NASA TECHNICAL NOTE

NASA TN D-5725

C. 1

NASA TN D-5725

A COMPUTERIZED ONBOARD EXPEDITIOUS MONITOR AND MAINTENANCE ANALYST (EMMA) FOR SPACECRAFT SYSTEMS

by Willard W. Anderson, Ralph W. Will, and Kenneth L. Jacobs

Langley Research Center
Langley Station, Hampton, Va.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION • WASHINGTON, D. C. • MAY 1970

1. Report No.
NASA TN D-5725

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle
A COMPUTERIZED ONBOARD EXPEDITIOUS MONITOR AND MAINTENANCE ANALYST (EMMA) FOR SPACECRAFT SYSTEMS

5. Report Date
May 1970

6. Performing Organization Code

7. Author(s)
Willard W. Anderson, Ralph W. Will, and Kenneth L. Jacobs

8. Performing Organization Report No.
L-6973

10. Work Unit No.
965-21-00-01-23

9. Performing Organization Name and Address
NASA Langley Research Center
Hampton, Va. 23365

11. Contract or Grant No.

12. Sponsoring Agency Name and Address
National Aeronautics and Space Administration
Washington, D.C. 20546

13. Type of Report and Period Covered
Technical Note

14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

A computerized monitor and maintenance system for automatic spacecraft system fault isolation and repair is defined. This system is called an expeditious monitor and maintenance analyst (EMMA). Rationale for the requirement of such a system and general criteria for the synthesis of such a system are presented. A simulation of the maintenance system in operation onboard a space station using a CDC 6600 computer programed to operate in real time and linked to a full-scale prototype control moment gyro (CMG) attitude control system is described. A discussion of the performance of the simulated maintenance system and its ability to diagnose correctly and repair CMG system failures is included.

17. Key Words (Suggested by Author(s))
Automatic maintenance
Fault isolation
Onboard checkout

18. Distribution Statement
Unclassified – Unlimited

19. Security Classif. (of this report)
Unclassified

20. Security Classif. (of this page)
Unclassified

21. No. of Pages
38

22. Price*
$3.00

*For sale by the Clearinghouse for Federal Scientific and Technical Information
Springfield, Virginia 22151

A COMPUTERIZED ONBOARD EXPEDITIOUS MONITOR AND MAINTENANCE ANALYST (EMMA) FOR SPACECRAFT SYSTEMS

By Willard W. Anderson, Ralph W. Will,
and Kenneth L. Jacobs
Langley Research Center

SUMMARY

A computerized monitor and maintenance system for automatic spacecraft system fault isolation and repair is defined. This system is called an expeditious monitor and maintenance analyst (EMMA). Rationale for the requirement of such a system and general criteria for the synthesis of such a system are presented. A CDC 6600 computer was used to simulate the maintenance system in operation onboard a space station. The CDC 6600 was programed to operate in real time and linked to a full-scale prototype control moment gyro (CMG) attitude control system. A discussion of the performance of the simulated maintenance system and its ability to diagnose correctly and repair CMG system failures is included.

INTRODUCTION

Future manned spacecraft will be required to perform more complex tasks than present spacecraft and to operate in space for increasingly longer periods of time. Spacecraft systems will accordingly become more complex and of necessity include more components. Program cost considerations will dictate that spacecraft system costs not rise appreciably; therefore, component costs must be decreased.

Given spacecraft systems comprised of larger numbers of components, with the components produced at lower cost, and adding the requirement of longer system operational life, a technology concerned with system, rather than component, reliability must evolve. System reliability through fast automatic replacement of faulty components by "off the shelf" components would be less expensive than insuring high individual component reliability. This technology should consider system maintenance, system status monitoring, system fault diagnosis, and component replacement. The technology should utilize automatic deterministic logic schemes to the extent that the technology is concerned with repetitious events. Man's participation should be minimal if at all; thus the technology is required to utilize machine information processing and decision making with visual display, printed, or vocal information transmittal only when man's involvement is required.

The above concepts were the rationale for the development of a maintenance system, called an expeditious monitor and maintenance analyst (EMMA). The EMMA is comprised of a central unit containing digital processing and memory hardware, input-output and display hardware, and signal switching hardware local to each system being maintained. Advantages afforded by such a maintenance system onboard a large spacecraft include

1. Lower required component reliability and therefore lower cost
2. Extended system operational life, afforded by optimal use of remaining functioning components
3. Fault prediction based on high sensitivity system status signal monitoring
4. Rapid fault isolation and correction
5. Reduced astronaut "housekeeping" complement

Disadvantages include increased complexity and the possibility of computer error. Operator intervention consisting of direct component status signal readout augmented by printout of computer actions taken will permit error override and corrections.

SYMBOLS

$\dot{E}$	rate of energy accumulation
$\{e\}$	effort state vector
$\{f\}$	flow state vector
P	power
P_1	input power
P_2	output power
p	component-failure-prediction probability
$T(\{X\})$	signal-flow-component operator
t, t_0	time (fig. 18)
$\{X\}$	signal-flow-component input vector

x component test input

$\{Y\}$ signal-flow-component output vector

y response to test signal

ϵ performance constraint transducer reading

ϵ_0 transducer boundary

MAINTENANCE SYSTEM DESCRIPTION

Basic maintenance system operational blocks are shown in figure 1. These blocks include a signal converter, digital processing and memory units, control and display units for astronaut participation, and signal switching units, local to each system being maintained. The signal switching units allow signal (information) flow either to or from system components. The converter includes digital-to-analog, analog-to-digital, and discrete closure conversion and input/output equipment for the digital computer processor and the control unit. The memory unit contains system component reference, tolerance, and sampling-time information for the monitor routines; reference information for the diagnostic routines; and schedules for preventive maintenance.

The maintenance system has four main operational modes:

Monitor/Maintenance

Classification/Prediction

Diagnostic

Repair/Replace

Description of these modes of operation requires definition and discussion of the following terms and rationale concerning the spacecraft systems to be maintained.

Monitor/Maintenance

The basic maintenance unit for a system being maintained is arbitrarily designated as the component, where groups of components form subsystems of the spacecraft system being maintained. Component replacement is the basic maintenance action. The two basic types of components are designated as signal flow and energy flow. Signal-flow components require power for operation but approach, or can be idealized as, single-vector transfer functions with specified causality and negligible power flow. Figure 2(a) illustrates such a system component where the vector $\{X\}$ is operated on by $T(\{X\})$ causing $\{Y\}$, or

$$\{Y\} = \left[T\left(\{X\}\right)\right]\{X\}$$

For the idealized signal-flow component the power supplied is dissipated as heat with no storage of energy within the component. Energy-flow components (refer to fig. 2(b)) are those components concerned with the direct dynamics of the physical system and are characterized by an input or output state $\left[\{e\},\{f\}\right]$ where

$$\{e\}^T\{f\} = \text{Power} = P$$

The state vectors $\{e\}$ and $\{f\}$ refer to effort and flow variables (refs. 1 and 2), such as voltage and current, force and linear velocity, torque and angular speed, pressure and flow rate, and so forth. Energy can accumulate within an energy-flow component, the rate of energy accumulation $\dot{E}$ being

$$\dot{E} = P_1 - \left(P_2 + \text{Heat}\right)$$

Transducer signal outputs $\{Y\}$ and control signal inputs $\{X\}$ are available and provide state measurement and control capability. Positive energy flow direction is indicated by the energy flow-line half arrow (⇀), and single-allowed energy flow direction is denoted by a full arrow (→). For convenience, since both types of components may have heat loss, the heat-loss arrow is omitted unless the heat loss plays a significant part in system operation.

The operational status of a system is defined as being a function of two types of system constraints: design constraints associated with energy-flow components and performance constraints associated with signal-flow components. Design constraints refer to excessive energy accumulation or flow within an energy-flow component; performance constraints are those imposed on certain signal-flow vectors or formulations of these vectors by the system objectives. Examples of excessive energy design constraints are high accumulator pressure, high gyro rotor speed, and high stress in an actuator. Excessive energy flow design constraints could be overload currents or high volume flows in lines. Performance constraints refer to allowable limits for vectors of selected signal-flow components, examples being the servo error of a controller and the partial pressure of oxygen in a controlled environment.

Design constraints, because of the dangers associated with accumulated energy or energy flow, must be locally monitored with local action to effect a reversal of the accumulation of energy or excessive energy flow. Examples of such devices are safety valves on tanks or accumulators, fuses or circuit breakers in electrical lines, rotor overspeed trips on control moment gyros, and so forth.

Serial monitoring of the state of energy-flow-component local action devices and selected signal-flow performance constraints determines the operational status of a given system being maintained. This function plus scheduled preventive maintenance (programed address of maintenance actuators) constitutes the nominal operational mode (monitor/maintenance) of EMMA. The monitoring is accomplished by serial address of appropriate constraint transducers by processor controlled discretes sent to spacecraft-system switching units. The status signals thus addressed are compared with reference values for specific sampling times (multiples of the basic iteration rate) and the differences adjudged to be within or not within reference tolerances. This mode, including the transmittal of scheduled preventive maintenance signals to appropriate component maintenance actuators, continues until a status signal is adjudged not within its reference tolerance. When this occurs, the maintenance system mode changes to classification/prediction.

Classification/Prediction

In this mode statistical averaging routines are used over an increased sampling time to determine whether the indication of faulty operation is intermittent or continuous. If the indication is intermittent (i.e., cannot meet the failure criteria of the classification/prediction mode), the information is stored in the memory unit and forms the basis for failure prediction. Failure prediction requires that a status signal be intermittently out of tolerance at an increasing rate. When the increasing rate is detected, the rate is extrapolated and a failure date, based on not meeting the failure criteria of the classification/prediction mode, is predicted. One approach to this prediction is discussed in appendix A. This is the first category of information transmitted to the astronaut and has the lowest priority for specific action. This information includes system and component transducer identification, probable failure date, automatic action that will occur when failure occurs, and any required request for manual assistance. If the out-of-tolerance indication is adjudged continuous, the maintenance mode changes to diagnostic. This third mode includes the preponderance of the computer routines of the system and represents the bulk of the work reported herein. The diagnostic routines are called serially, as required, from the memory and replace the monitor or prediction routines in the processor.

Diagnostic

The diagnostic routines called depend on which performance or design constraints are adjudged not within reference tolerances. These routines establish which component is not functioning properly by using programed deterministic logic. The diagnostic routines include characteristically (1) appropriate system reconfiguration for diagnosis, (2) test pulse firing to pertinent components, and (3) machine decision based on component response to test pulses. Diagnostic routine decisions are internal to the computer and require no action by the astronaut.

Repair/Replace

Subsequent to diagnostic decision and diagnostic routine termination, the maintenance mode changes to repair/replace. This final mode calls pertinent repair/replace routines from the memory unit based on diagnostic-mode output, searches hardware availability logs, and takes appropriate action. These actions may include automatic parallel-component switching, automatic system reconfiguration, or manual component repair or replacement. Logic pertaining to these actions is discussed in appendix B. In any case, the astronaut receives information which includes system and component identification, diagnostic results, automatic action taken, and again, any required request for manual assistance. The mode control then returns to monitor/maintenance.

CRITERIA FOR SYSTEM SYNTHESIS

The criteria for system synthesis pertain to the spacecraft systems to be maintained by the EMMA, in particular to the required modifications to these systems for automatic maintenance by the EMMA. An example of the application of these criteria to a control moment gyroscope (CMG) attitude control system is given in the next section of this paper. These criteria, which are based on the general rationale discussed in the previous section, are as follows:

- Identify the energy-flow and signal-flow components of the system to be maintained.
- Determine the design constraints associated with the energy-flow components and designate appropriate local action devices.
- Determine the performance constraints associated with the signal-flow components and designate transducers for monitoring the state of these constraints and also the state of the local action devices.
- Specify required preventive maintenance actions, schedules for actions, and actuators.
- Specify data for component-failure-prediction routines (appendix A).
- Determine the appropriate logic for the diagnostic routines. This logic includes system reconfiguration for diagnosis, component test inputs and required responses, and associated constraint address module (CAM) and pulse address module (PAM) discrete commands (appendix B).
- Determine the appropriate logic for the component replacement routines. This logic includes component selection, component warmup, system reconfiguration, and associated CAM and PAM discrete commands.

EMMA SIMULATION DESCRIPTION

The operational characteristics of an onboard expeditious monitor and maintenance analyst (EMMA) have been simulated on a CDC 6600 digital computer programed to operate in a real-time mode. This simulation is incorporated in the space station dynamics simulation at the Langley Research Center which includes a complete flexible spacecraft model, simulated control computer software, and a pilot control console (fig. 3). The space station dynamics simulation links to full-scale laboratory prototype control moment gyro (CMG) system hardware (figs. 4 and 5). The CMG system consists of three double-gimbaled, constant-speed wheels which are precessed by servocontrollers to provide spacecraft control torques as described in reference 3. This simulation has allowed the EMMA rationale and criteria to be evaluated for a typical spacecraft system requiring automatic monitoring and maintenance. The EMMA software communicates with the CMG hardware with both analog and discrete input and output functions. The simulation is controlled from the program control station shown in figure 6. This station allows control over the CDC 6600 computer and input-output hardware. The station includes a simulation console for data entry and control, a display console for postoperative data display, recorders, XY plotters, a typewriter for data exit and operator comment, and site communications.

