PREFERRED
RELIABILITY
PRACTICES

SNEAK CIRCUIT ANALYSIS GUIDELINE FOR ELECTRO-MECHANICAL SYSTEMS

Practice:

Sneak circuit analysis is used in safety critical systems to identify latent paths which cause the occurrence of unwanted functions or inhibit desired functions, assuming all components are functioning properly. It is based upon the analysis of engineering and manufacturing documentation. Because of the high cost of a sneak circuit analysis, it should be conducted only in areas where there is a high potential for a hazard.

Benefit:

Identification of sneak circuits in the design phase of a project prior to manufacture can improve reliability; eliminate costly redesign and schedule delays; and eliminate problems in test, launch, on-orbit, and protracted space operations. Sneak circuit analysis can also be beneficial in identifying drawing errors and design concerns.

Programs That Certified Usage:

Redstone, Apollo, Skylab, and Shuttle.

Center to Contact for More Information:

Marshall Space Flight Center (MSFC)

Implementation Method:

Some of the devices and equipment benefiting from hardware sneak circuit analysis are solid state electronic devices, relay logic systems and digital systems. The relay equipment includes associated items such as: resistors, capacitors, single load devices, diodes, switches, integrated circuits, and other semiconductors. Another type, analog equipment, includes amplifiers, inverters, converters, and feedback systems. Sneak circuit analysis is an effective tool for locating potential problems in software, and for identifying potential drawing errors and design concerns.

Sneak circuit analysis is a labor intensive technique which requires specialized training and is often limited to those areas of a design where safety compliance is an issue. When considering sneak circuit analysis as an applicable tool to be applied to a program, the following considerations are recommended:

SNEAK CIRCUIT ANALYSIS GUIDELINE FOR ELECTROMECHANICAL SYSTEMS

1. Reasons for conducting a sneak circuit analysis:
   a. Improve reliability which results from the identification and resolution of system problems.
   b. Conduct an independent analysis of the design.
   c. Locate unresolved system problems that could not be found by other analyses or tests.
   d. Identify high criticality items (crew and mission-critical).
   e. Respond to a high change rate in baseline design.

2. Applicable systems:
   a. Systems which perform active functions.
   b. Electrical power distribution and controls.
   c. Computer programs which control and sequence system functions.

Sneak circuit analysis can be implemented on a limited subsystem, a complete functional system or a complete vehicle or program. Analysis is based on documentation in the form of "as built" schematics, drawings, wire lists and "as coded" source computer programs. The preferred start time to begin sneak circuits analysis is during the engineering development phase prior to Critical Design Review (CDR), but sneak circuit analysis can be performed during any phase of the program. The analysis cannot be completed until the overall program/project drawings are baselined. Performing sneak circuit analysis during the last phases of the program tends to drive program costs up because of the potential redesign effort. The effects of making a change later in a program are illustrated in Figure 1.

