SUPPORT SYSTEMS DESIGN AND ANALYSIS

Robert M. Ferguson*
DL-NED-2
NASA, Kennedy Space Center

ABSTRACT

The integration of KSC ground support systems with the new Launch Processing System and new Launch Vehicle provided KSC with a unique challenge in system design and analysis for STS. Approximately 70 support systems were to be controlled and monitored by the Launch Processing System. Typical systems are Main Propulsion Oxygen and Hydrogen loading systems, Environmental Control Life Support system, Hydraulics, etc. An "End-to-End" concept of documentation and analysis was chosen and applied to these systems.

Unique problems were resolved in the areas of software analysis, safing under emergency conditions, sampling rates, and control loop analysis. New methods of performing "End-to-End" reliability analyses were implemented. This paper discusses the systems design approach selected and the resolution of major problem areas.

KSC SYSTEMS PROBLEM IN SHUTTLE ACTIVATION

The integration of ground support systems with the new sophisticated Launch Processing System (LPS) presented KSC with a unique challenge in system design and analysis for STS.

It was the intent that the LPS would be used to control and monitor approximately 70 support systems. An applications software set would be developed for each system. Examples of these systems are: Fuel Cell Servicing System, Hypergol Loading System, Main Propulsion Oxygen and Hydrogen Loading systems, Environmental Control System, Orbiter/SRB (Solid Rocket Booster) Hydraulics, Environmental Control Life Support, etc. The challenge was to develop methods to document, define software requirements, and assure a "fail safe" design for these systems.

A system usually consists of many components which have been designed by KSC and other NASA Centers. A multitude of different design disciplines are involved. (See Figure 1). There existed a need to tie these diverse elements together in a systematic manner to define an end-to-end system.

THE SYSTEM DESIGN APPROACH SELECTED

In reviewing existing KSC design, documentation and reliability analysis procedures at the time, it became apparent that new and innovative approaches were needed to design, document and analyze software controlled systems. The system design approach was to bring together some quality engineering talent who were familiar with total system requirements and assign them the job to integrate fluids, electrical, LPS, controls, and sensor designs into an end-to-end system design. The design process selected is shown in Figure 2. Some of the unique elements in this process are the SMS/EMCD (System Mechanical Schematic/Electro-Mechanical Control Diagram), and the Operating Criteria. The SMS/EMCD (see Figure 3) was developed as a new drawing to aid designers, operators, and application software programmers, to understand a system end-to-end. The SMS/EMCD depicted a system from the GSE thru the Orbiter/SRB/ET (External Tank) showing those elements on board the vehicle that function as part of Ground System Operation. In addition, the SMS/EMCD showed all commands and monitors with their function designators to aid the system software programmers. The Operating Criteria explains the step by step operation of a system; for instance, in Main Propulsion Lox, these are such things as set-ups, chill down, slow fill, fast fill, topping, and replenish. This document had been used previously by KSC, but it was expanded to provide additional information for the software programmer. As an example, a section was added to satisfy control logic software interlocks. The intent was that with the SMS/EMCD, Operating Criteria, and Electrical Schematic systems operating personnel would have all information needed to develop software flow diagrams, and code the application software. Referring to Figure 2, many other documents are needed, but the key documents are the SMS/EMCD, Operating Criteria, and Electrical Schematic. With this documentation it is also possible to provide an end-to-end system assurance analysis which will be addressed later. To implement the system design process at Kennedy, System Integration teams were formed consisting of designers, operators, safety, and reliability personnel. The teams met on a regular basis to review and assure that all necessary requirements were incorporated into the system design.