The CDC 6600 computer itself uses 60-bit words; the digital-to-analog converter (DAC) and analog-to-digital converter (ADC) input-output units have 15-bit resolution over a ±100-volt range; and the discrete functions represent relay contact closures with 2.5-millisecond response times. The required computer interface with the CMG hardware for EMMA consists of 12 discrete computer outputs, one analog input (ADC), and one analog output (DAC). Interface with the pilot control console for display and manual monitoring requires 15 discrete computer outputs, 18 discrete computer inputs, one analog input, and one analog output. An on-line typewriter provides a second display function and record of system operation. Digital computer requirements for EMMA are 4100 words of memory and an average of 200 microseconds for each pass through the EMMA logic.

There has been no attempt to minimize the storage of the present simulation. An immediate reduction of this memory requirement by two-thirds could be accomplished since the CMG system consists of three identical CMG's. Further reduction could be realized through overlay techniques whereby only the routine (monitor, diagnostic, etc.) presently being utilized by the system would reside in the central memory at any one time. All routines could be stored on a slow-access memory unit (tape, disk file, etc.) and called into the central memory as required. This overlay technique could be applied to an EMMA responsible for all spacecraft systems by "occupying" the central processor with an executive routine which calls up specific maintenance system routines from the slow-access memory. Because of the serial requirements for such maintenance routines, the central processor memory and speed requirements become small.

The space station simulation operates at 32 iterations (computer cycles) per second and requires about 10 milliseconds per computer cycle. In addition to the computer hardware three types of peripheral hardware, local to the spacecraft system being maintained (the CMG system for this simulation), are required. These are (1) switching units (CAM and PAM), (2) measurement transducers, and (3) computer-controlled actuators.

The switching units used in this simulation are conventional relay "trees" (fig. 7) requiring six discretes to define a path from any one of 2^6 (64) signal leads to a single lead. Two such relay trees are required – one to enable the computer to read the measurement transducers and another to enable the computer to command the actuators within the system being maintained. Mechanical relays rather than electronic switches, such as field-effect transistors (FET's) and metal oxide silicon field-effect transistors (MOSFET's), were chosen for several reasons. The basic computer cycle time is compatible with the closure times of available relays. Simplicity of design was obtained when relays were utilized since the problem of individual gating voltages associated with electronic switches was avoided. The use of relays with two-pole capacity reduced the number of switching components by a factor of 2. The reliability of a tree utilizing relays is higher than one associated with electronic switches, and finally, highly conditioned power supplies are not necessary.

Thirty-two double-pole double-throw relays were utilized in each tree. The type of relay chosen has a low inertia and low response time and is highly reliable. Flight-qualified models are available commercially. The relay tree used for measurement transducers connects various chosen CMG parameters to an operational amplifier of ±100-volt capability with a 1-megohm input impedance. The high input impedance allows relay contacts in the monitor tree to accumulate as much as several kilohms of resistance without detrimental effects. The second relay tree (internally identical with that above) receives a command voltage from a computer-controlled DAC and directs the voltage to one of the actuators within the CMG system.

Measurement transducers convert various CMG system parameters such as heat, wheel speed, wheel vibration, and so forth to signals that the computer can recognize. The desired signals in this application must have large time constants relative to the monitor cycle time to prevent aliasing. Mechanical parameters such as temperature, vibration, and wheel speed are measured by thermistors, accelerometers, and inductive pickups, respectively. Electrical parameters such as rotor current are measured by current transformers. In addition, local action devices are required to insure that energy accumulation is bounded. All measured parameters which are cyclic in nature must further be filtered or rectified to prevent aliasing as previously mentioned, except for performance constraint transducers readings, in which case the computer sample rate is increased.

The computer control actuators for CMG system reconfiguration and component switching provide the final link between the computer and the CMG hardware. These actuators assist in the diagnostic portion of the program by providing the capability of isolating various hardware components from the system for performance checks and also provide the capability of removing a defective component and replacing it with a spare.

The actuators chosen were magnetic latching relays. These relays were used because of their high reliability, simplicity of design, and broad range of voltage and current handling capability. Also, latching relays do not require continuous coil energization in either contact position. This feature was highly desirable in this application since the relay may be required to remain in either position for indefinite periods of time.

EMMA Logic Description

Figure 8 shows a block diagram of the overall EMMA simulation routine. The system operation is divided into two basic sections: a monitor routine which simulates the first two EMMA modes and a diagnostic scheme which simulates the second two EMMA modes. The monitor addresses the CMG system transducers in binary code and monitors their output, and the diagnostic, called upon detection of a system malfunction, interrogates individual CMG components to locate the specific failure and initiate corrective action. Both the monitor and diagnostic routines are accessible through manual inputs from the pilot control console. The system utilizes one analog input channel (ADC) for the monitor and one analog output channel (DAC) for the diagnostic. The binary-coded relay-tree addresses for the monitor and diagnostic require six output discretes each and provide the capability to monitor 64 CMG system parameters and issue 64 corrective action commands.

The monitor routine (monitor/maintenance) operation is described schematically in figure 8. The computer uses a gray code format shown in table I to address sequentially the 64 CMG system parameters. The six-discrete-parameter address is made up and issued to the monitor relay tree. At the same time, the proper reference and tolerance values for the CMG system parameter to be monitored are placed in the comparator routine. A finite time later (at least 50 milliseconds), the analog line is read by the comparator. If the value is within tolerance, a sequencer notifies the system to set up the address of the next parameter. Preventive maintenance commands are not included in this simulation. If the monitored value is not within tolerance, an averaging routine (classification/prediction) is set up which reads the value continuously (32 times per second) for a specified time associated with the time constant of the parameter in question. At the end of this time, the averaged value of the parameter is checked by the comparator. If this value is within tolerance, the sequencer is tripped; if not, the diagnostic scheme is called. This information would form the basis for component or system failure prediction. Several parameters such as bearing temperature and vibration initiate no diagnostic action but involve shutting off the CMG spin power. The monitor routine continues to check the parameter and turns the CMG on again if the value comes back within tolerance.

Before the diagnostic scheme is described, a brief description of the manual interface with the monitor routine will complete the monitor description. In the automatic mode, the computer will continuously sequence through the CMG system parameters (table I) at any rate desired up to approximately 16 parameters per second, a limit imposed by simulation equipment input/output restrictions. The parameter readings may be displayed continuously on a digital voltmeter on the pilot control console, shown in figure 9. Binary coding of the addressed parameters is displayed by lights in the lower section of the manual address switches. The astronaut may elect at any time to check any parameter by setting up its binary code on the manual address switches and inserting this information into the computer. This halts the automatic sequence, addresses the desired parameter, and displays its output continuously on the digital voltmeter. This manual override provides the capability for manual system checkout and manual monitoring of a questionable system component.

The diagnostic routine is basically a logic scheme which takes the malfunction indication from the monitor, interrogates additional components to isolate the specific failure (diagnostic), checks whether redundant equipment is available for replacement, determines what corrective action is in order, and initiates action either to repair the fault (repair/replace) or to notify the control computer that the system must operate in a failure mode (1 CMG failed and removed from the control loop). The specific diagnostic logic employed is necessarily different for each type of system failure. Indeed, some system malfunctions such as bearing temperature and bearing vibration require no further diagnosis to determine that the CMG must be shut down until the lack of input power reduces the temperature or vibration. This fact would be noted by the monitor and the CMG reactivated. Other than these obvious cases, there are two primary sets of diagnostic logic: that used to determine specifically which power supply has failed and that to determine which component of a CMG gimbal servo loop is causing a servo error (performance constraint). These will be discussed separately in detail along with their associated component replacement sequences to illustrate this operation.

Power Supply Diagnostic

The individual CMG rotor and gimbal devices operate on several types of input power: 28 volts, ±15 volts, 5 volts, and 26 volts. A schematic of a typical CMG system power distribution system, including appropriate replacements, is shown in figure 10.

The entire system operates from a 28-volt dc bus with separate 15-volt, 5-volt, and 26-volt power supplies for each individual CMG. These are driven by a separate inverter for each CMG. The power supplies are thus interrelated, and the indicated failure of a 15-volt supply for example could be due to an inverter failure or a 28-volt-supply failure. Isolation of the exact malfunction involves a straightforward check back up the line until the faulty component is located. No provision has been made for the 28-volt-bus failure since this will shut down the entire system and should be monitored as a part of the spacecraft electrical power system. An example of failure isolation logic is shown schematically in figure 11 for a typical 15-volt-failure indication. One of the other power supplies operating from the inverter, in this case the 5-volt supply, is immediately addressed and monitored. If this output is within tolerance, the 15-volt supply has been identified as the malfunctioning component; if the 5-volt supply is also out of tolerance, interest is shifted to the inverter. The 28-volt output is then addressed and checked to determine whether the fault lies within the inverter or the 28-volt supply. When the faulty component is isolated, a check is made to determine whether a replacement is available. As shown in figure 10, one replacement unit of each type of power supply is available for use in any individual CMG. The status of this unit is stored within the computer and once it has been used, any future call for that power supply type will not locate a replacement. This will result in a CMG shutdown unless the replacement has been restored by the crew since the previous failure.

Identification of the faulty power supply and location of an available replacement initiates the following power-supply replacement sequence:

1. Switch CMG out of control loop
2. Start replacement power supply
3. Shut down CMG spin power (Warmup period)
4. Disconnect inner-gimbal power amplifier output (Warmup period)
5. Disconnect outer-gimbal power amplifier output (Warmup period)
6. Switch out failed power supply (Warmup period)
7. Switch in replacement power supply
8. Connect outer-gimbal power amplifier output
9. Connect inner-gimbal power amplifier output
10. Reactivate CMG spin power
11. Switch CMG into control loop

Note: All operations except 1 and 11 require two computer iterations – one to set PAM address and one to pulse system actuator relay.

The commands in this sequence are transmitted via the six binary-coded discretes to the command relay tree of figure 7. The replacement power supply is activated first so that it may warm up prior to being switched in. The CMG spin power is shut down and the CMG remains out of the control loop during the entire sequence. The gimbal servo loop power amplifiers for both gimbals are disconnected from the gimbal torque motors to avoid transient-created damage to the gimbal drives during power-supply switchover. The faulty power supply is then switched out, and when the warmup period for the replacement is over, the new unit is switched in. The gimbal servo loops are reconnected and spin power again applied. The sequencer then notifies the computer routine that the operation is complete so that the CMG may again be switched into the control loop and the monitor sequence may resume.

The original parameter error and the corrective action taken are stored in binary-coded form which is available for pilot interrogation from the manual console shown in figure 9. In addition, both are recorded in alphanumeric form by an on-line typewriter for permanent record and subsequent analysis as shown in figure 12.

CMG System Error Diagnostics

A general system diagnostic technique is discussed in appendix B for a hypothetical system. This technique, in principle, was used to synthesize diagnostic routines for the CMG system illustrated in figure 13. These diagnostic routines are aimed at isolating a faulty component in the system when an out-of-tolerance performance constraint at any of the lettered points is indicated. The diagnostic software sequence described below is outlined in figure 14 for the CMG system block diagram of figure 13. These two figures represent a special case of the two general system figures discussed in appendix B and the notation is the same. The vehicle-attitude sensor loop is not included in this simulation since actual sensor hardware is not used but modeled in the computer. The performance constraint at point C is generated by comparing the desired control computer output rate of change of momentum with a rate of change of momentum based on CMG gimbal sensor outputs. The performance constraint at point D is generated by comparing steering-law-generated CMG precession-rate commands with motor tachometer outputs (servo loop errors). Both performance constraints are monitored. The necessity for monitoring point D arises from the relative insensitivity of the performance constraint to failure or partial failure of one of the six CMG gimbal servo loops (point D).

A performance constraint error at point C may be due either to one servo loop error (loop D) or a steering-law-loop failure. A failure of this type involves opening the resolver feedback and serially pulsing each of the six servo loops and checking their outputs. If these are all correct, the six servo loops are again pulsed and the gimbal tachometers checked to determine whether the gimbals are moving. Once gimbal motion is established, the gimbal sensors (resolvers) are checked by again pulsing the gimbal servo and checking the resolver outputs. Positive indications on all checks indicate an error in the steering law in the control computer.

