REDUNDANCY SWITCHING ANALYSIS

Practice:

To verify that the failure of one of two redundant functions does not impair the ability to transfer to the second function, a rigorous failure modes, effects, and criticality analysis (FMECA) at the piece part-level is performed for all interfacing circuits.

Benefits:

By using a systematic method to assure the switching functionality of designed-in redundancy, the long-term performance of complex systems can be assured.

Programs That Certified Usage:

Voyager, Galileo, Magellan

Center to Contact for Information:

Jet Propulsion Laboratory (JPL)

Implementation Method:

Redundancy switching analysis (RSA) is a subset of the general FMECA process, but it is performed in greater detail because of its criticality. RSA includes the following steps:

1. Identify and diagram all functional blocks which involve the two redundant elements.

2. Expand the functional blocks to show the interface circuitry at the piece part level.

3. Postulate all credible part failures (viz, shorts, opens, saturated high or low, etc.) and determine the effect on the functional redundant path. Verify design compliance with the following objectives:

    a. Hardware failures do not propagate across inter-unit interfaces to produce hardware failures in other units.

    b. There is sufficient isolation that the postulated failure does not produce a functional failure capable of disturbing the transfer to, or operation of, the redundant function.

Technical Rationale:

There have been numerous instances of presumably redundant systems which have failed to successfully transfer to the backup path when the primary path is non-

REDUNDANCY SWITCHING ANALYSIS

functional. A rigorous, systematic search could have foretold the failure and, through design change, averted the problem.

The first objective-- preventing failure propagation-- is of most value in a repairable system. Non-propagation minimizes the number of units requiring repair. In spacecraft, this would correspond to the preflight phases of either subsystem or system testing. The key to this investigation is a complete diagram of the involved interface circuits which penetrates each unit to a circuit depth sufficient to prove that no possible failures in Unit 1 can propagate to become irreversible hardware failures in Unit 2. The second key ingredient is a complete list of part or assembly failure modes for hypothesis.

The second objective-- guaranteeing successful transfer (or equivalently independence of the primary and back-up functions)-- is a necessity for either repairable or non-repairable systems and requires the same complete interface diagram and complete list of failure modes. The list includes such items as:

- Part failure (viz, opens, shorts, "stuck-ats"),
- Single event effects (viz, latch-up, transfer), and
- EMI (viz, latch-up, transfer, overvoltage).

These last two items are critical since they can effect both sides of a redundant pair.

Figures 1 and 2 are illustrations of the process of a redundancy switching analysis for several typical interfaces.

Impact of Non-Practice:

The long-term survival of complex systems is usually achieved through the practice of design redundancy. There are often unforeseen deficiencies in the redundancy switching which result in non-independence, thereby defeating the intent.

Failure to use this practice will very probably result in several instances of defective switching in a complex system such as a spacecraft. Experience has shown that initial designs have about a 10 percent chance of non-independence. Just one such defect reduces a presumed redundant system to a single channel system with its inherently shorter life expectancy.

References

1. Polovko, A.M. (1968). Fundamentals of Reliability Theory, (Chapter 5-4). New York: Academic Press, Inc.

2. Feduccia, A.J. (1993). Reliability Engineer's Toolkit. Griffiss Air Force Base, New York: Rome Laboratory.

REDUNDANCY SWITCHING ANALYSIS

Observation

If the postulated short exists and source A is unpowered, its "off"-state load resistance must be high compared to the "on"-state source resistance of source B to assure that adequate VA voltage will be received at LOAD A. If not, the diodes must be made series redundant.