*Chief, Systems Design Branch

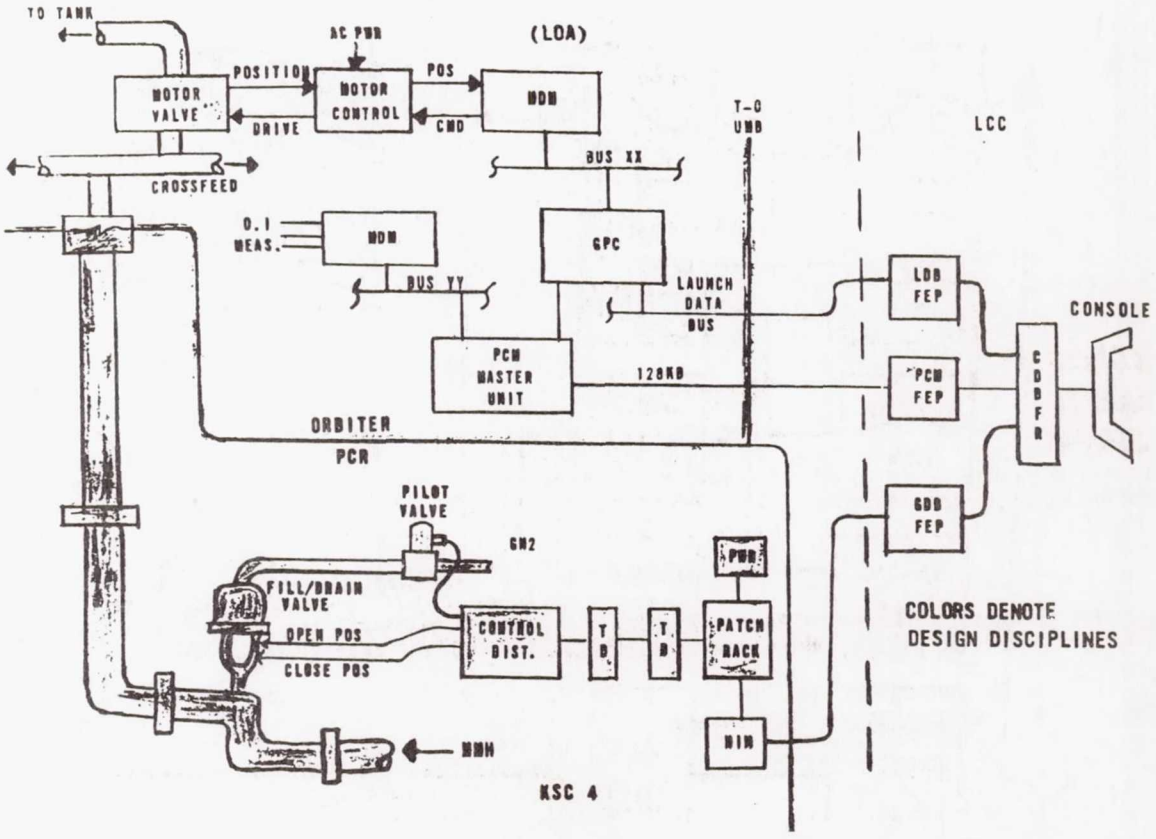


Figure 1.- Typical valve control/monitor.

SPECIAL PROBLEMS

Software would have to be analyzed to satisfy an end-to-end system assurance analysis. The amount of software and changes to software would be of such a tremendous quantity that it would be impossible to analyze the software and maintain the analysis current. To circumvent this problem, it was decided that critical interlocks would be placed in the control logic portion of the application software set (See Figure 4). By doing this, the amount of software to be analyzed would be highly restricted, making it practical to perform a software analysis. The objective achieved was to place GOAL applications programs under Operations control and Control Logic programs under Design control. Criterias were structured so that each system control logic requirement was spelled out. To analyze these hazardous situations the requirements were stated in the Operating Criteria and the implementing software was written in control logic, making it relatively easy to perform a software analysis.

Emergency Safing took on a new meaning when coupled with the new LPS. While the LPS was designed to have a standby console, it would take approximately 15 or 20 minutes to bring the redundant console on line and, if a hazardous propellant loading were in process at the time, the vehicle could be left in a hazardous condition during this transition to another console. Another example is a failure mode in the LPS common data buffer which stops processing of all LPS information. To circumvent these situations and others of this nature, an emergency hardwire safing system was implemented. This system bypasses the LPS system from a control panel located in each LPS console which is used to place the system in a safe condition until the LPS has regained control (see Figure 5). For example, in Main Propulsion Lox, if an LPS failure occurs, the integration console assumes the safing function; if the integration console has also failed, the Emergency Safing system commands the pumps to stop, opens the vehicle vent valves, and leaves the system in a safe stand by condition. Further, if the problem were of an extreme nature, the Emergency Safing system can be used to drain liquid oxygen and liquid hydrogen from the vehicle. Systems other than MPS, LOX and LH2 (such as Hypergols, Fuel Cells, etc.) fail to the Emergency Safing as back-up. Thru STS-6 there has been only one usage of the Emergency Safing System which attests to the reliability of the LPS.

