The ALSEP Data Subsystem has been evaluated by an independent contractor to provide added confidence that no allowable sequence of commands can prevent proper operation of the ALSEP System. This report assesses the significance of the failure modes disclosed in this study.

RETURN TO MILLEY

SHARPE IBLS

JAMES

McDONALD

Prepared by: R. Fatka

R. Fatka, Command Decoder
Project Engineer

J. Mansour

J. Mansour, Reliability

Approved by: E. S. VanValkenburg

E. S. VanValkenburg
Engineering Manager

INTRODUCTION

A subcontract study was assigned to VEDA Incorporated to"... to analyze the current design of the ALSEP Data Subsystem to determine if design errors exist which would prevent proper operation of the ALSEP due to a peculiar or unplanned series of operations. In particular, the concern is whether or not logic trains exist in the logic design which can allow the ALSEP to enter an irrecoverable state." (Ref. 1).

Results of this study are documented in Reference 2. In general, it has been concluded that "...under normal conditions the Data Subsystem has no irrecoverable states. There are, however, several abnormal situations which could result in a premature loss of ground control over the ALSEP". (Ref. 2).

The sections which follow contain statements of these abnormal situations as presented in Section 6 of Reference 2 and joint engineering/reliability assessments on the significance of these failure modes along with conclusions.

Situation (a). Failure Modes - Action of timer inhibit command no. 27 (33 OCTAL) would prevent the circuit breaker reset action from occuring should the command receiver trip its circuit breaker.

Discussion. During normal operation, the receiver circuit breaker is automatically energized to the power-on condition by readily available 12 hour timer output pulses. This feature has been incorporated primarily to attempt to restore receiver power in the event a receiver malfunction should cause an extreme receiver overload condition. Even though the restoration of power assumes that the receiver malfunction is self-correcting this feature was incorporated because of the critical nature of the receiver.

As pointed out in Section 4.3 of Reference 2, command no. 27 (33 OCTAL) provides the capability to ignore the timer one minute and 12 hour output pulses. This shut-off capability is intended to be used only for the protection the ALSEP experiment users in the event of erratic timer operation.

Consequently, even though the conditions of situation (a) is recognized, it presupposes the occurance of two serial malfunctioning events: (1) timer malfunction which necessitated the execution of command 27 (33 OCTAL) and (2) a self-correcting receiver malfunction which caused an extreme overload condition. The probability of this occuring is remote.

It is recommended however that the use of command no. 27 (33 OCTAL) be flagged as a critical command in the Operations Manual and that its use be limited only to circumvent an erratic timer operation.

Situation (b). Manual Switching of PCU. - Commands 48 and 50 direct either section of the PCU to be used. Directing the second section be used by command 50 could disable ALSEP if the second PCU section were unknowingly inoperative.

Discussion. The philosophy behind the PCU design was to eliminate single points of failure. The automatic switch-over circuit will cause power conditioner (PC) 1 to turn off and PC2 to turn-on in the event of an over-or-under voltage condition. The automatic switch-over circuit will not switch back to PC1 in the event of an over-or-under voltage. This is to prevent oscillation between PC1 and PC2 in the event of any one of six failures in the switch over circuit.