The CMG gimbal servo error, whether detected by the monitor or the CMG system error diagnostic, involves opening the motor tachometer feedback and pulsing the gimbal power amplifier. The output of the power amplifier (E), gimbal tachometer (12), and motor tachometer (4) are checked to isolate the specific faulty component. All positive responses to these pulses indicate that the preamplifier itself is bad. Once the preamplifier has been isolated as the source of the problem, a replacement sequence similar to the CMG power supply replacement is initiated. The CMG spin power is shut off and the power amplifier outputs on both gimbals are disconnected to avoid gimbal damage. The bad preamplifier is switched out and the replacement preamplifier input is connected. After preamplifier warmup, the preamplifier output is switched into the loop and the gimbal actuators are again connected to the power amplifier. The CMG spin power is reactivated and the CMG placed back in the control loop.

SIMULATED SYSTEM PERFORMANCE

The EMMA software was programed, and computer-generated failure conditions were used to check out the basic logic operations. The simulation was then linked to the CMG hardware and actual component failures simulated to verify the EMMA diagnostic logic and repair sequences. Since it is not desirable to fail operational CMG system components, only those failure conditions which could readily be simulated were investigated. Mechanical failures such as sheared gear trains and gimbal binding could not be represented but most of the system component failures were considered. A description of how the CMG system failures were generated and the action taken by EMMA follows. The prediction mode was not simulated because computer time (and therefore cost) would have been excessive.

The bearing-temperature and vibration signals were biased to simulate high values of these parameters. The EMMA routine detected these out-of-tolerance conditions and shut off CMG spin power so that the situation might be allowed to improve. The bias signals were then removed, and when the monitor determined that the readings were again normal, the CMG was reactivated and switched back into the control loop. EMMA then noted that the CMG wheel speed was below tolerance and issued a request for manual assistance. The typewriter record of CMG shutdown because of excessive bearing temperature or vibration showed that the CMG could be left in the control loop until the rotor speed returned to normal.

The CMG power-supply failures were simulated by simply disconnecting the power-supply output. EMMA detected the failure and proceeded with the power-supply replacement sequence previously described. The power-supply replacement was simulated by a computer-actuated relay which reconnected the power-supply output and thus actually made the CMG operational. Inverter and 28-volt-bus supply failures were simulated by disconnecting the output of the affected power supplies shown in figure 10. It was not possible to simulate the replacement of this equipment since the laboratory prototype hardware does not use these components, as would a flight system for which the EMMA logic was designed.

Several servo loop failures were simulated to check out the servo loop diagnostic routines. Preamplifier and power amplifier failures were simulated by imposing on their output a bias which represented the opening of these components and drove the gimbal open loop. Disconnection of the bias signal as a part of the replacement sequence simulated the switching in of a new component. A feedback loop failure was simulated by disconnecting the motor tachometer output. No repair was effected in this case since a bad motor tachometer would have to be replaced or repaired manually for the prototype CMG's. Gimbal resolver failures were simulated by disconnecting the gimbal potentiometer output. Again, this repair would have to be accomplished manually for the prototype CMG's. The computer action consisted of printing out the error and a request for manual assistance. These were all the CMG system failures which could be realistically simulated with the prototype hardware.

The monitor and diagnostic sampling period used for the hardware checks was 0.5 second so that the entire system was monitored every 32 seconds. At this sampling rate, the longest diagnostic (servo loop) required approximately 3 seconds to locate the failure component. The component replacement sequence is characteristically about 1 second in duration excluding component warmup time. The overall system, including the hardware interface, worked well for the component failures simulated, which should be representative for all system malfunctions. The automatic switching sequence for component replacement also works smoothly and appears reasonable for spacecraft applications where automatic repair or replacement is feasible.

The prototype hardware interface verification runs have indicated a strong need for checking out the logic with actual hardware to make sure that the symptoms exhibited by the faulty hardware are properly recognized and diagnosed by EMMA. For this reason, techniques of simulating all CMG system failures including mechanical failures should be developed and the logic checked completely prior to implementation in an actual spacecraft application. EMMA system operation from the manual console has been checked out in conjunction with the monitor routine and the binary display of system malfunctions. From these operations, it appears that a manual override capability is extremely desirable for all steps of the fault isolation and repair operation. The binary error display proved to be much more limited than the typewriter readout in the amount of information which could be provided for analysis by man. For this reason, it is felt that an alphanumeric display of some type is essential for an onboard fault isolation and maintenance system. The EMMA printout, shown in figure 12, provides the time of failure detection, the faulty component, the average output of that component when the failure was detected, and the action taken or requested by the computer. As shown in figure 12, one possible EMMA action is the activation of the spacecraft reaction control system (RCS). For actual spacecraft applications, an entire serial record of the operations performed and the diagnostic and repair routines used by the computer in isolating and correcting the system error would be more useful to an astronaut in any subsequent analysis of the problem.

CONCLUDING REMARKS

The feasibility of a maintenance system which can automatically monitor, diagnose, and repair onboard spacecraft systems in operation has been demonstrated. Ground rules which permit the design of an automatic maintenance system have been established by the synthesis of an expeditious monitor and maintenance analyst (EMMA).

Laboratory operation with the EMMA system has shown that an automatic checkout and repair capability is extremely useful. The EMMA simulation has minimized simulation setup time to such a degree that this routine has been incorporated in all control moment gyro hardware simulations. It has been concluded that a fully automatic maintenance system which includes component replacement capability, such as the EMMA described in this report, is essential and should offset increasing spacecraft system cost, complexity, and lifetime requirements.

Evaluation of the performance of a simulated EMMA indicated several factors pertinent to system checkout and astronaut participation. The system software should be linked to the actual spacecraft system hardware to validate performance prior to finalizing the software routines. In addition, the computer printout should be as complete as possible in informing an astronaut what has been found wrong in the spacecraft system and what the computer has done to isolate and correct the fault. Also, the astronaut should have complete manual override capability over the automatic monitor, diagnostic, and repair operations as a backup in the event that computer software routines contain errors or omissions. This override capability should include astronaut callup of the appropriate routines and reprograming capabilities.

Langley Research Center,
National Aeronautics and Space Administration,
Langley Station, Hampton, Va., December 16, 1969.

APPENDIX A

COMPONENT FAILURE PREDICTION

This appendix presents one approach to the problem of automatic component failure prediction. In figure 15 a typical performance constraint transducer reading ϵ is plotted against time. The area, bounded by the positive and negative values of the performance constraint ϵ_0 represents monitor/maintenance mode allowed transducer readings. The durations of the out-of-tolerance readings are shown in the lower part of the figure, as are the points in time at which the computer samples the reading. Also shown is the number of readings detected to be out of tolerance. Assuming that the samples are taken at random, the probability of detection p is equal to the total out-of-tolerance duration divided by the total time and also equal to the number of detected out-of-tolerance readings divided by the number of samples. Therefore, by setting the values of ϵ_0 used in the monitor/maintenance mode to be more stringent than those used in the classification/prediction mode (this permits a large number of initial out-of-tolerance readings prior to system diagnosis and component replacement), the probability p becomes a measure of performance. Finite Taylor's series extrapolation can be used to predict when, in time, this parameter p will increase to a value where system diagnosis and component replacement are required.

APPENDIX B

SYSTEM DIAGNOSTIC ROUTINES

A maintenance block diagram for a hypothetical spacecraft system typical in principle to most spacecraft systems containing energy-flow components (EFC-1) and signal-flow components (SFC-1) is illustrated in figure 16. The energy flow for this system is indicated by solid lines and the signal flow by broken lines. Even-numbered signal-flow components represent measurement devices and odd-numbered components represent analog computation (preamplifier) or digital computation hardware. The numbers refer to points at which signal-measurement transducers are located, points at which EMMA controlled input commands can be applied, or points at which the signal path can be broken. The lettered points refer to performance constraint transducers and would be, typically, errors between desired performance and performance as measured by the even-numbered signal-flow components. The performance constraint transducer at point A is considered indicative of overall system performance and as such is the only constraint checked by the monitor. If this performance reading is out of tolerance, a diagnostic routine is necessary to isolate the component of the system that is responsible for the poor performance.

A general procedure for synthesizing the diagnostic logic for the system of figure 16 is shown in figure 17. The logic flow begins at point A and ends by designating the faulty component. The scheme followed is to (1) open the outermost feedback loop; (2) evaluate the performance of the conglomerate internal loop; and (3) evaluate the transfer functions of all components outside the internal loops with the conglomerate loop being used as a portion of the input signal path to the faulty component. The diagram may be followed through to the isolation of a specific faulty component. The code words "Pulse" and "Check" refer to the application of a specific input and the evaluation of the response to that input, relative to a computer-stored characterization of the required response.

A simple method of characterizing the required response of a component that includes a measure of both the static and dynamic response is illustrated in figure 18. The response y of a component to a step input x is illustrated, with the lettered points referring to changes in the sign of the slope of the response y. The computer samples the response at intervals which are sufficiently smaller than the oscillation period of the component and stores the values of the response at points A, B, C, . . . using a simple logic scheme to detect when the slope of the response changes sign. Both the magnitude and the time of occurrence of these data are compared with desired values to test component performance – the simplest scheme being to store only the last two points until their difference divided by their sum is less than a specified fraction. This point in time is a direct measure of settling time, a common dynamic response characterization; the average value of these two points is a measure of component static, or "dc," response.

REFERENCES

1. Paynter, Henry M.: Analysis and Design of Engineering Systems. M.I.T. Press, 1961.
2. Paynter, H. M.; and Karnopp, D. C.: Design and Control of Multiport Engineering Systems. Reprinted from Proceedings of IFAC Tokyo Symposium on Systems Engineering for Control System Design, 1965, pp. 443-454.
3. Kurzhals, Peter R.; and Grantham, Carolyn: A System for Inertial Experiment Pointing and Attitude Control. NASA TR R-247, 1966.

TABLE I.- GRAY CODE FORMAT TO ADDRESS CMG PARAMETERS

Sequence number	Gray code address					CMG system parameter
1						Spare
2					1	28-volt supply, CMG 1
3				1	1	+15-volt supply, CMG 1
4				1		-15-volt supply, CMG 1
5			1	1		5-volt supply, CMG 1
6			1	1	1	28-volt supply, CMG 2
7			1		1	26-volt supply, CMG 2
8			1			Rotor speed, CMG 1
9		1	1			Spin current, CMG 1
10		1	1		1	+15-volt supply, CMG 2
11		1	1	1	1	28-volt supply, CMG 3
12		1	1	1		-15-volt supply, CMG 2
13		1		1		Left-bearing temperature, CMG 1
14		1		1	1	5-volt supply, CMG 2
15		1			1	Right-bearing temperature, CMG 1
16		1				Bearing vibration, CMG 1
17	1	1				Inner-gimbal power amplifier, CMG 1
18	1					Outer-gimbal power amplifier, CMG 1
19	1		1			Inner-gimbal servo error, CMG 1
20	1	1	1			26-volt supply, CMG 2
21	1	1	1	1		+15-volt supply, CMG 3
22	1		1	1		Rotor speed, CMG 2
23	1			1		Outer-gimbal servo error, CMG 1
24	1	1		1		Spin current, CMG 2
25	1	1		1	1	-15-volt supply, CMG 3
26	1			1	1	Left-bearing temperature, CMG 2
27	1		1	1	1	5-volt supply, CMG 3
28	1	1	1	1	1	26-volt supply, CMG 3
29	1	1	1		1	Rotor speed, CMG 3
30	1		1		1	Right-bearing temperature, CMG 2
31	1				1	Inner-gimbal motor tachometer, CMG 1
32	1	1			1	Bearing vibration, CMG 2

Sequence number	Gray code address						CMG system parameter
33	1	1	1			1	Spin current, CMG 3
34	1	1	1		1	1	Left-bearing temperature, CMG 3
35	1	1	1	1	1	1	Spare
36	1	1	1	1		1	Right-bearing temperature, CMG 3
37	1	1		1		1	Bearing, vibration, CMG 3
38	1	1		1	1	1	Inner-gimbal power amplifier, CMG 3
39	1	1			1	1	Outer-gimbal power amplifier, CMG 3
40	1	1				1	Inner-gimbal power amplifier, CMG 2
41	1					1	Inner-gimbal tachometer, CMG 1
42	1				1	1	Outer-gimbal power amplifier, CMG 2
43	1			1	1	1	Inner-gimbal servo error, CMG 3
44	1			1		1	Inner-gimbal servo error, CMG 2
45	1		1	1		1	Outer-gimbal servo error, CMG 3
46	1		1	1	1	1	Inner-gimbal motor tachometer, CMG 3
47	1		1		1	1	Inner-gimbal tachometer, CMG 3
48	1		1			1	Outer-gimbal servo error, CMG 2
49	1		1				Outer-gimbal motor tachometer, CMG 1
50	1	1	1				Inner-gimbal motor tachometer, CMG 2
51	1	1					Outer-gimbal tachometer, CMG 1
52	1						Outer-gimbal power amplifier, CMG 1
53	1			1			Inner-gimbal power amplifier, CMG 1
54	1	1		1			Inner-gimbal tachometer, CMG 2
55	1	1	1	1			Outer-gimbal motor tachometer, CMG 3
56	1		1	1			Outer-gimbal motor tachometer, CMG 2
57	1		1	1	1		Outer-gimbal tachometer, CMG 3
58	1	1	1	1	1		Outer-gimbal power amplifier, CMG 3
59	1	1		1	1		Inner-gimbal power amplifier, CMG 3
60	1			1	1		Outer-gimbal tachometer, CMG 2
61	1				1		Spare
62	1	1			1		Outer-gimbal power amplifier, CMG 2
63	1	1	1		1		Spare
64	1		1		1		Inner-gimbal power amplifier, CMG 2