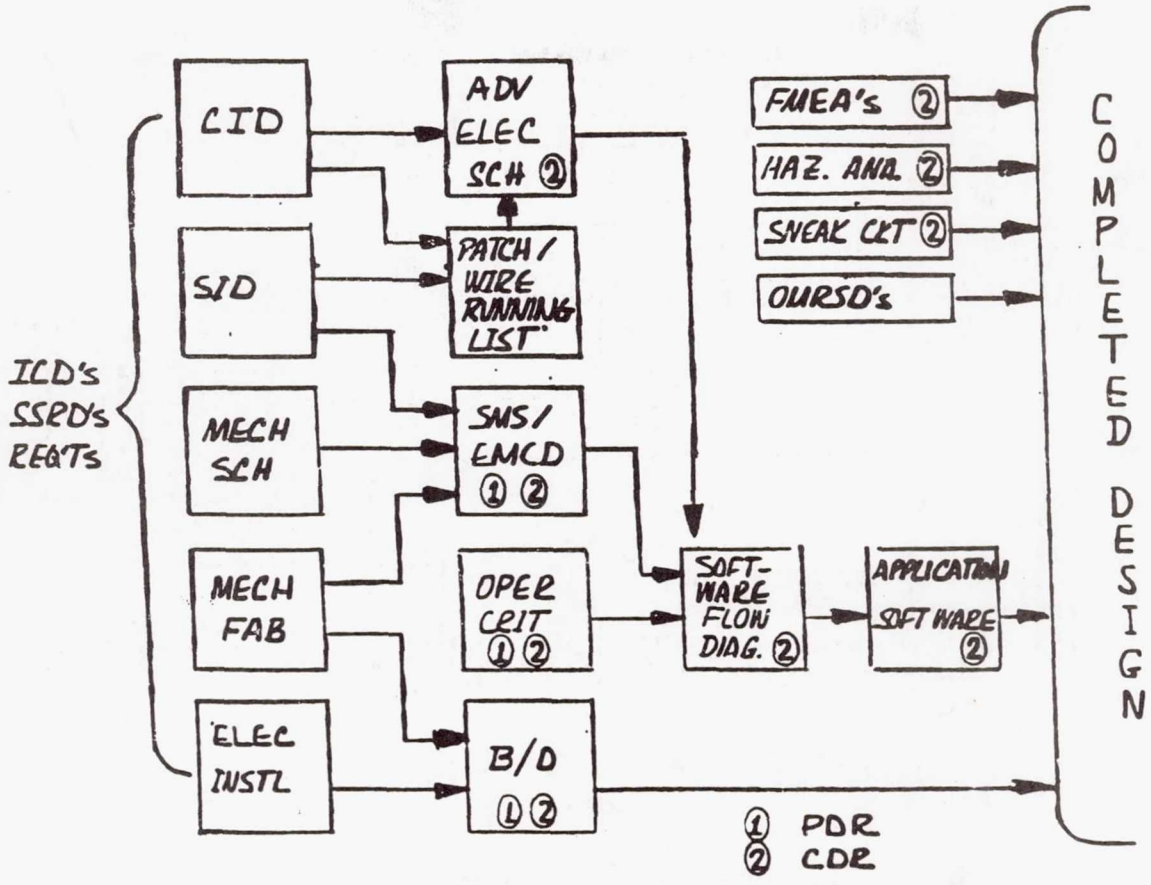


Figure 2.- DE systems design process.

Since sample rate is of prime importance for proper utilization of a computer control system, a basic requirement was levied on designers to use a sampling rate of one sample per second for all commands and monitors, and that higher sampling rates would require special approval. This did not preclude that during an operation the samping rate could be raised at the time a higher sampling rate was required. The sizing of this task is better understood by the fact that 6500 commands and monitors are used in the launch configuration.