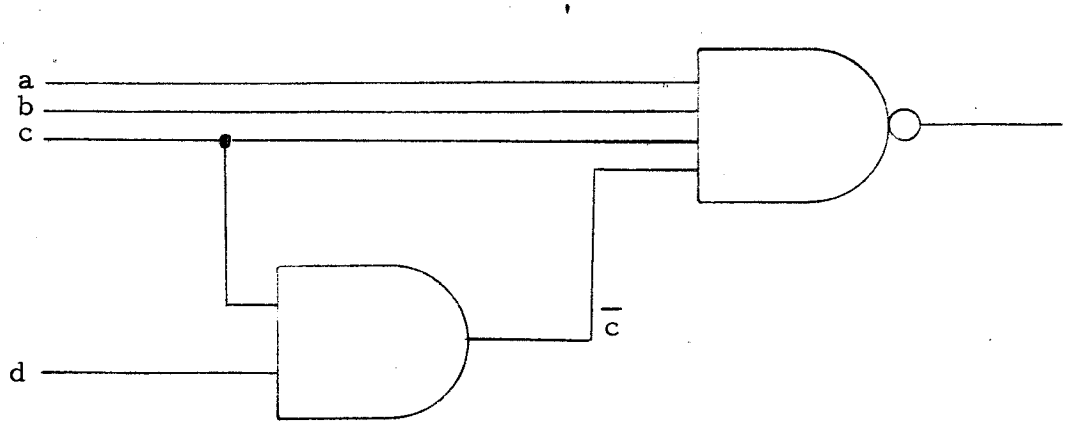
There is no way to determine if PC2 is operational while PC1 is operating or vice versa. The non-operating PC is a redundant circuit which is inactive when the other PC is operating. Therefore it is very important that commands 48 and 50 be used only if the operating PC gives indications of impending failure and/or the automatic switch over circuit does not switch when an over-or-under voltage condition exists. The latter condition could only occur if the regulator in PC1 and the switch over circuit failed.

Situation (c). Failure of Address Memory Flip-Flop. - Both sections of the command decoder would be inoperable if the address memory flip-flop failed in either section.

Discussion. This situation has been thoroughly investigated. As documented in Reference 3, "Several alternate designs were evaluated to determine their effectiveness for eliminating this failure mode. It was concluded the reliability improvement that could be realized was negligible and did not justify the cost, weight, and schedule impact."

Situation (d). Abnormal Generation of Switching Pulse. - Under an unusual combination of logic gate operations a switching pulse could be generated in the loss of threshold reset circuit. This could result in a premature reset occurring preventing either command execution or command verification from occurring.

Discussion. The circuit considered in situation (d) is schematically shown below for discussion purposes.



The point in question is the switching time delay between points c and $\overline{c}$, where $\overline{c}$ is the inverted output of c. As per Fairchild LPDTμL 9042 data sheet, the delay time between the input and output signals are typically 60 nanoseconds and are 150 nanoseconds maximum for devices sinking and supplying current to 10 other logic devices. For one unit load application, as described above, the average delay time is greater than the maximum specified for 10 unit loads.

The situation described is therefore not a potential problem area because 150 nanoseconds delay is more than sufficient to guarantee proper operation.

Situation (e). Inhibit of Reset. - A decoder programmer failure occurring between counts 43 and 63 prevents normal reset. As a result the alternate decoder section is continually locked-out of use.

Discussion. As stated in Section 5.4 of Reference 2, this type of failure is peculiar primarily to the first six stages of the programmer counter and is a function of the operational state of the command decoder. That is, the following exact sequence must occur before this failure mode could occur.

1. The programmer counter must be operational at the time a proper address is detected.

2. The counter must function normally between counts 29 and 43.

3. First six stages of counter and/or associated drive logic must malfunction prior to count 63 (20 msec interval).

A cursory analysis by ALSEP reliability pertaining to the conditional probabilities stated above indicate the probability of the failure mode occurring is extremely remote. In addition the criticality of the failure mode with respect to loss of uplink command capability (as defined by reference 3) is negligible.

Failure of count 63 gate in the high state will not produce the referenced failure mode unless the counter is also inoperative.

Situation (f). Loss of Threshold. - Should a loss of threshold occur during a command execution, the command will continue to be executed until the threshold is restored. This could be detrimental to user logic or create an abnormal power demand.

Discussion. The situation described cannot occur and was reported because of an error in the command decoder logic diagrams (2332973, shts 2 and 5). This potential problem was discovered during the development of the command decoder brassboard model and has been corrected on all subsequent models. Unfortunately the logic diagram error was not discovered until after the VEDA review. Refer to CRD 51097 for change description.

Situation (g). Uncertainty of Enable Flip-Flop State. - The data processor shift pulses enable flip-flop (in the command decoder) can start-up in either state. Because this flip-flop can only be reset by the data processor, certain data processor malfunctions can disrupt the operation of the command decoder.