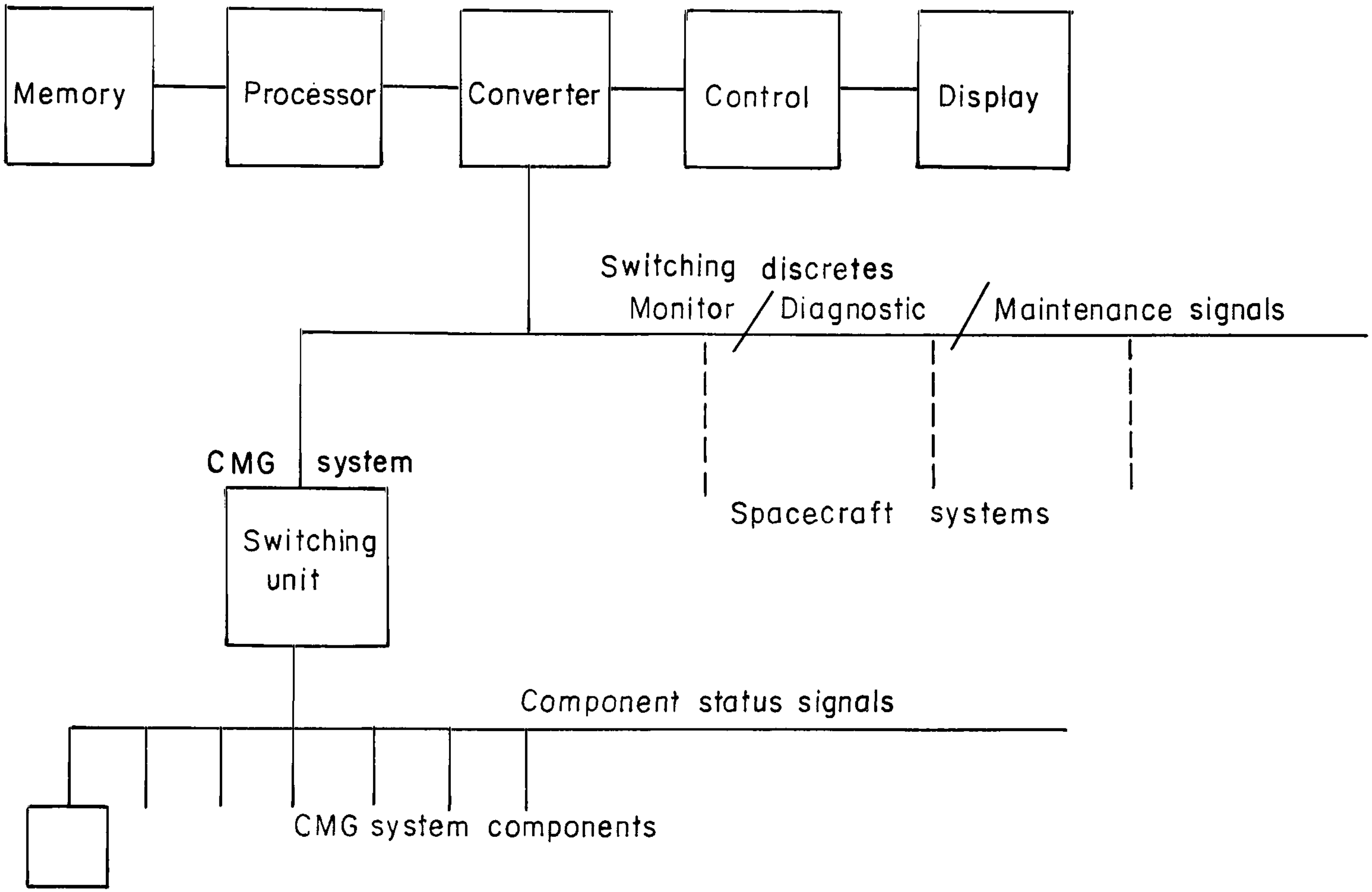
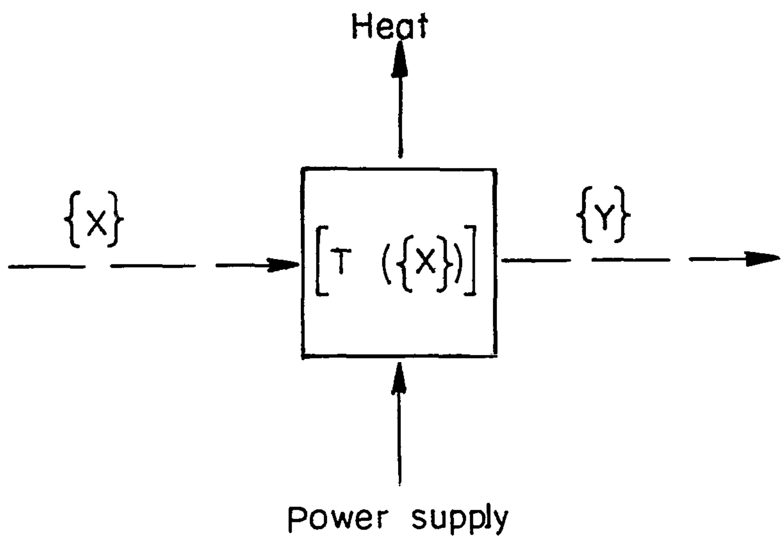
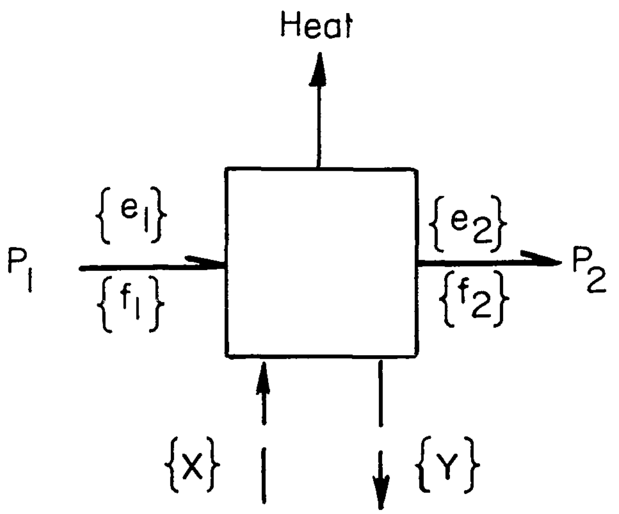


Figure 1.- Maintenance system block diagram.



(a) Signal-flow component.



(b) Energy-flow component.

Figure 2.- Idealized maintenance components.

