Array E Uplink

Redundancy Method Justification

This ATM provides the reliability justification for the redundancy method employed in the Array E uplink. The Array E uplink employs standby redundancy without cross-over and automatic switch-over after 61 hours in the event of uplink failure.

Prepared by: R. J. Dallaire
R. J. Dallaire
ALSEP Reliability P. E.

D. J. Thomas
D. J. Thomas
ALSEP Systems Engineering

Approved by: S. J. Ellison
S. J. Ellison
ALSEP Reliability Manager

I Introduction

The Array E Uplink consists of a Receiver, Demodulator, Decoder, and Output Gates in standby redundancy. Switchover is accomplished by ground command or automatically within 61 hours after loss of uplink control (122 hours in slow bit rate). This redundancy approach differs from the previous designs and from the ELLSEP study design. This ATM will provide the reliability justification for the standby redundancy method and the lack of cross-strapping to the Uplink selected for the Array E design..

II Background

The difficulty associated with the implementation of redundancy in the command receiving and decoding portion of any system is inherent in the function of the subsystem itself. A failure in the downlink may be easily circumvented by a ground command to switch in the redundant element. A failure in the uplink usually cannot be rectified by ground command to the redundant side because the uplink itself has failed.

One method of handling uplink redundancy is to sense the failure and to switch over to the redundant unit automatically. The problem with this method is that single point failure modes cannot be avoided. Sensing a failure often requires very complex circuitry which may itself cause the uplink to fail.

III Three Methods of Uplink Redundancy

Method 1

The earlier ALSEP's employed partial active redundancy in the uplink, with automatic output selection from redundant receivers and cross-inhibiting of redundant digital decoders; the demodulator and command output gates were common to both channels. There were several potential sources of single point failure. The Reliability Block Diagram is shown in Figure 1. The probability of failure for this partially redundant system is 5.74% for two years of lunar operation.

Other than the single thread demodulator and output gates, in which every part is a single point of failure, the cross-inhibiting in the redundant digital decoders is also a single point of failure which could not be removed by making the demodulator and output gates redundant.

Method 2

To improve the reliability of the uplink for Array E, the ELLSEP study proposed a completely redundant uplink and dual cross-inhibitors to eliminate single point failures. One half of the dual cross inhibitor is shown in Figure 2.

The dual cross-inhibitor eliminated the single points of failure in the cross-inhibitor itself but did not remove the single point failure of the decoder not generating a command reset and thus locking out the good decoder. A SPF was added by the dual cross-inhibitors with the address detector gate G15 indirectly causing false executions in the presence of uplink noise.

The probability of failure of the ELLSEP uplink design is calculated to be 0.220%. It has 5 SPF's. The Reliability Block Diagram is shown in Figure 3.

Method 3

For Array E the preferred method is to have two completely redundant uplink channels, with the minimum of cross-linking. The only common points are the RF input to the redundant receivers, and the wire OR'd outputs of the redundant command gates. Only one uplink channel is powered at any time, for the following reasons:

1.0 In general with active redundancy a fault in one output can override the other output and produce an overall single point failure of the system. The probability that any output gate will by itself fail in this manner is low; however, each output gate is at the end of a chain of logic elements, each of which produces a phase reversal. In the limit a random failure in either direction, anywhere in a chain has a 50% chance of producing an overall false output. Two active redundant channels, each of which