Analysis was performed on the control Loops of a higher complexity first; and, then as time allowed, this analysis was extended to less complex situations. As a result of control loop analysis, problems were uncovered on propellant replenish and hypergol loading.

RELIABILITY ANALYSIS

Previously at KSC, reliability analysis had been performed in piece parts. There was a mechanical systems analysis for the Lox system and an electrical systems analysis for the LOX system. In addition, there was a vehicle analysis for the Lox system. These analyses were not tied together end-to-end. The SMS/EMCD was made to depict an end-to-end system with the onboard vehicle components that function as part of the GSE operations. In the KSC System Assurance Analysis four areas (see Figure 6) were analyzed to assure that the analysis was end-to-end: These areas were:

1) The KSC GSE system (electrical/mechanical/electronic).

2) The control logic software.

3) The LPS CCMS hardware and Executive software.

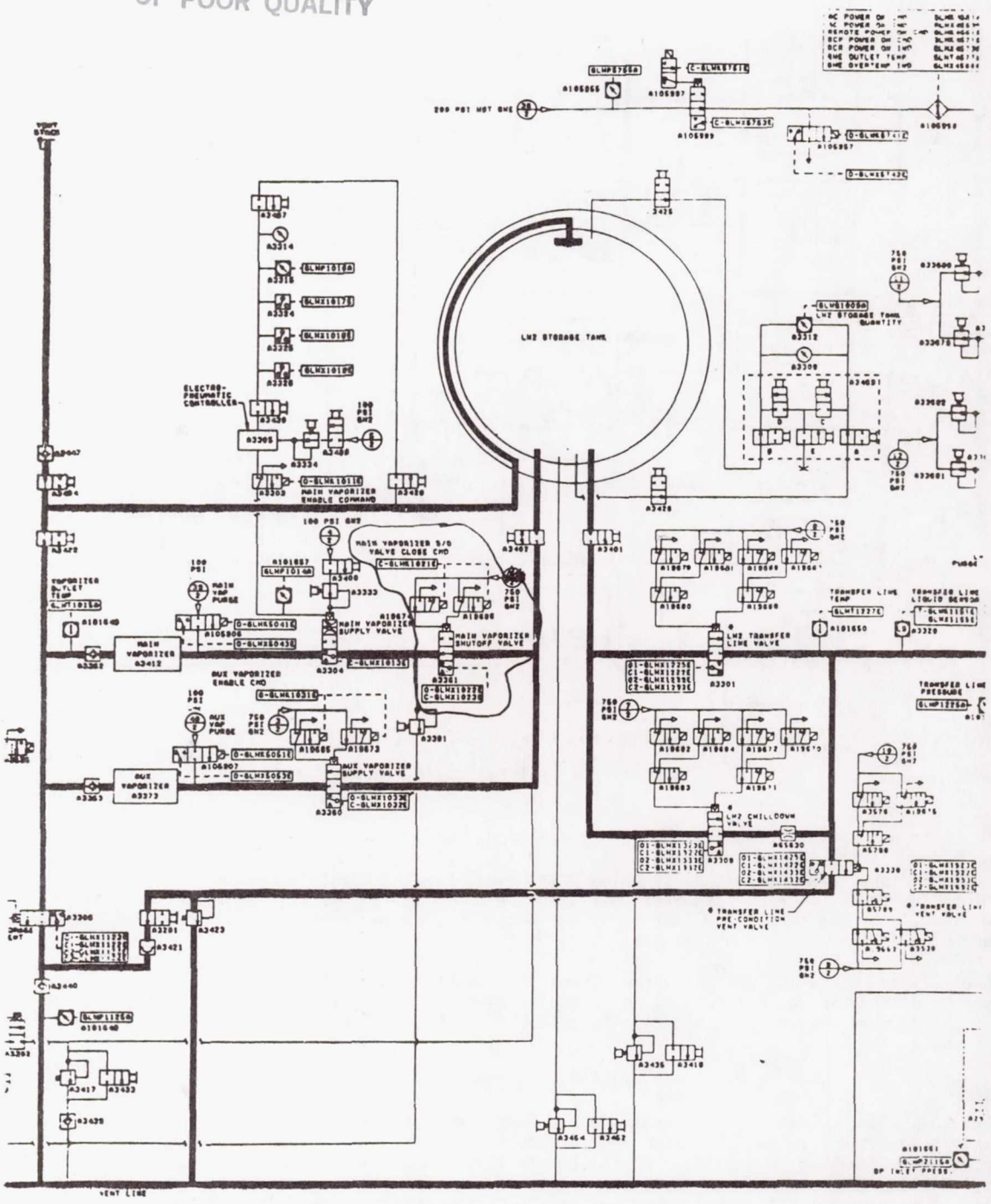


Figure 3-1

4) Other Center Analyses. A review was made of the analyses provided by other Centers of the on board vehicle components. When problems were uncovered in analyses from other Centers, these problems were presented to other Centers as "Items of Concern". Several "Items of Concern" were identified, due to the fact that other Centers used different analyses techniques, and that their analyses addressed the flight configuration instead of the ground servicing configuration. An example of one of these Items of Concern was a failure to the closed position of the LOX Inboard Fill Valve during GSE loading operations. This was not addressed in the Orbiter FMEA (Failure Mode Effect and Analysis). This failure mode was classified hazardous as a result.