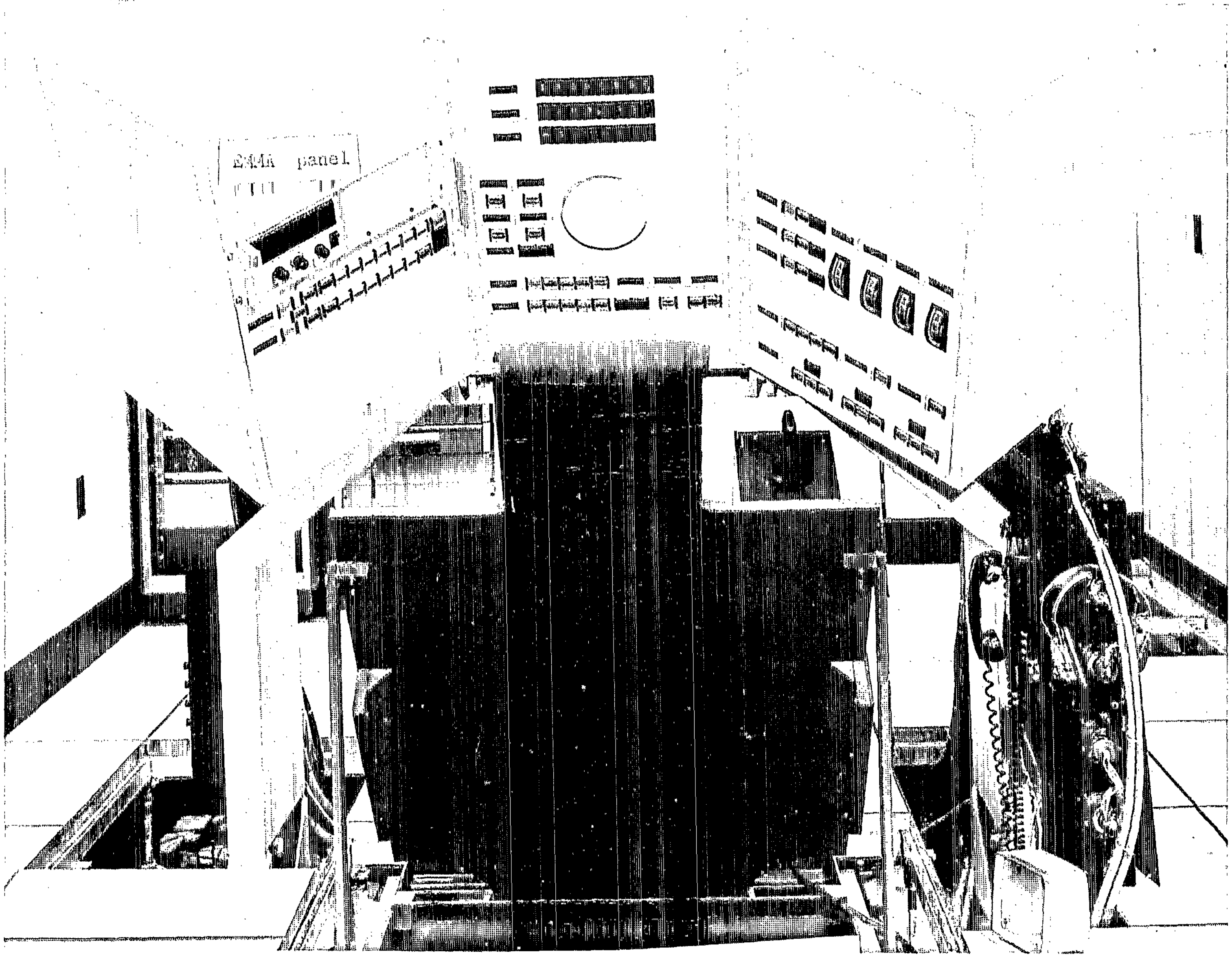


Figure 3.- Pilot control console. L-69-4970.1

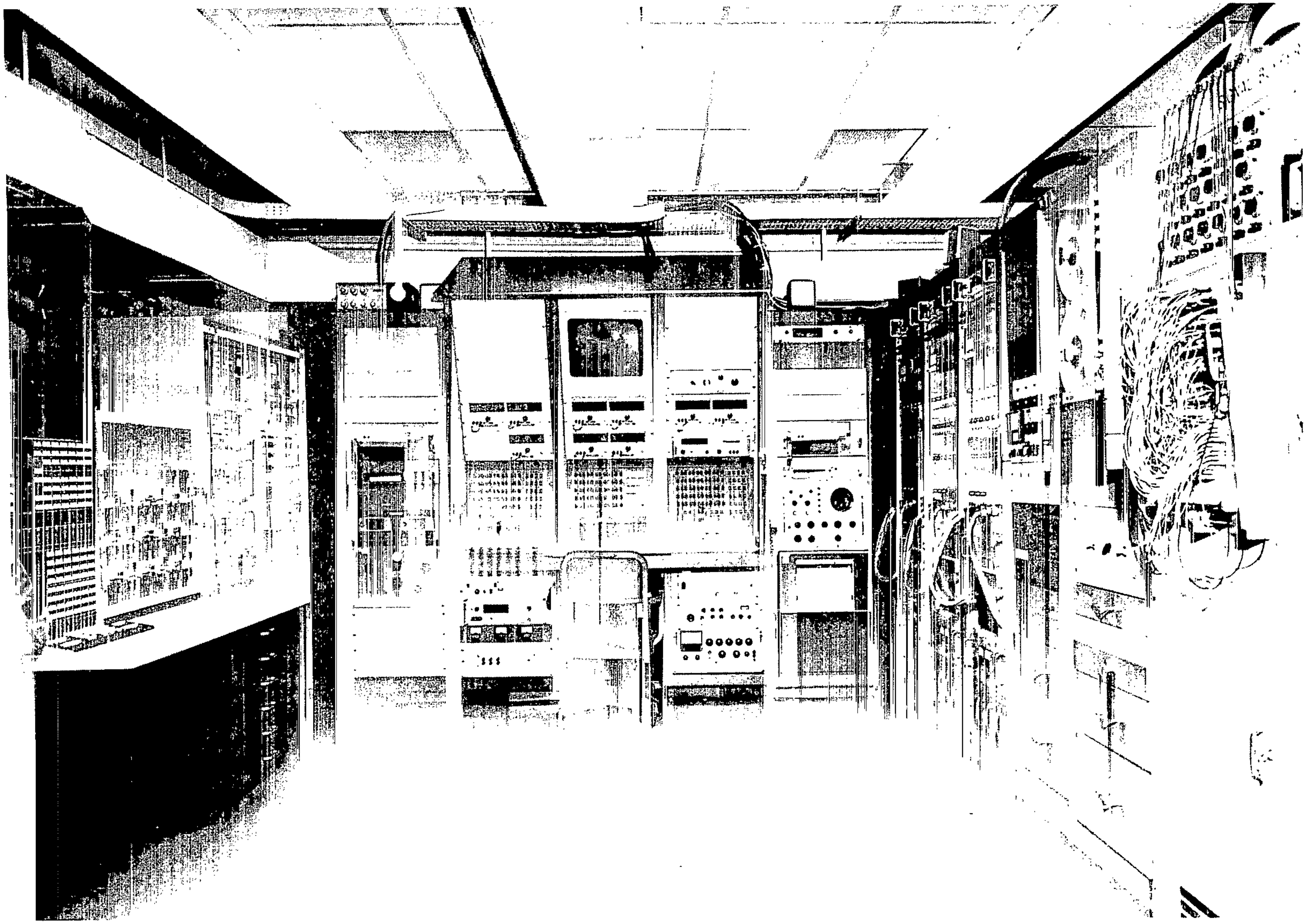


Figure 4.- CMG control electronics laboratory.

L-69-5141

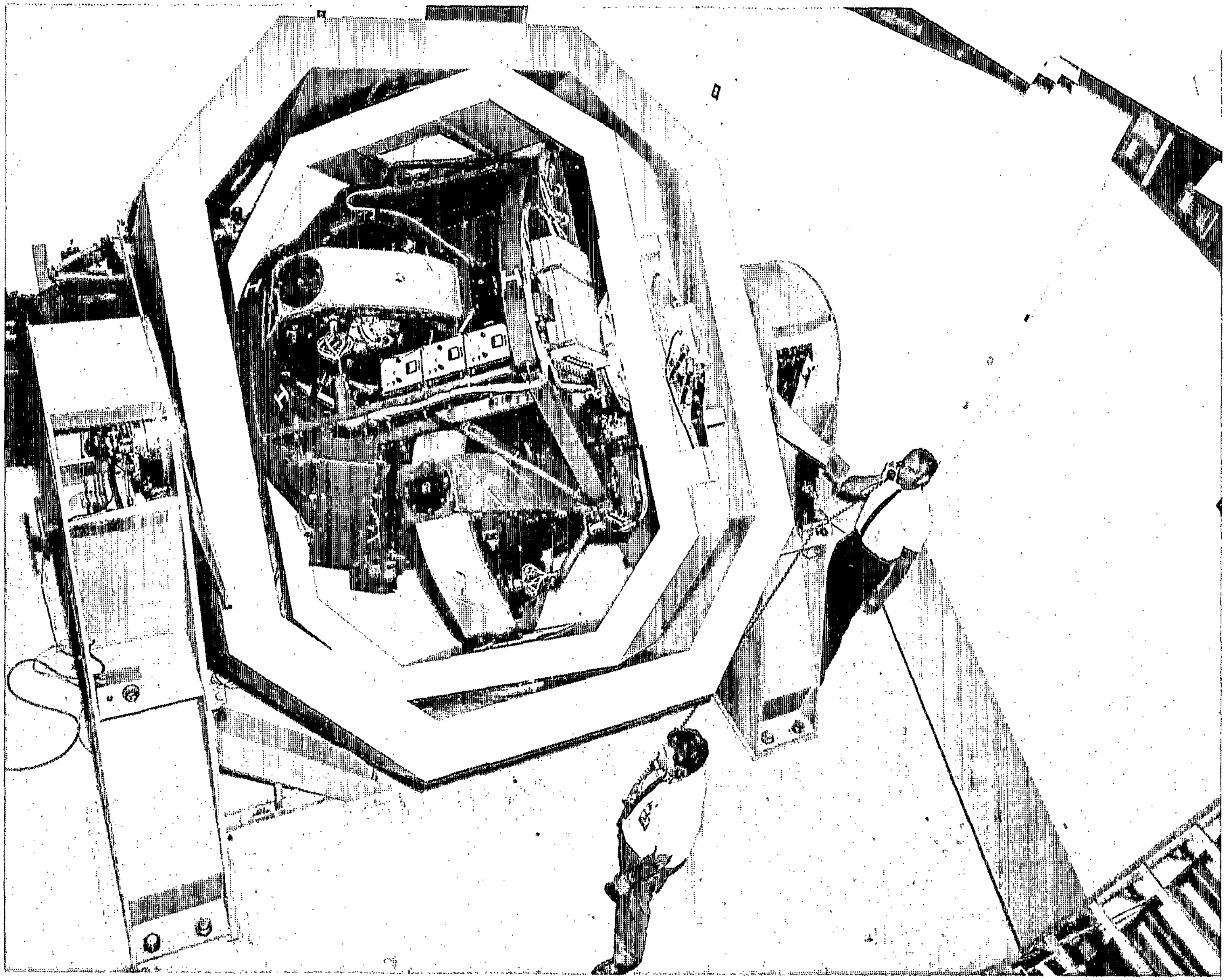
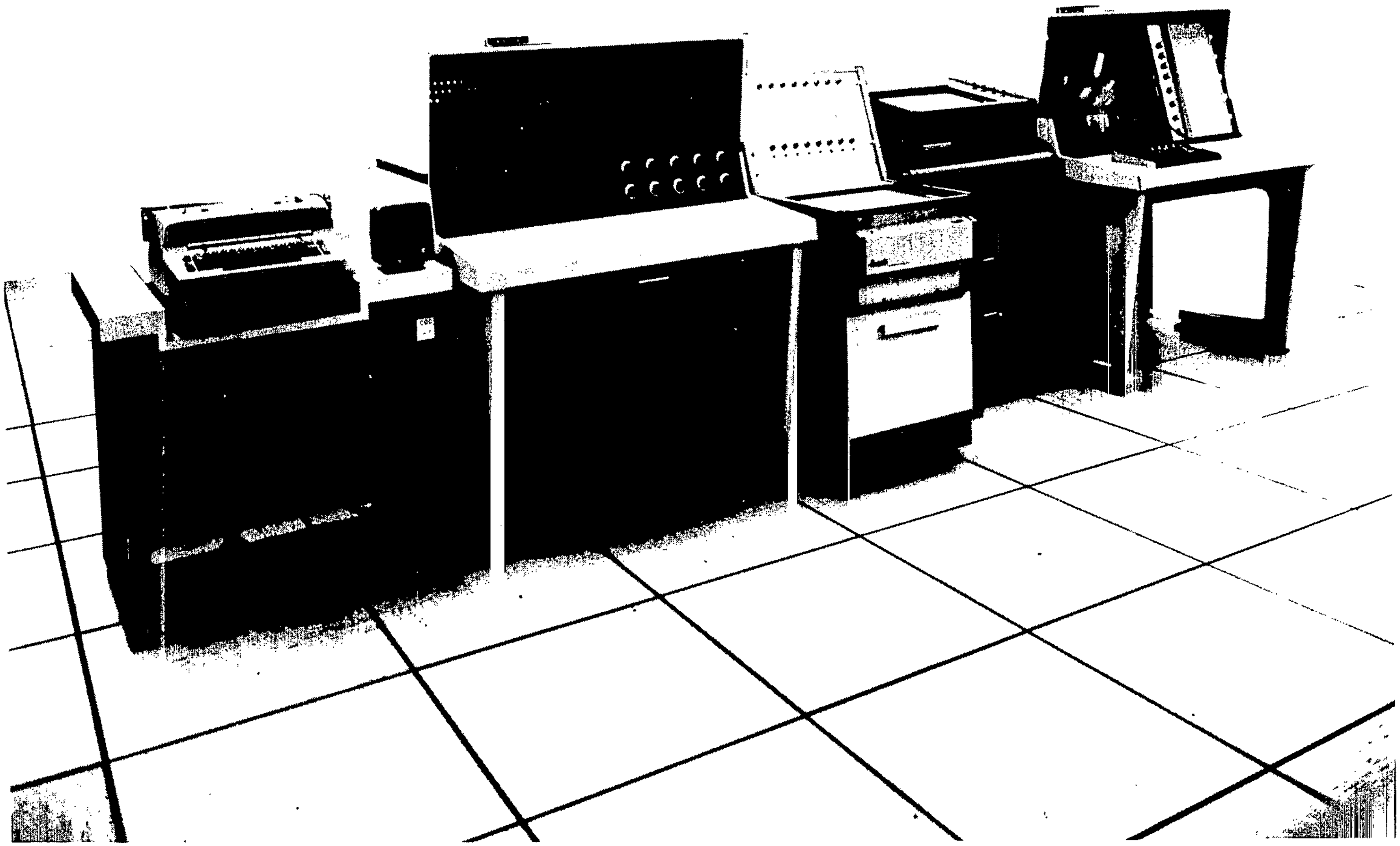


Figure 5.- CMG system on moving base simulator. L-69-5142



L-69-5143

Figure 6.- Simulation program control station.

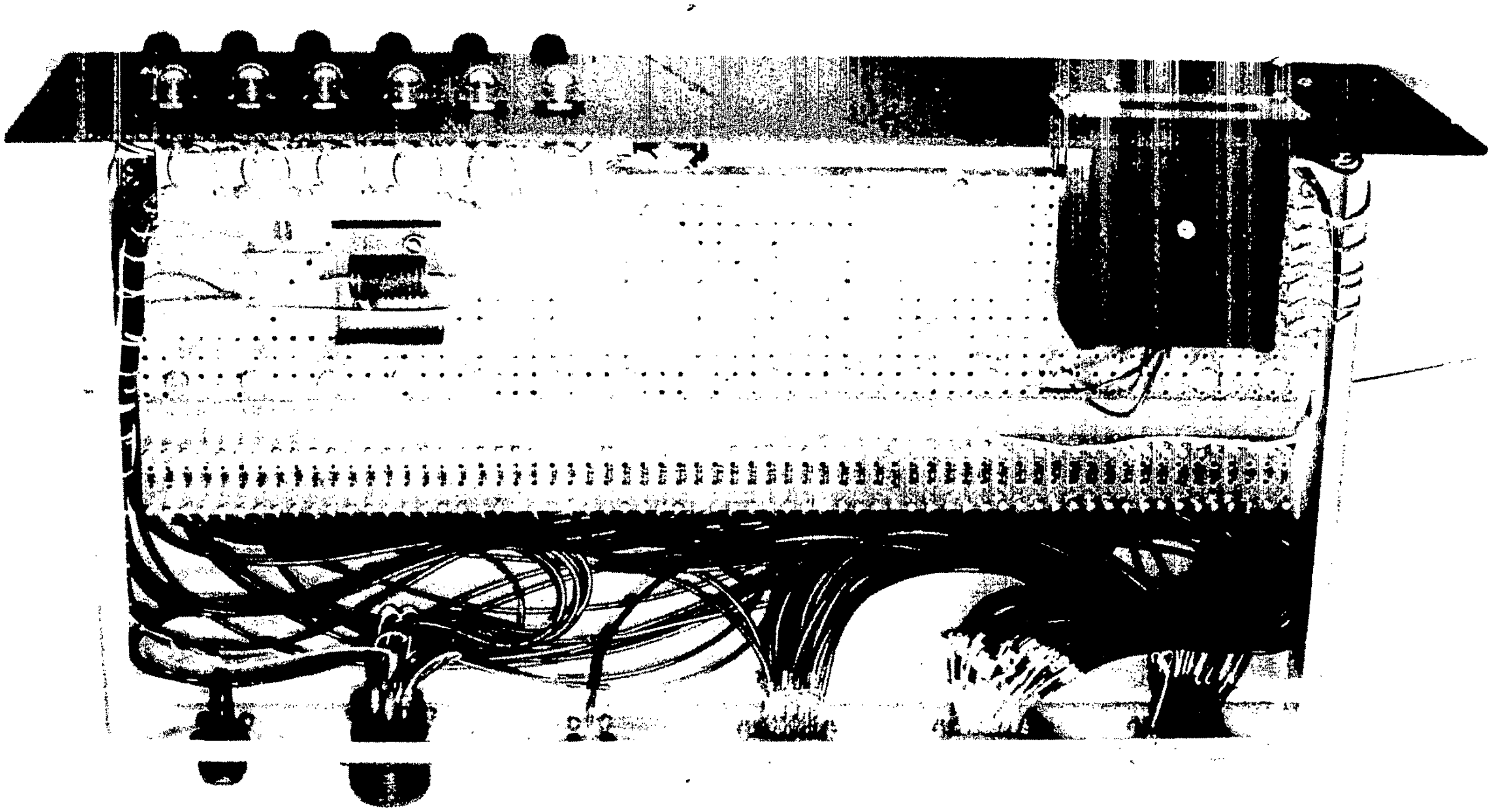


Figure 7.- EMMA signal switching unit.