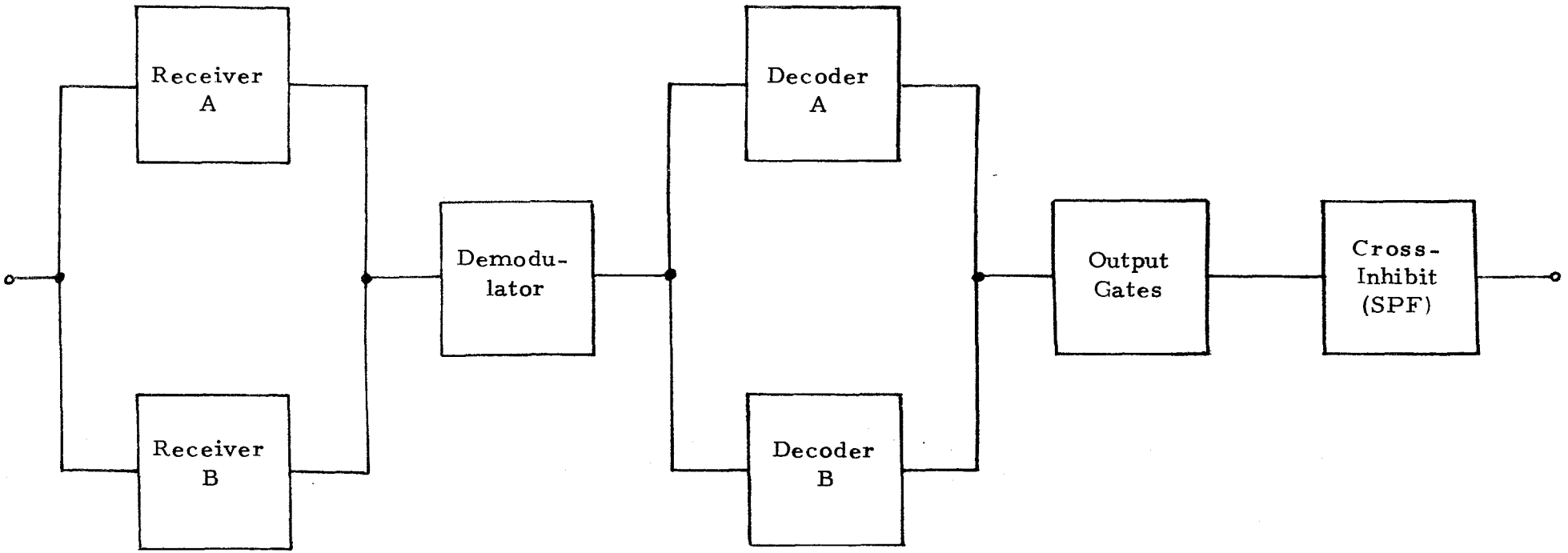

Figure 1 Array A Uplink Reliability Block Diagram

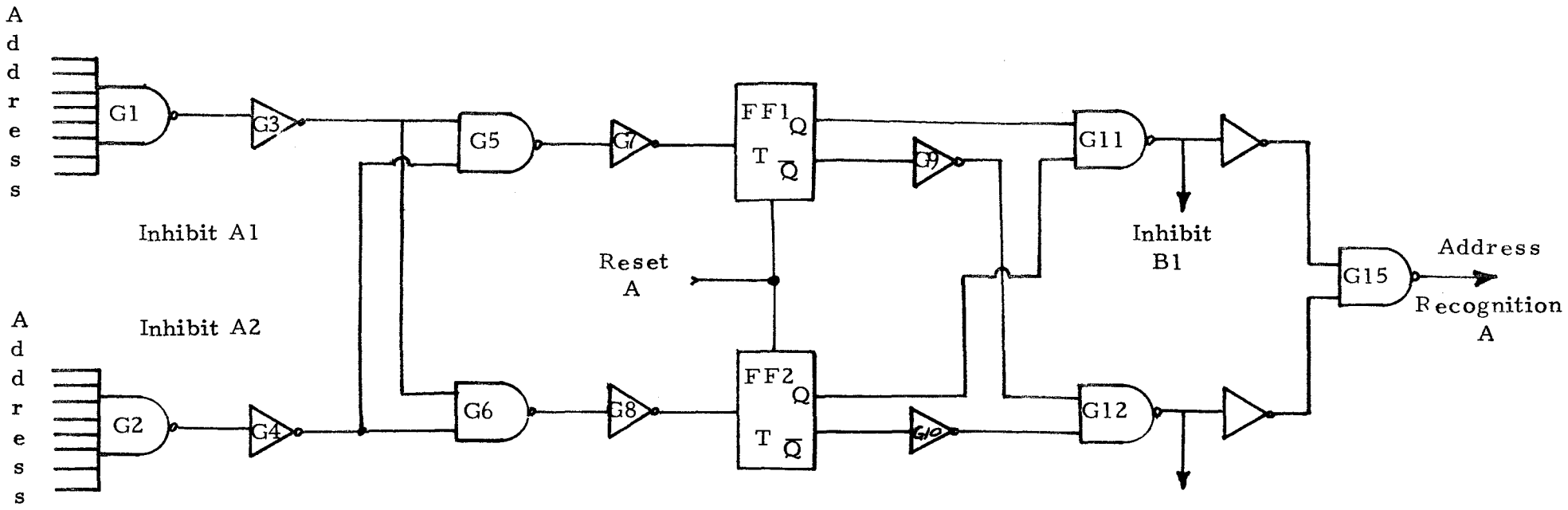

Figure 2 One of the Two Cross-Inhibit Circuits

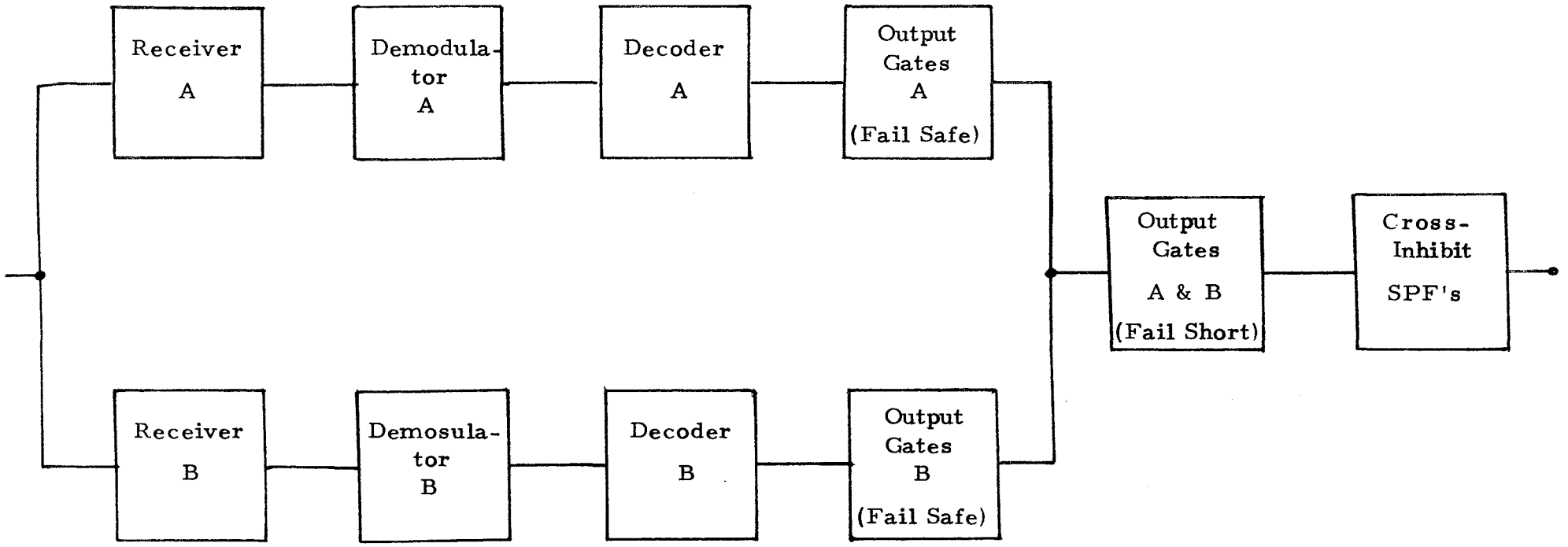

Figure 3 ELLSEP Uplink Reliability Block Diagram

has a 50% chance of failing the whole system, have in combination no greater reliability then either channel by itself. In order to obtain the maximum possible reliability from redundant uplinks one of them must be run in standby. Standby redundancy removes the need for cross-inhibiting.

The standard logic chip in Array E is the TTL 54L type, with which active wire OR'ing is not permitted but standby wire OR'ing is. Standby wire OR'ing provides a fail-safe redundancy technique; only transistor Q4 in Figure 4 shorting collection to emitter will cause the loss of the command by shorting the signal to ground. The probability of this failure is only one thirteenth of the failure probability of the output gate instead of 50% of all the gates controlling the output gate.

Standby redundancy roughly halves the power required for uplink operation. Strictly, only the OR'd output stage must be in standby in order to obtain the increase in reliability, but there is little point in leaving the preceding stages of the standby channel powered if they are not effective.

2.0 Having established the necessity of standby redundant operation it is then necessary to ensure that if the uplink channel in use fails then the standby channel will be brought into operation immediately, or within a reasonable time. The switchover system must be entirely automatic and must be incapable of being permanently inhibited by command--failures occur at random and could occur at a time when the automatic system had been inhibited.