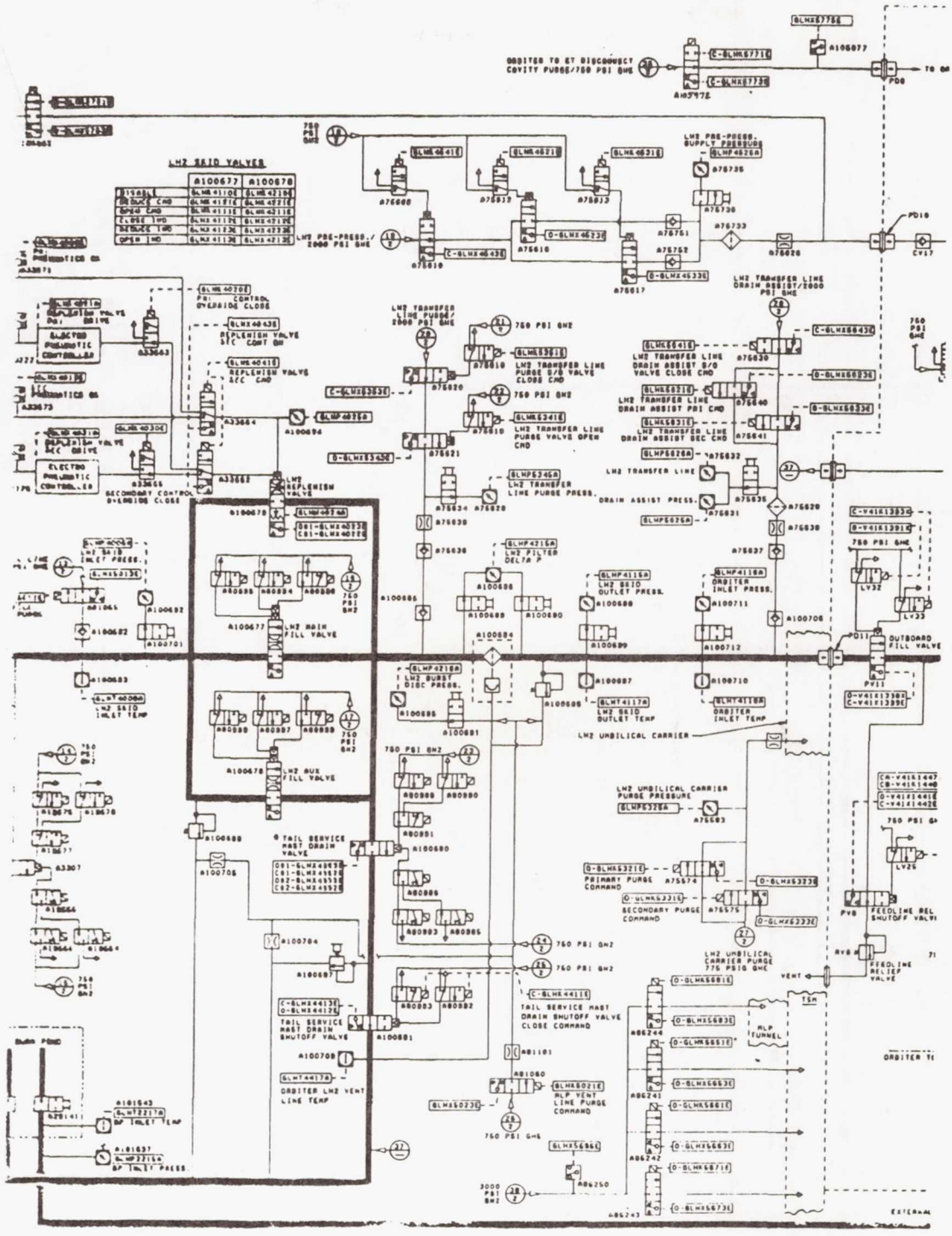


Figure 3-2

The Shuttle program offered many challenges to system designers at KSC. The implementation of the LPS for control contributed to the expansion of the system design function. The methods that have been developed as being refined and applied to such current programs as Centaur and the nuclear power control field. These methods have produced reliable systems for STS and will serve well in the operations era.