L-69-5144

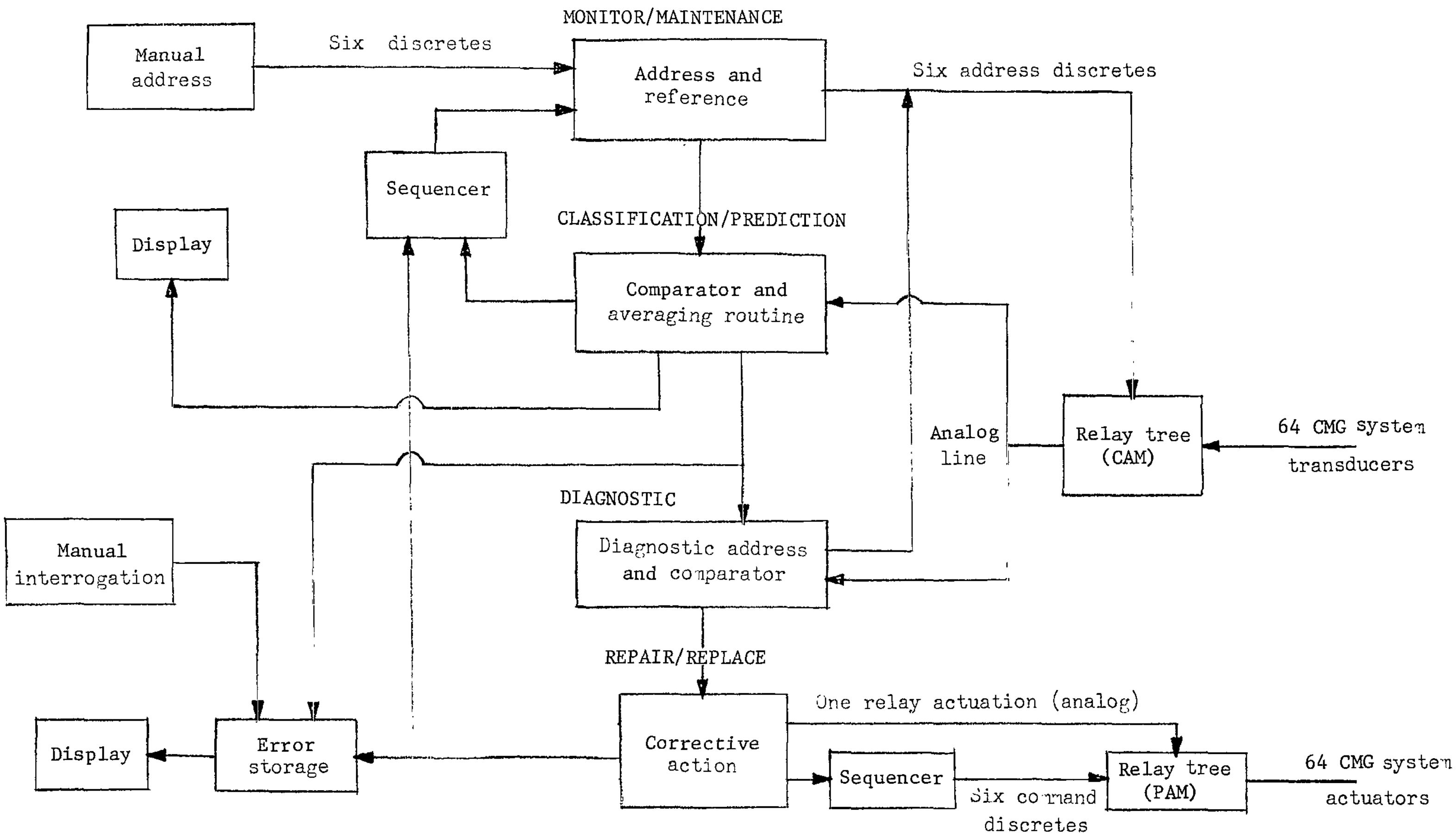


Figure 8.- EMMA software and input-output block diagram.

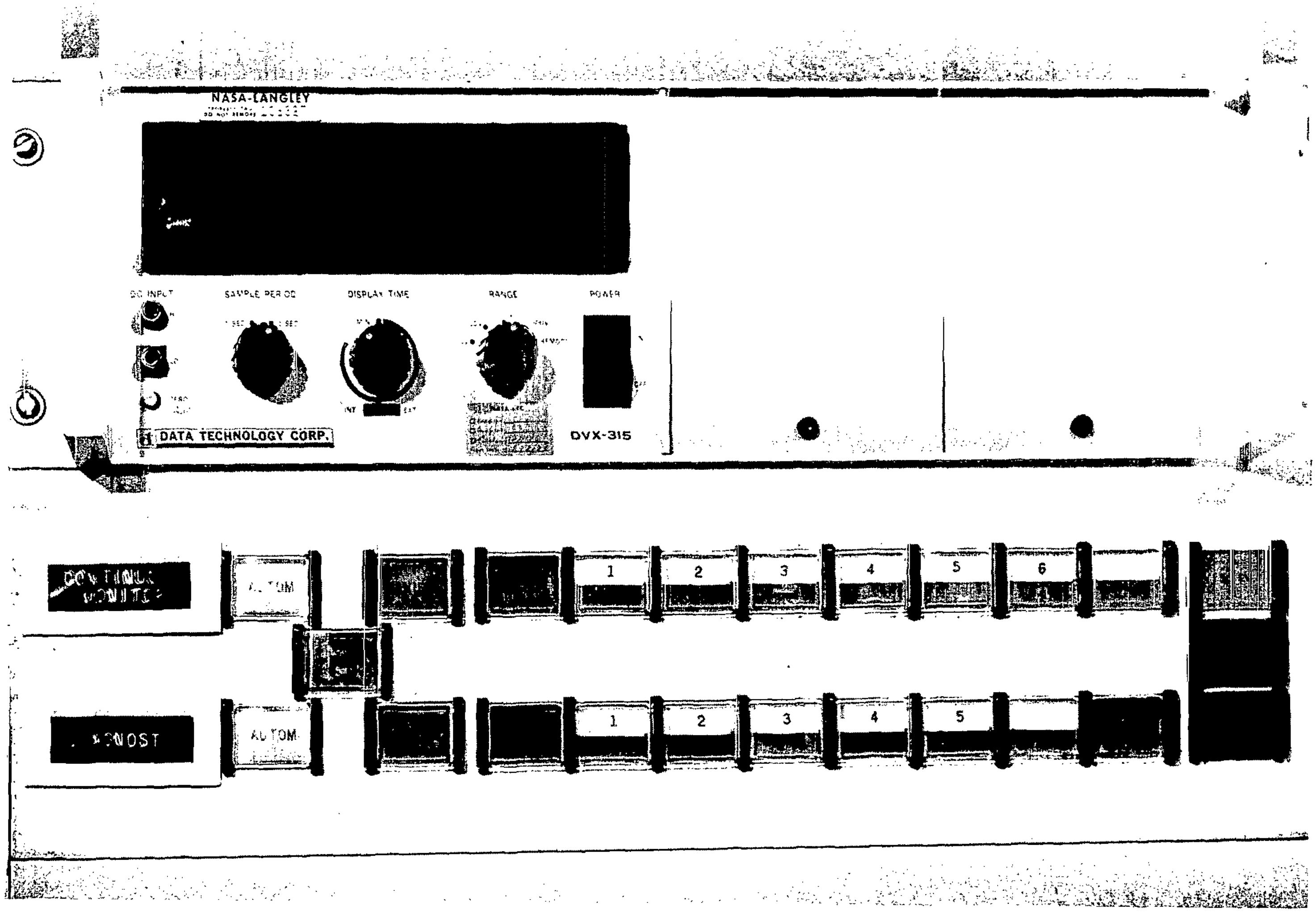


Figure 9.- EMMA pilot console panel. L-69-4977

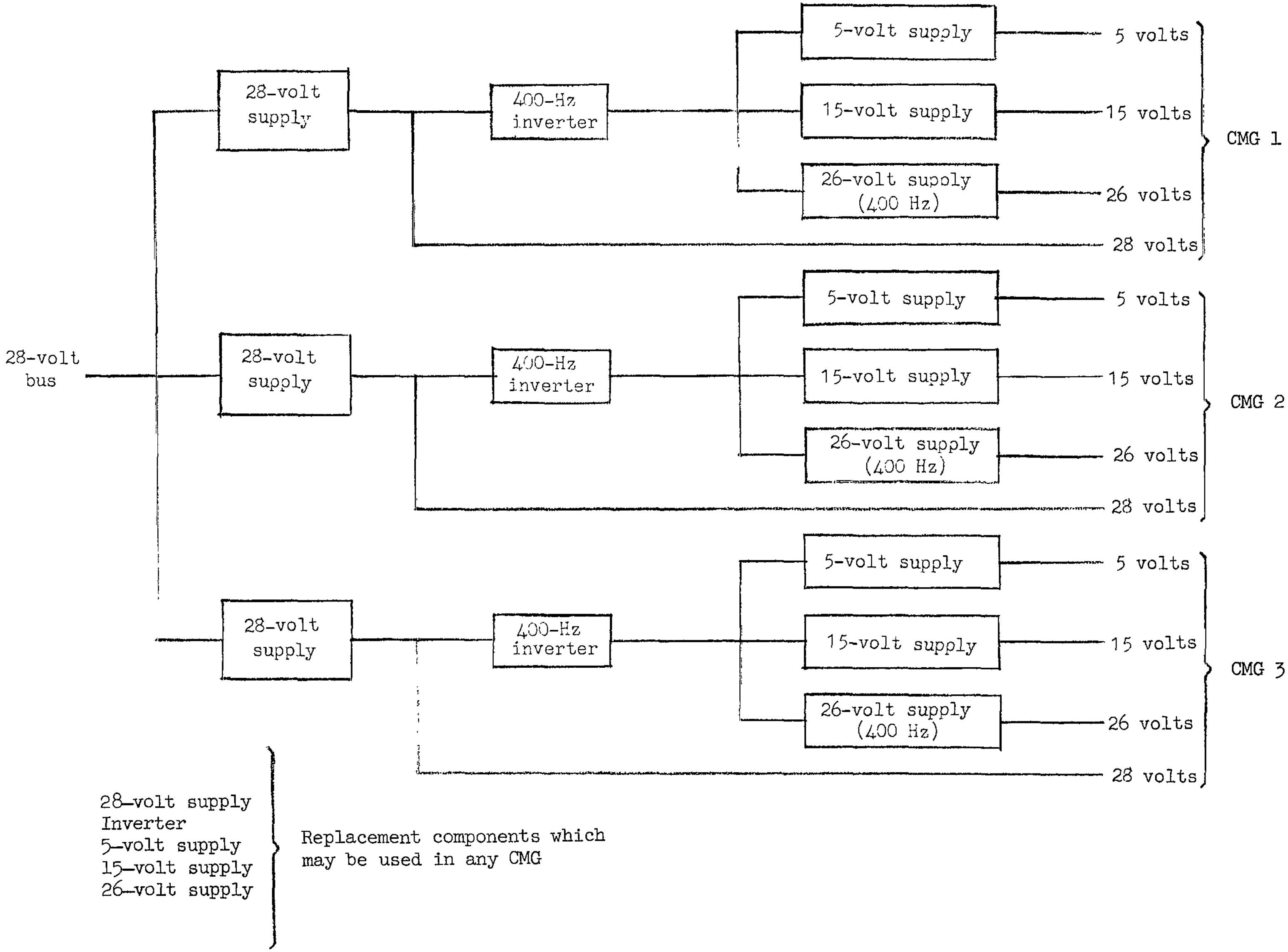


Figure 10.- CMG system power-supply diagram.

