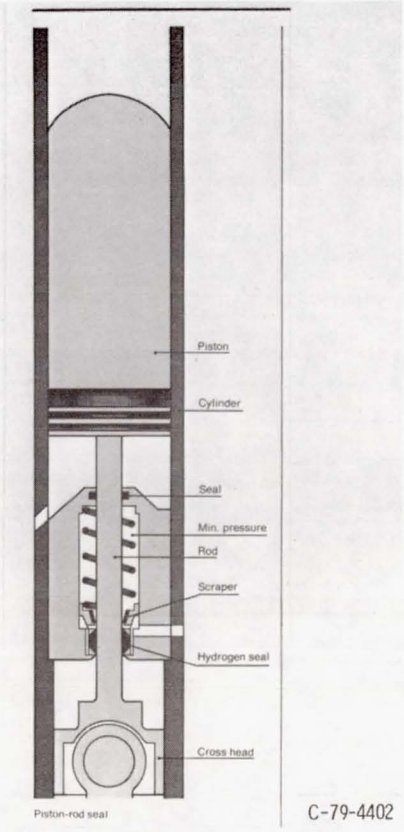


Figure 7. - Schematic of Stirling engine piston rod seal.

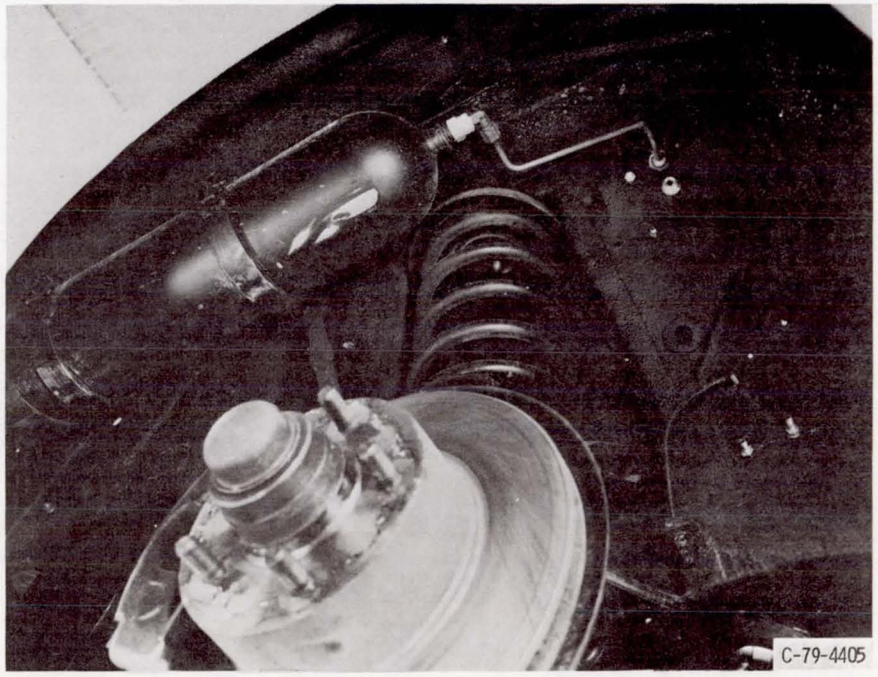


Figure 8. - Hydrogen bottle mounted in AMC Spirit wheel well.

1. Report No. NASA TM-82615	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle SYSTEM SAFETY IN STIRLING ENGINE DEVELOPMENT		5. Report Date 6. Performing Organization Code 778-35-03
7. Author(s) H. Bankaitis		8. Performing Organization Report No. E-867 10. Work Unit No.
9. Performing Organization Name and Address National Aeronautics and Space Administration Lewis Research Center Cleveland, Ohio 44135		11. Contract or Grant No. 13. Type of Report and Period Covered Technical Memorandum
12. Sponsoring Agency Name and Address U.S. Department of Energy Office of Transportation Programs Washington, D.C. 20545		14. Sponsoring Agency ~~Code~~ Report No. DOE/NASA/51040-25

15. Supplementary Notes

Prepared under Interagency Agreement DE-AI01-77CS51040. Prepared for Fifth International System Safety Conference, Denver, Colorado, July 26-31, 1981.

16. Abstract

The Department of Energy has established a number of broad programs aimed at reducing highway fuel consumption. One of the programs addresses the Stirling engine propulsion system as a possible alternative to the conventional spark-ignition engine. The objective of this program is the development, by 1984, of a Stirling engine system having at least 30 percent improvement in fuel economy (mpg) over production vehicles powered by conventional spark-ignition engines of the same weight and performance, based on equal BTU content of fuel used. The DOE/NASA Stirling Engine Project Office has required that contractors make safety considerations an integral part of all phases of the Stirling engine development program. As an integral part of each engine design subtask, analyses are being evolved to determine possible modes of failure. The accepted system safety analysis techniques (Fault Tree, FMEA, Hazards Analysis, etc.) are being applied in various degrees of extent at the system, subsystem and component levels. The primary objectives are to identify critical failure areas, to enable removal of susceptibility to such failures or their effects from the system and to minimize risk.

17. Key Words (Suggested by Author(s))	18. Distribution Statement
Automotive Stirling engine System safety	Unclassified - unlimited STAR Category 85 DOE Category UC-96

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price*
Unclassified	Unclassified		

* For sale by the National Technical Information Service, Springfield, Virginia 22161