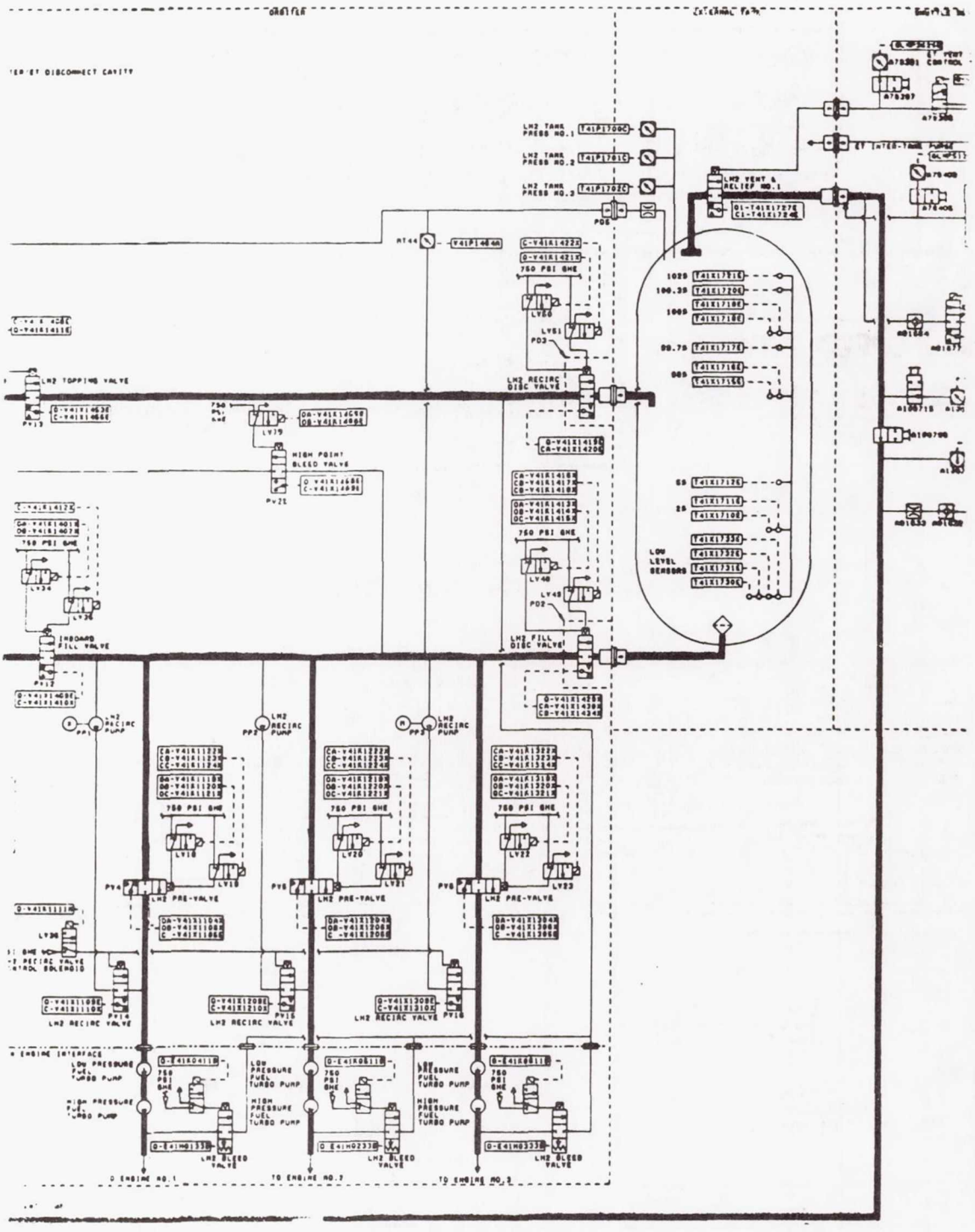


Figure 3-3

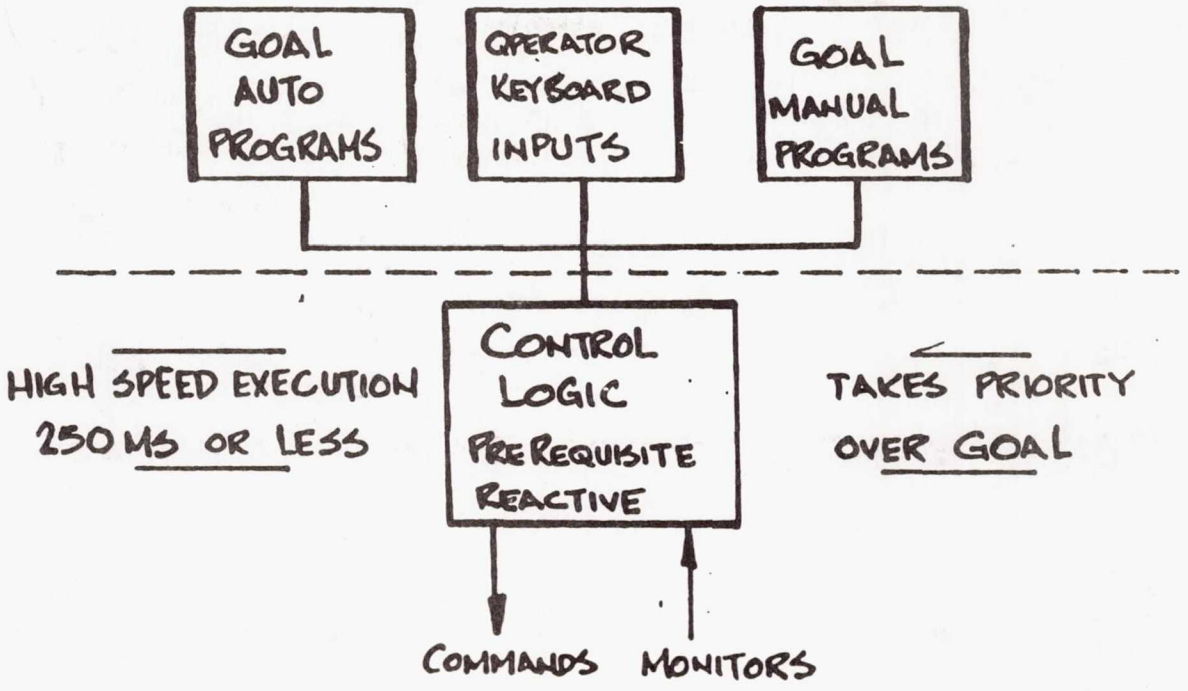


Figure 4