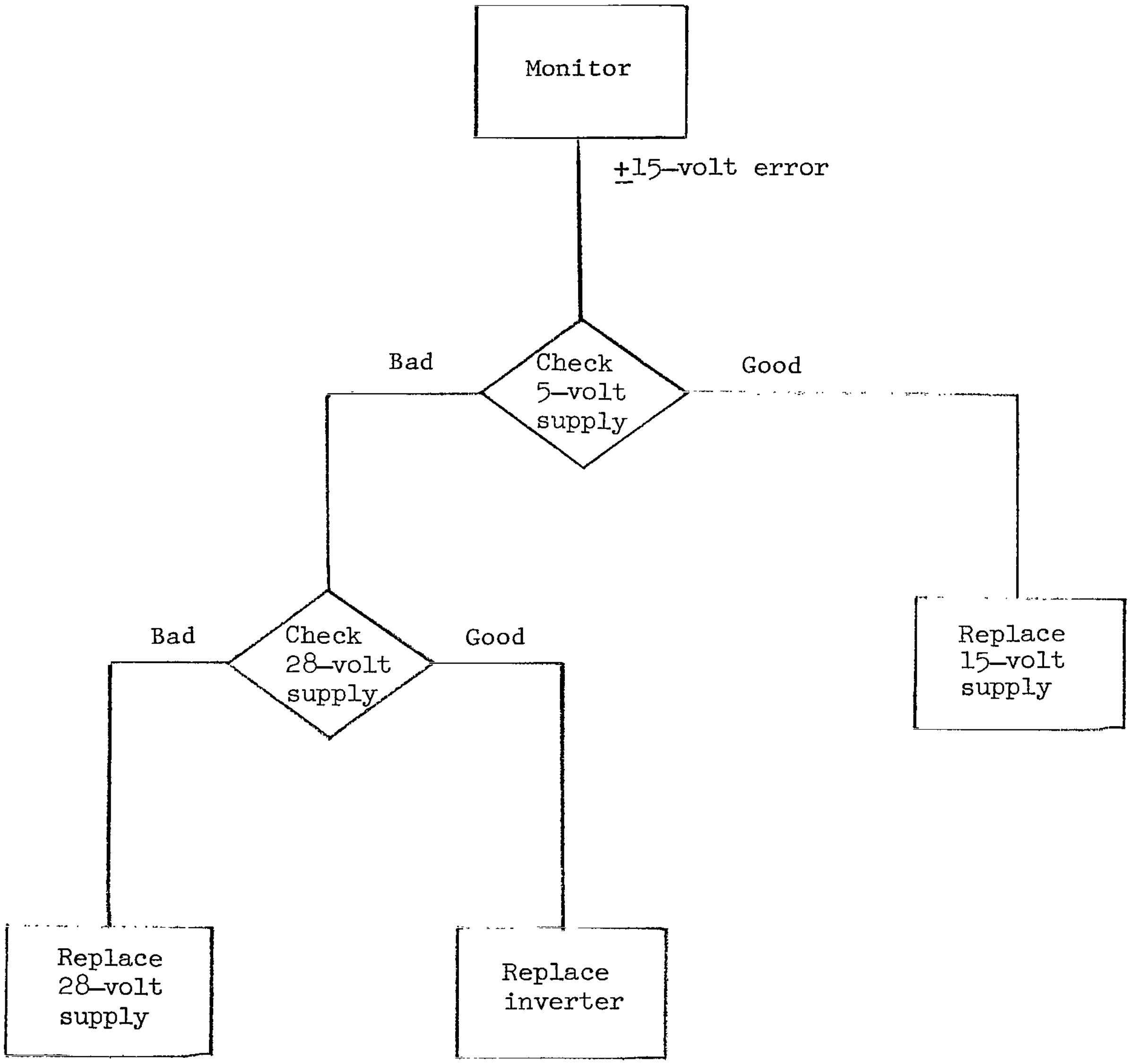


Figure 11.- CMG power-supply-failure isolation logic.

```
 Ø9/19/69  Ø8.18.42.
CMG SYSTEM FAILURE DETECTED
 +28 VOLT         * CMG 3 * AV READING=   .Ø11
          POWER SUPPLY REPLACED
***********************************************

 Ø9/19/69  Ø8.19.3Ø.
CMG SYSTEM FAILURE DETECTED
 +26 VOLT         * CMG 3 * AV READING=   .Ø11
          POWER SUPPLY REPLACED
***********************************************

 Ø9/19/69  Ø8.21.39.
CMG SYSTEM FAILURE DETECTED
 +15 VOLT         * CMG 3 * AV READING=   .ØØ7
          POWER SUPPLY REPLACED
***********************************************




 Ø9/19/69  Ø8.24.13.
CMG SYSTEM FAILURE DETECTED
 + 5 VOLT         * CMG 3 * AV READING=   .ØØ9
          POWER SUPPLY REPLACED
***********************************************

 Ø9/19/69  Ø8.24.28.
CMG SYSTEM FAILURE DETECTED
 SPIN CURRENT     * CMG 3 * AV READING=   .Ø37
          CMG FAILED
     MANUAL ASSISTANCE REQUESTED
***********************************************


      CMG SYSTEM CRITICAL FAILURE

CMG SYSTEM SHUT DOWN - RCS SYSTEM ACTIVATED
        REQUEST MANUAL CHECKOUT


 Ø9/19/69  Ø8.28.11.
CMG SYSTEM FAILURE DETECTED
RIGHT BEARING TMP* CMG 1 * AV READING= -5.427
          CMG FAILED
     MANUAL ASSISTANCE REQUESTED
***********************************************
```

Figure 12.- On-line typewriter output for EMMA operation.

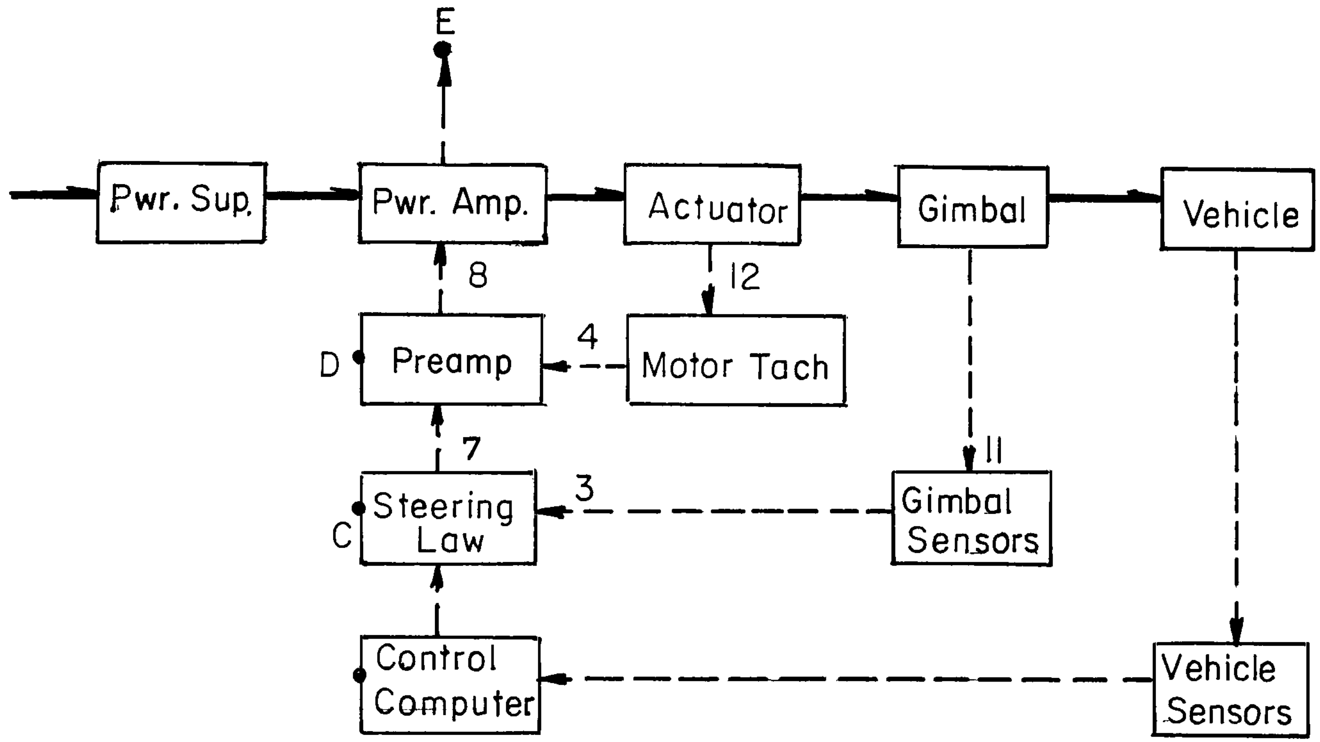


Figure 13.- CMG system maintenance block diagram.

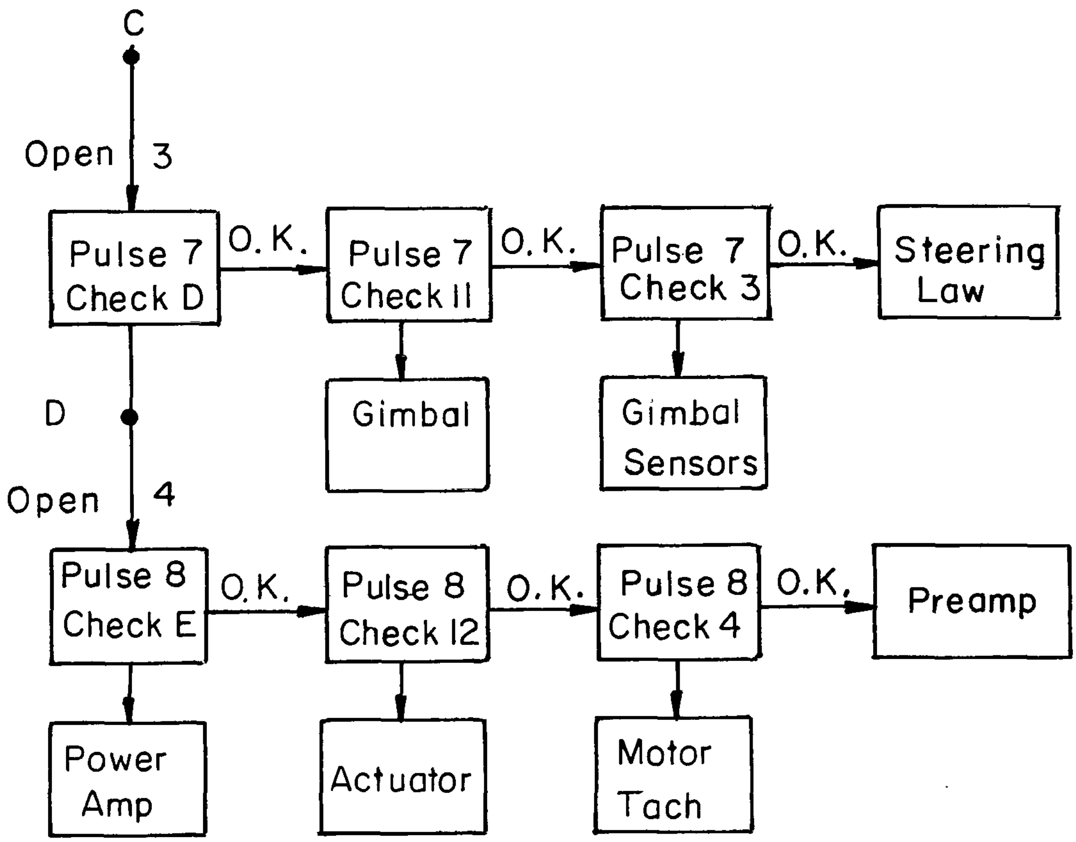


Figure 14.- CMG system diagnostic logic flow.