The overall purpose of each uplink channel is to provide command pulses on the command lines in response to transmissions from MSFN; the only valid criterion for uplink failure therefore is that command pulses are not being received. It has been suggested that the Motorola receiver threshold signal could be used in some way but that is not an acceptable approach, for the following reasons:

2.1 The receiver threshold signal is not affected by failures in the remainder of the uplink channel and is not therefore an overall performance monitor. If Receiver "A" is good, but Demodulator "A" and/or Digital Decoder "A" has failed, then the complete system has failed.

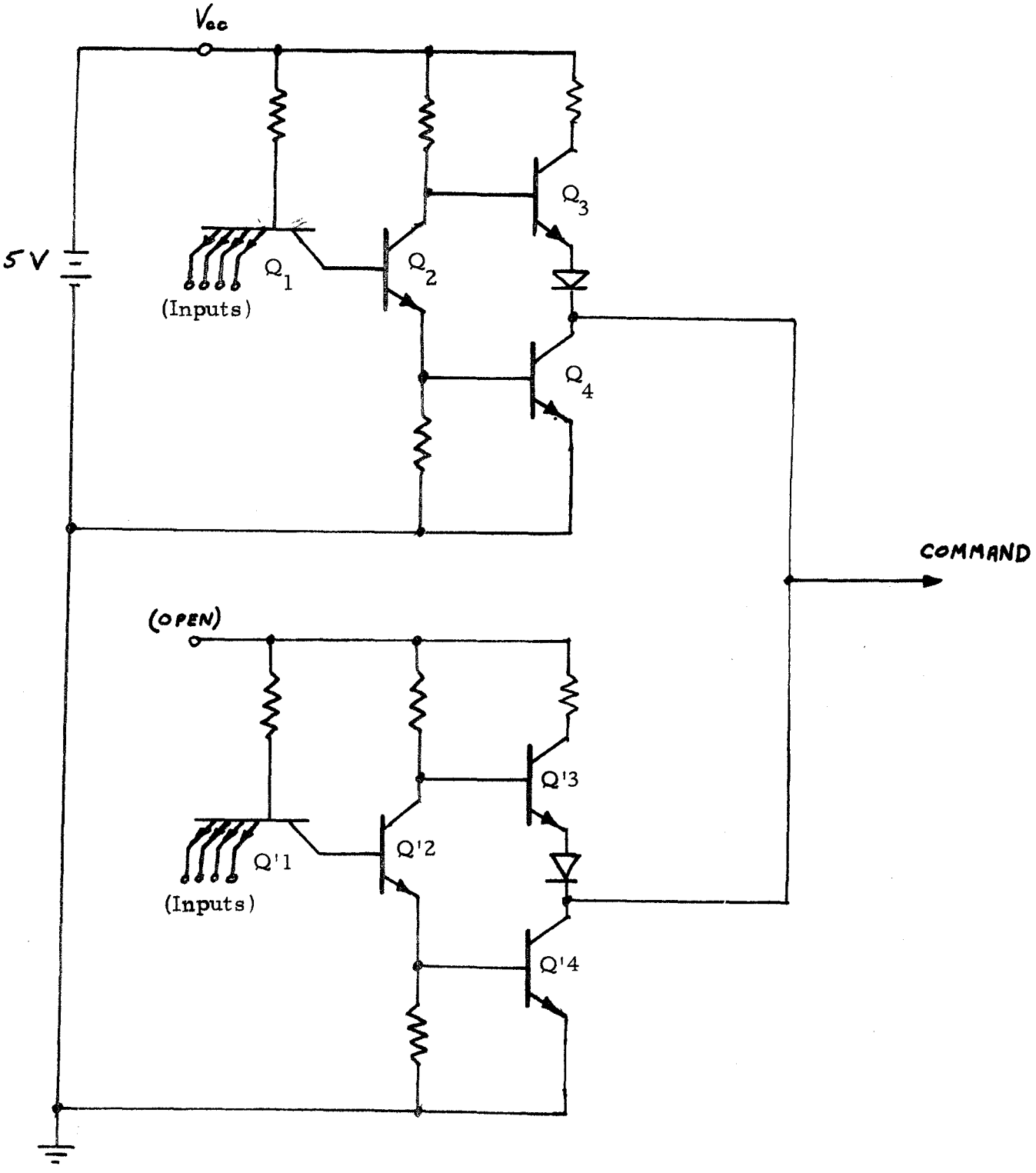

Figure 4 TTL "Wire ORed" Output Configuration

2.2 The method of "If A, then A; if not A, then B" used in the dual receiver is a potential single point failure. If 'A' fails so as to produce enough noise in the 1 kHz region to activate the threshold switch then the system could be locked up to a meaningless input.