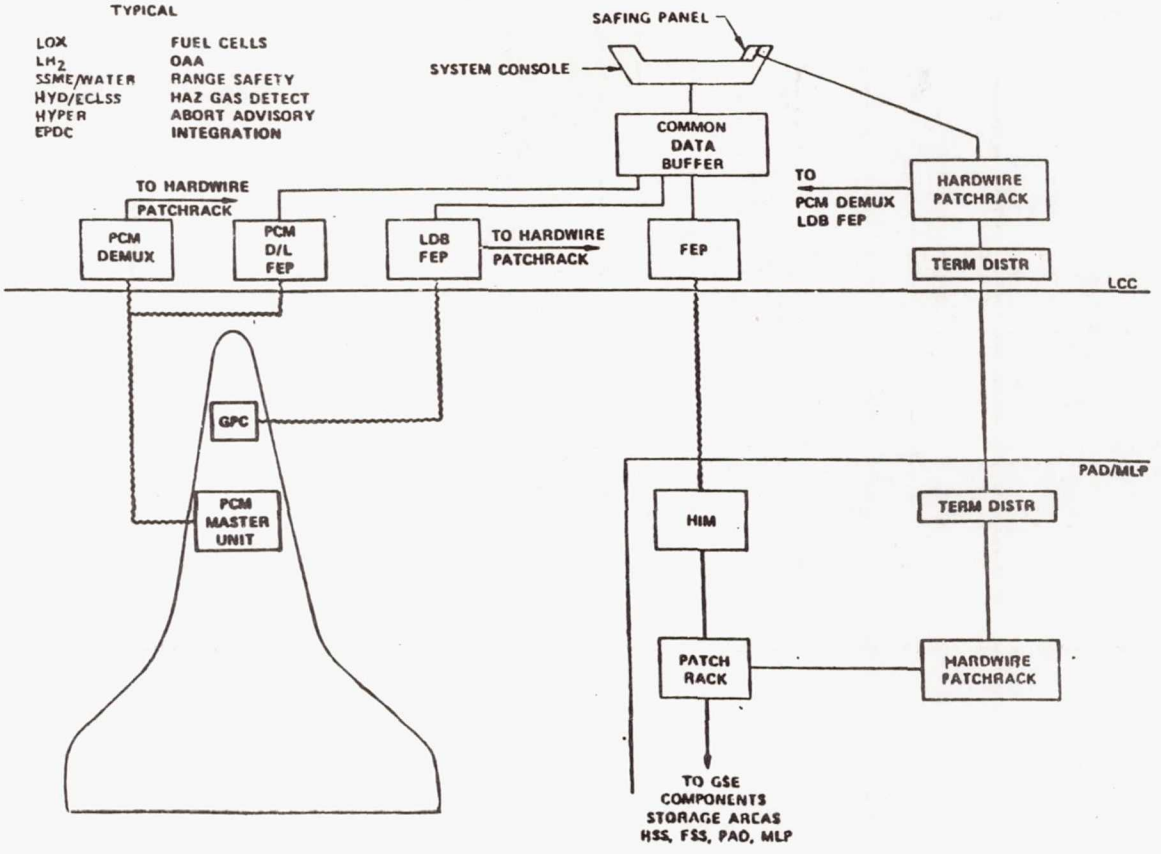
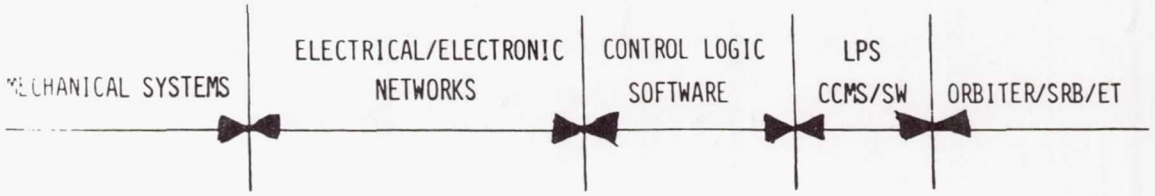


Figure 5.- Emergency safing system.



CATEGORY I HAZARDS -- LOSS OF LIFE/LOSS OF VEHICLE

CATEGORY II HAZARDS -- LOSS/DAMAGE OF VEHICLE SYSTEM

Figure 6.- Reliability analysis.