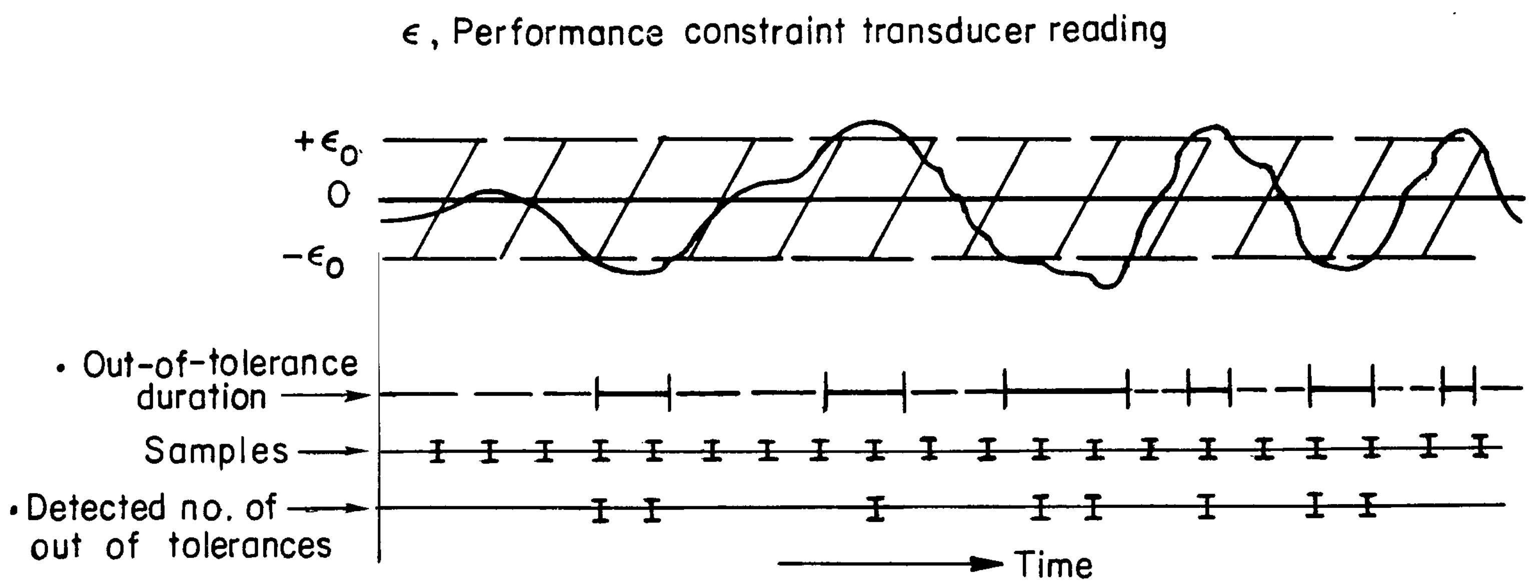


Figure 15.- Out-of-tolerance constraint detection.

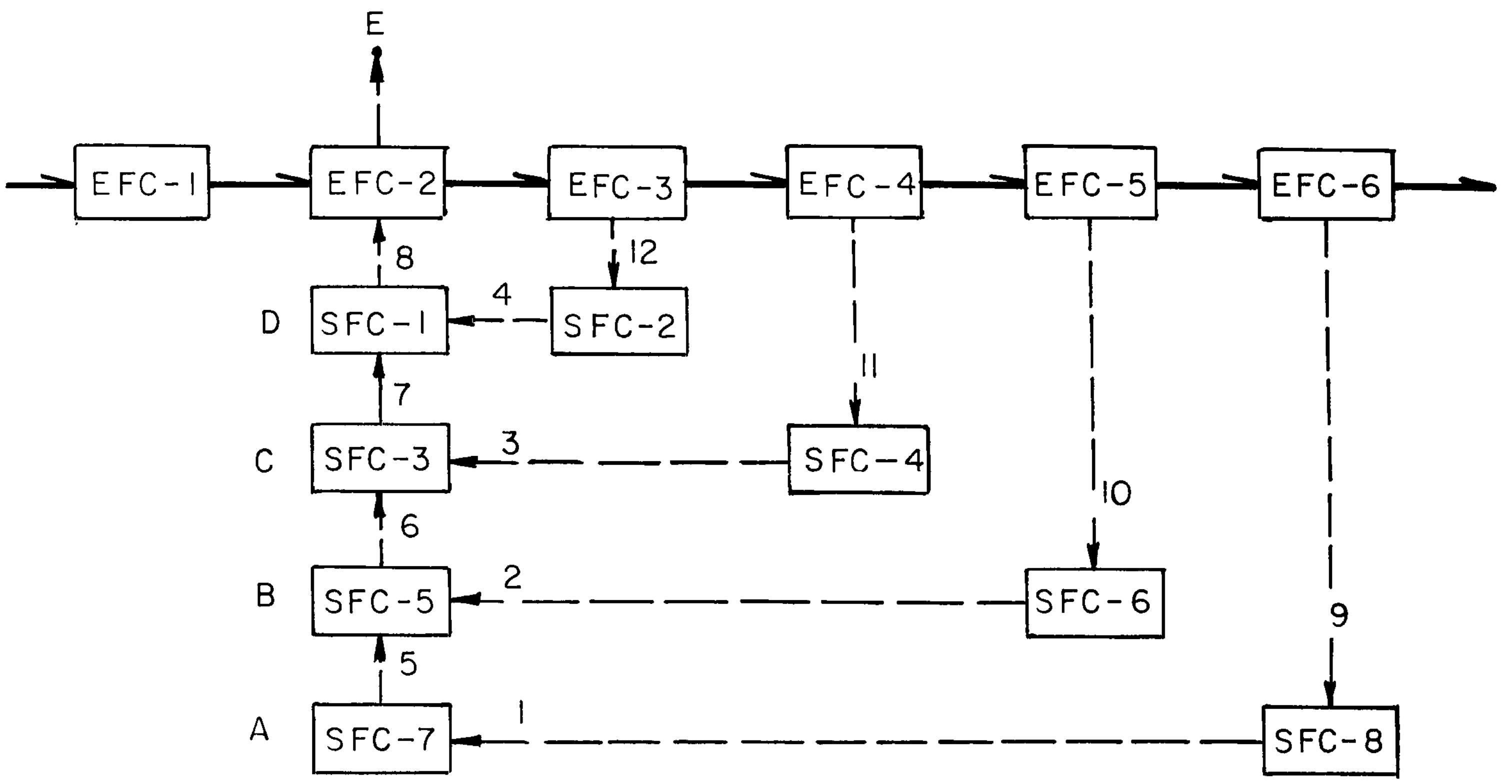


Figure 16.- Spacecraft system maintenance block diagram.

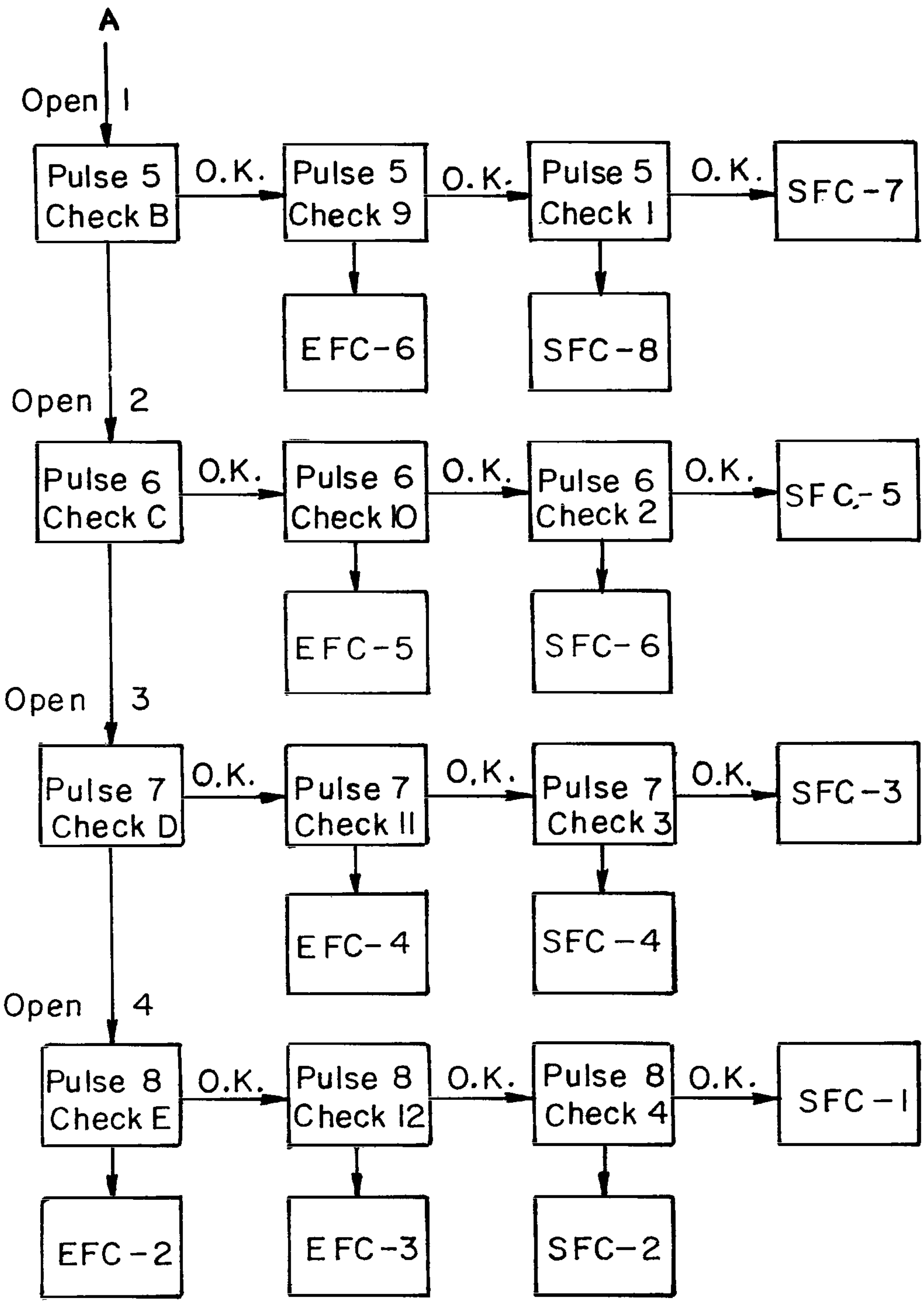


Figure 17.- Diagnostic logic flow.

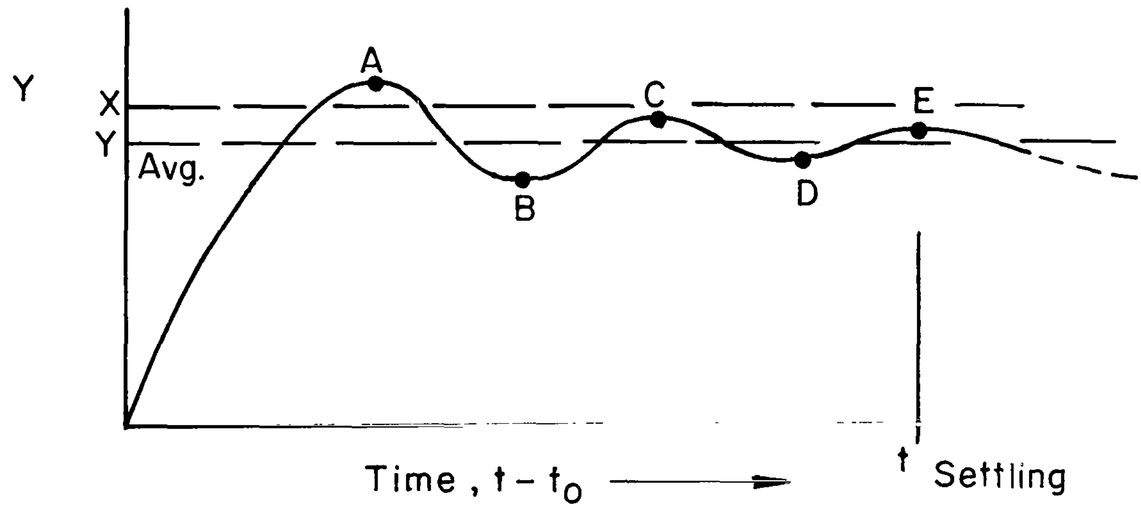


Figure 18.- Characterization of component dynamic and static response.

NASA-Langley, 1970 —— 9 L-6973

"The aeronautical and space activities of the United States shall be conducted so as to contribute . . . to the expansion of human knowledge of phenomena in the atmosphere and space. The Administration shall provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof."

—NATIONAL AERONAUTICS AND SPACE ACT OF 1958

NASA SCIENTIFIC AND TECHNICAL PUBLICATIONS

TECHNICAL REPORTS: Scientific and technical information considered important, complete, and a lasting contribution to existing knowledge.

TECHNICAL NOTES: Information less broad in scope but nevertheless of importance as a contribution to existing knowledge.

TECHNICAL MEMORANDUMS: Information receiving limited distribution because of preliminary data, security classification, or other reasons.

CONTRACTOR REPORTS: Scientific and technical information generated under a NASA contract or grant and considered an important contribution to existing knowledge.

TECHNICAL TRANSLATIONS: Information published in a foreign language considered to merit NASA distribution in English.

SPECIAL PUBLICATIONS: Information derived from or of value to NASA activities. Publications include conference proceedings, monographs, data compilations, handbooks, sourcebooks, and special bibliographies.

TECHNOLOGY UTILIZATION PUBLICATIONS: Information on technology used by NASA that may be of particular interest in commercial and other non-aerospace applications. Publications include Tech Briefs, Technology Utilization Reports and Notes, and Technology Surveys.

Details on the availability of these publications may be obtained from:

SCIENTIFIC AND TECHNICAL INFORMATION DIVISION

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Washington, D.C. 20546