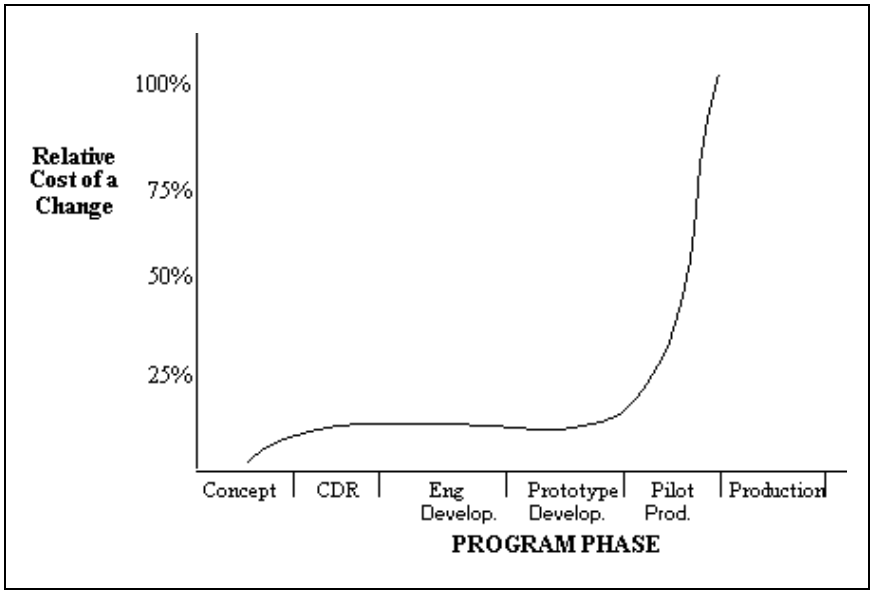

Figure 1. Relative Change Costs Versus Program Phase

SNEAK CIRCUIT ANALYSIS GUIDELINE FOR ELECTROMECHANICAL SYSTEMS

The data used for sneak circuit analysis must represent the system circuitry as built, contingent upon quality control checks, tests, and inspections. The technique for sneak circuit analysis requires the analyst to accumulate detailed circuit diagrams and wire lists, arrange circuit elements into topological network trees, and to examine these network trees for suspected sneak circuits.

After the topological trees have been produced, the next step is to identify the basic topological patterns that appear in each tree. The five basic topological patterns are: (1) the single line (no-node), (2) the ground dome, (3) the power dome, (4) the combination dome, and (5) the "H" pattern. These topological patterns are illustrated in Figure 2. The "PWR" represents electrical power, "S"=switching element, "L"=electrical load, and "G"=ground. The "H" pattern usually

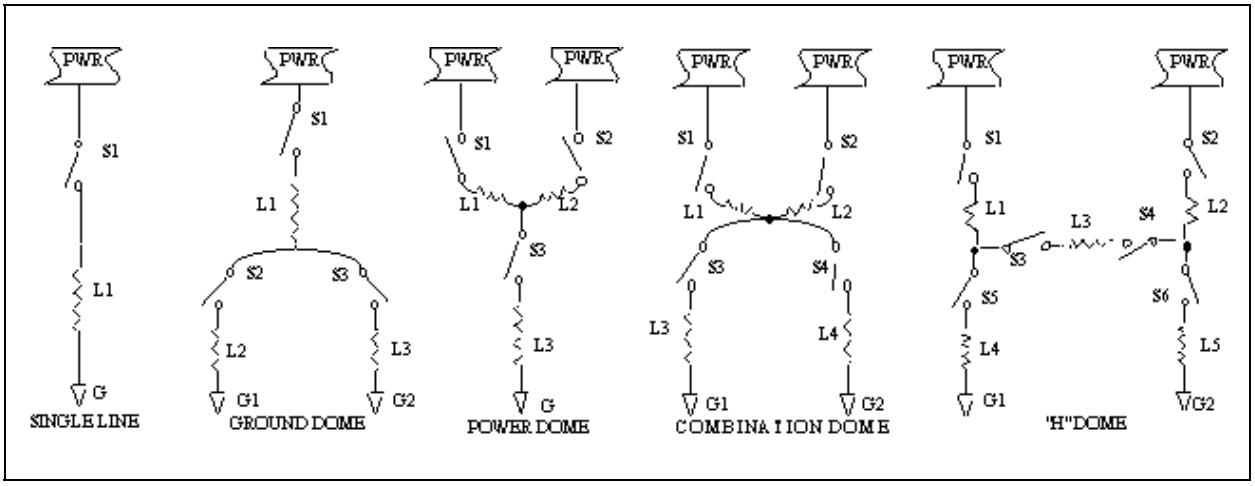

Figure 2. Basic Topographs

has the highest incidence of problems due primarily to the higher number of power sources, returns, loads, and switches. The problems normally occur in the "H" crossbar, which includes L3, S3, and S4. This can result in power reversals, ground reversals and current reversals. As the analyst examines each node in the network tree, the analyst must identify which pattern or patterns that node is part of and apply the basic clues that have been found to typify sneak circuits involving that particular pattern.

Associated with each pattern is a list of clues to help the analyst identify sneak circuit conditions. The clues are questions that the analyst must ask about the circuit in question. The clue list becomes longer and more complicated with each successive topograph. The clue list for the "H" patterns includes more than 60 clues. Almost half of the critical sneak circuits can be attributed to the "H" pattern so this pattern should be analyzed very carefully. (Depending upon contract provisions, the developed clues may be proprietary to the performing contractor.)