2.3 The uplink carrier and modulation are not continuous, which means that power would be switched from one channel to the other every time a command was sent to Array E or any other ALSEP - perhaps 15,000 to 50,000 switchings in two years.

3.0 The difficulty in using lack of command pulses as the switching criterion is that ALSEP has no independent indication that a command has been transmitted, and it therefore has no positive means of detecting that an uplink failure has occurred. The only acceptable approach is to switch from one uplink to the other at predetermined intervals unless a specific command has been received in the intervals inhibiting each switchover. A 'specific' command, rather than 'any' command, is used because for practical reasons the latter method would require monitoring of the common execute enable output, which is a potential single point failure.

4.0 The source of the uplink timing signal must be reliable and the period must be convenient from the operational point of view. Regularly occurring natural phenomena such as the twice per cycle brightness and/or thermal variations associated with each lunation are reliable timing signals, but two weeks is too long a period. A period of 48 to 72 hours was selected as a reasonable compromise which inevitably means some form of clock internal to the Central Station. Previous unsatisfactory experience with mechanical timers, and the complication of the RSST, led to a completely new approach, concentrating heavily upon simplicity, with consequent reliability. Unless the estimated failure rate of the switching device is many times smaller than the estimated failure rate of either uplink channel, the full potential increase in uplink reliability cannot be obtained.

5.0 The possible sources of the basic clock signal were the uplink, the downlink and, if neither of these was satisfactory, an independent oscillator.

6.0 The uplink clock was rejected for the following reasons:

6.1 Failure of the phase lock oscillator in the uplink in use could simultaneously block commands and stop the switchover counter - a single point failure.

6.2 The slowest pulse repetition rate from the Command Decoder is considerably faster than the lowest PRF from the Data Processor, necessitating more counter stages, with lower reliability.

6.3 The exact frequency is known only when the phase-lock loop is locked to ground transmissions; predicting switchings with any accuracy would be impossible.

7.0 The Data Processor downlink clock was found to be completely satisfactory:

7.1 The lowest PRF is once per 54 seconds - the 90th Frame Pulse - requiring only 12 counter stages to generate a 61-hour switching period.

7.2 The frequency is crystal controlled to within ±0.01%, allowing precise switching predictions to be made.

7.3 The 90th Frame Pulse outputs from the standby redundant downlinks are OR'd into the uplink counter, so that it should continue to operate as long as one downlink clock is serviceable. If both downlink clocks fail the counter will stop, but this is unimportant as the system will in any case be effectively dead as far as MSFN is concerned.

8.0 The final point to decide was whether the uplink switch counter should be single or redundant. A single counter was chosen. Since a single counter and uplink switch circuit comprises only three 4-stage counter chips, two flip-flops and ten gates - 8 logic chips in all - it has an extremely high predicted reliability, more than sufficient to obtain the full potential reliability of the redundant uplinks. The counter is not a single point failure, in that both the counter and an uplink channel must fail before uplink is permanently lost. Finally, if redundant counters are used, the full potential reliability cannot be obtained without the occurrence of the usual problems of active/active and active/standby operation, with consequent circuit complications and individual reductions in reliability.

9.0 In operation the uplink switch counter is set to a predetermined starting condition by the initial application of power to the Central Station and from then on runs continuously. It cannot be reset or controlled in any way by the MSFN. Every 61.8 hours it produces an output pulse, and unless this has been specifically blocked by command Octal 174 sometime during the preceding 61 hours an uplink change will occur. The flip-flop which "remembers" that Octal 174 has been sent is reset back to the 'switchover enable' condition after each switchover pulse, whether or not a switchover was actually permitted to occur. Even if an uplink is known to have failed there is no facility by which the remaining good uplink can be locked into permanent operation except by sending Octal 174 at least once per 61 hours. This is deliberate - the capability of permanently locking to one uplink or the other would invalidate the overall uplink reliability predictions. Multiple transmissions of Octal 174 have no further effect on the system than a single transmission, i.e., successive transmissions do not cause a toggling action or the inhibition of more than a single switchover. The memory flip-flop can be reset only by the counter, once per 61 hours.