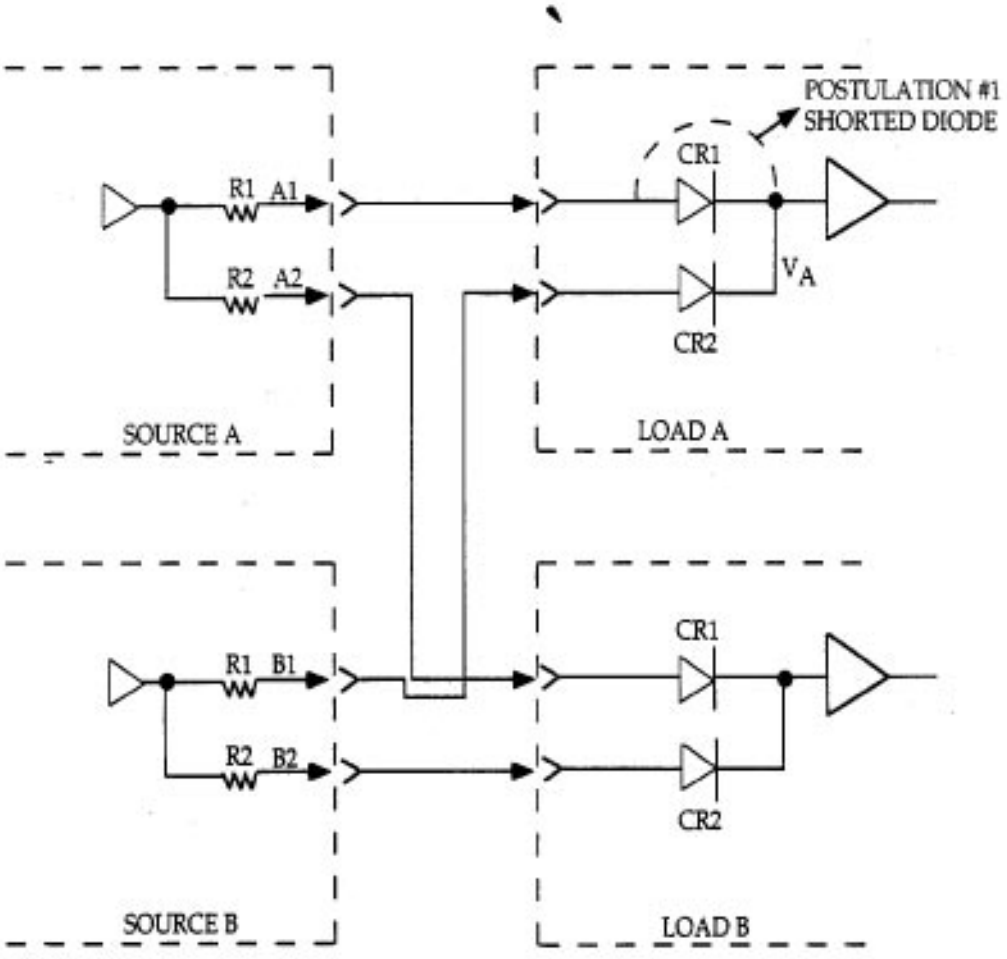

Figure 1.

Example of Passive Redundancy Switching for Cross-Strapped Dual Sources and Dual Loads

REDUNDANCY SWITCHING ANALYSIS

Observation

If the postulated short exists, the isolation resistor R1 must be large compared to the output source resistance of amplifier A1 to assure that adequate VB voltage is received at LOAD B.

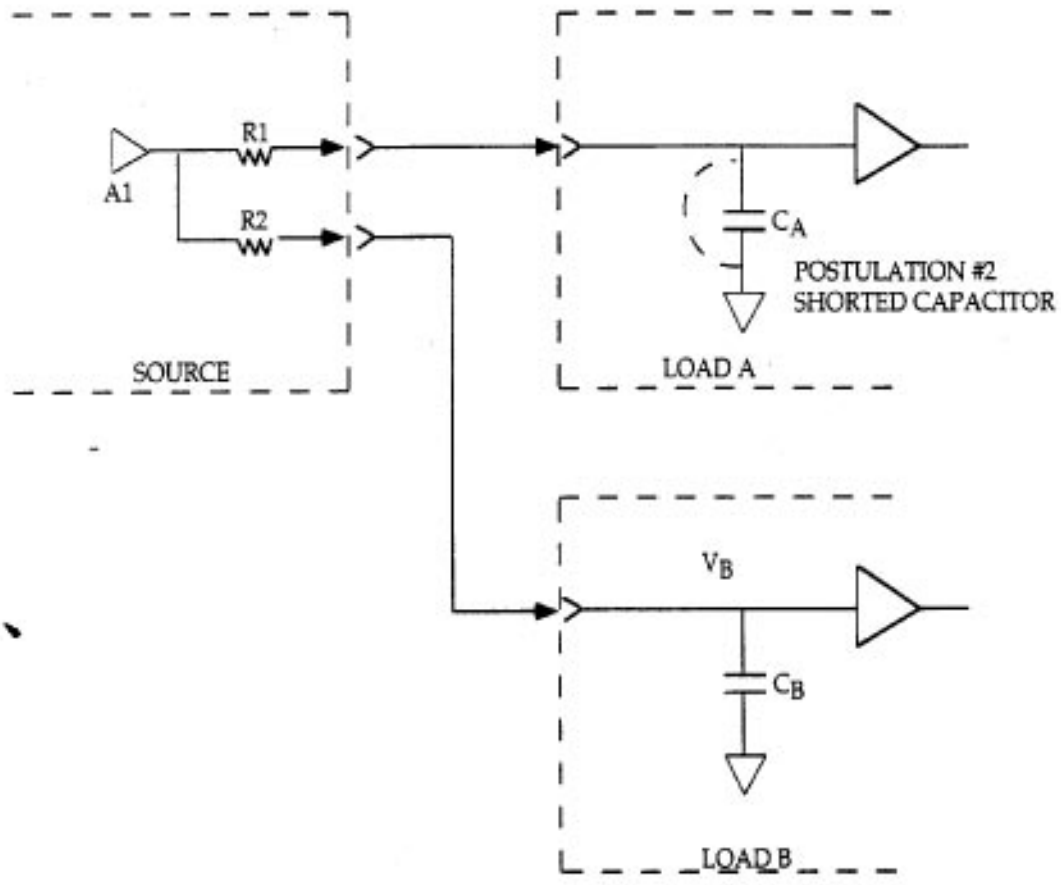

Figure 2.

Example of Passive Redundancy Switching for Single Source and Dual Load