Discussion. Discussions pertinent to the data processor interface failure modes, presented in Section 5.4 of Reference 2, are summarized in Table 1.

Failure modes 1 through 5 represent conditions which allow the command decoder to successfully process and execute commands. The command verification capability is either disabled or operable depending upon the type of failure. (See Table 1).

BxA concurs with VEDA relative to failure mode #6 which results in the loss of uplink command capability*.

This would occur as a result of either of the following failures.

1. Open circuit in DP/CD interface harness.

2. Failure of CVW flip-flop or output inverter in either data processor.

This failure mode will be included in the forthcoming update of the FMECA document (Reference 3). The probability of occurrance will be combined with documented failure modes causing the same system effect (e.g., loss of command receiver, demodulator, diplexer filter). However, its criticality is anticipated to have a negligible effect.

In the event a harness failure occurred, the failure effect, as stated, would be correct. However, if this failure occurs in the data processor, an operational procedure can be implemented which will circumvent the loss of uplink command capability. Should the data demand signal fail high while the command decoder is in the search mode or actively processing a command, the capability of executing one or two additional commands exists. This capability will permit commanding of the DP to be switched to the redundant side, thus clearing the problem.

* NOTE: This failure will not cause system abort.

In order to effectively implement this procedure, monitoring of the command verification word (CVW) would be required prior to processing an uplink command.

Under normal operation the CVW will be either:

1. Present after the execution of a command.

2. All "0" in the event the command was executed but Data Demand did not occur.

3. All "0" when the CD is in the search mode.

In the malfunctioned state, random data will be present in the CVW, regardless of the operational states of the CD. Therefore, by implementing an operational procedure to switch DP's when the CVW is either incorrect or not all "0"s, the loss of uplink command capability can be circumvented.

CONCLUSIONS

This Bendix assessment on failure modes associated with mission commands for the Data Subsystem indicates no requirement for design changes however certain precautions should be exercised prior to using certain commands and an operational procedure is required to recover control in event of malfunctions in the data processor. Therefore, the following actions are recommended.

1. Inform Apollo Operations (MCC-H) of the criticality of commands no. 27, 48, and 50.

2. Prepare an operational procedure for recovering from data processor malfunctions.

3. Compare the probability of loss of command capability resulting from conductor malfunction in the harness, CVW flip-flop failure or output inverter failure with other non-redundant parts in the up-link and document this in the next issue of the FMECA.

TABLE 1. Data Processor Interface Failure Mode Summary

Failure Mode Condition	Data Processor Interface Failure Mode			Effect on Command Decoder
	Shift Line (SL1ZN)	Data Gate (DG1ZP)	Data Demand (DD1ZP)	
1	Fails HI or LOW			CD will be capable of processing commands via either redundant section but command verification will be lost. Assuming failure in DP - command verification can be restored by commanding DP to redundant side. Assuming failure in DP/CD harness - command verification capability is lost.
2		Fails LOW before leading edge of data demand time		Same effect as 1.
3		Fails LOW during the 9.4 msec data demand time		CD section in operation at time of failure can process and execute subsequent commands between data demand times, but with loss of command verification. Redundant CD section can process and execute subsequent commands with the loss of command verification. Assuming failure in DP - command verification can be restored by commanding DP to redundant side.
4		Fails HI anytime		Same effect as 1, however, partial loss of command verification words.
5			Fails LOW during a data demand time	Same effect as 1.
6			Fails HI anytime	Disables both sections of the command decoder. (See discussion).

REFERENCES

1. Statement of Work for Verification of the ALSEP Data Subsystem Logic Design, Bendix Aerospace Systems Division, SWA-070, 29 March 1967.

2. Review of the ALSEP Data Subsystem Logic Operation, Report No. V0502U/3.516-05, VEDA Incorporated, Ann Arbor, Michigan, 19 May 1967.

3. ALSEP Failure Mode, Effects, and Criticality Analysis, ATM-501, 1 January 1967, Pg. 2.2-7.