SNEAK CIRCUIT ANALYSIS GUIDELINE FOR ELECTROMECHANICAL SYSTEMS

Sneak conditions are classified into four basic types:

1. Sneak paths - which cause current to flow along an unexpected route.
2. Sneak timing - which may cause or prevent the activation or inhibition of function at an unexpected time.
3. Sneak indications - which may cause an ambiguous or false display of system operating conditions.
4. Sneak labels - which may cause operator error through inappropriate control activation.

When a suspect sneak condition is identified, the analyst should verify that the circuit is valid. The circuit should be checked against the latest drawings, revisions, as-built documentation and equipment; and operational information should be reviewed concerning the system in question. Upon verification of the sneak condition, a sneak circuit report should be written which includes the drawings, an explanation of the condition, system level impact, and a recommendation for correcting the sneak circuit. Software sneak analysis should be used to discover program logic which causes one of the four sneak condition types.

During the sneak circuit analysis, unnecessary or undesired conditions may be discovered. These conditions could be newly identified failure points, unsuppressed inductive loads, unnecessary components, unnecessary software codes and inadequate redundancy provisions. These conditions should be documented in design concern reports. Any documentation discrepancies should be reported in document error reports. A final sneak analysis report should be written that details the scope, procedures, results and conclusions of the analysis. The final report should also include all sneak conditions, design concern reports, documentation error reports and report tracking status sheets.

Technical Rationale:

Sneak analysis is a reliability-enhancement method used to identify designed-in conditions that could introduce undesired events and inhibit desired system functions which could adversely affect crew safety or mission success. The sneak circuit analysis technique differs from other system analysis techniques in that it is based on identification of designed-in inadvertent modes of operation and is not based on failed equipment or software.

Impact of Nonpractice:

Sneak circuits that escape cursory design screening can result in schedule delays, damage to equipment during test, downtime during operation, increased cost, and possible loss of spacecraft or crew. Too-late implementation of a sneak analysis can result in high project costs due to redesign and redevelopment efforts.

SNEAK CIRCUIT ANALYSIS GUIDELINE FOR ELECTROMECHANICAL SYSTEMS

Related Guidelines:

None

References:

1. Buratti, Davey L. and Sylvia G. Godey: "Sneak Analysis Application Guidelines", RADC-TR-82-179, Boeing Aerospace Company for Rome Air Development Center, Griffis AFB, NY 13 441, June, 1982.
2. Hill, E.J. and C. J. Bose: "Sneak Circuit Analysis of Military Systems", Boeing Aerospace Company, Seattle, WA, 2nd AIAA International Systems Safety Conference, San Diego, CA, July 21-25, 1975, Proceedings, A77-16726-31, Newport Beach, CA, System Safety Society, 1976, pgs. 351-372.
3. Miller, Jeff: "Integration of Sneak Analysis with Design", RADC-TR-109, Vol. 1 of 2, Sohar Incorporated for Rome Air Development Center, Griffis AFB, NY 13441, June, 1990.
4. Walker, Frank Ellis: "Sneak Circuit Analysis Automation", Boeing Aerospace, Seattle, IEEE, 1989 Proceedings Annual Reliability and Maintainability Symposium.
5. Wilson, Joe L. and Robert C. Clardy: "Sneak Circuit Analysis Application to Control System Design", The Boeing Company, Houston, TX, AGARD-AG-224, In AGARD Integrity of Electronic Flight Control Systems for Aircraft Reliability, April, 1977.
6. Vogas, James L.: "Sneak Analysis of Application Specific Integrated Circuits", Boeing Aerospace Operation, Inc., Houston, TX, AIAA-92-0976, 1992 Aerospace Design Conference, Irvine, CA, February 1992.
7. MIL-STD-785B: "Reliability Program for Systems and Equipment Development and Production", Military Standard, September 15, 1980.
8. NSTS 22254B: "Methodology for Conduct of Space Shuttle Program Hazard Analysis", NASA, Johnson Space Center, Houston, TX 77058, December 30, 1993.