10.0 An additional uplink control command, Octal 122, causes an immediate uplink switch, overriding Octal 174 even if Octal 174 is being activated continuously. This is necessary in order to overcome a potential single point failure, by which a group of commands including Octal 174 could be permanently activated, partially disabling ALSEP and preventing an automatic changeover. Octal 122 is routed through the decoding gates as widely separated as possible from Octal 174. This ensures that a single point failure cannot fault both commands and prevent an automatic changeover.

11.0 The Reliability Block Diagram for the Array E design is shown in Figure 5. The probability of failure is 0.085%.

IV Conclusion

Table 1 below demonstrates that the reliability of the Array E system is superior to the proposed ELLSEP design. The improvement in reliability justifies the trade-off of not having uplink control for 61 hours in the event of a failure.

TABLE 1

TWO YEAR UPLINK RELIABILITY COMPARISONS

	ELLSEP	ARRAY E
Failure Probability (Two Years)	0.220%	0.085%
Number of Single Point Failures	5	2
Probability of Single Point Failure	0.074%	0.002%

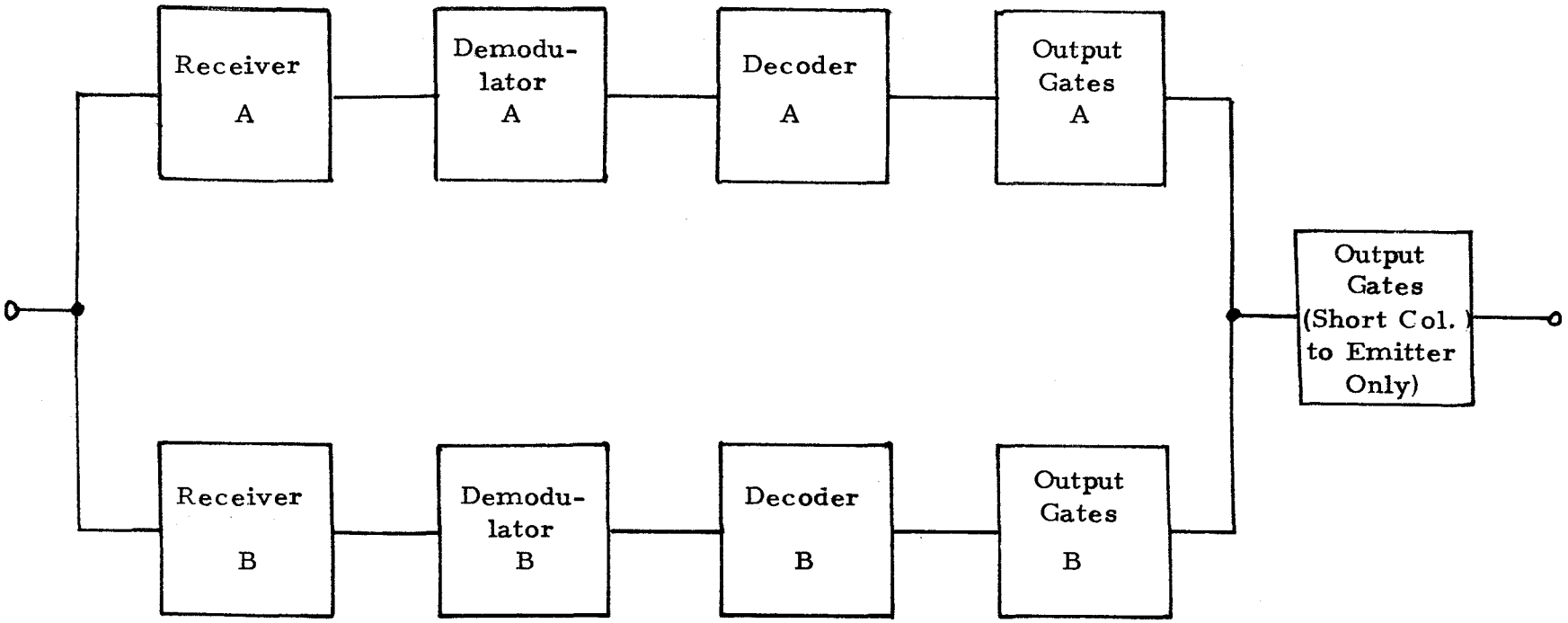

Figure 5 Array E Uplink Reliability Block Diagram