PREFERRED
RELIABILITY
PRACTICES

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

Practice:

Analyze all systems to identify potential failure modes by using a systematic study starting at the piece part or circuit functional block level and working up through assemblies and subsystems. Require formal project acceptance of any residual system risk identified by this process.

Benefit:

The FMECA process identifies mission critical failure modes and thereby precipitates formal acknowledgment of the risk to the project and provides an impetus for design alteration.

Program that Certified Usage:

Viking, Voyager, Magellan, Galileo

Center to Contact for More Information:

Jet Propulsion Laboratory (JPL)

Implementation Method:

Through the use of formal spread sheets, each potential failure within an assembly is recorded together with its resultant assembly, subsystem, and system effect. The severity of the system failure effect is assigned from a pre-defined list ranging from "negligible effect" to "mission catastrophic." Design alterations can be made at the circuit level (thereby modifying the assembly level) to eliminate a failure mode or to reduce its severity. The remaining failures are evaluated as potential subsystem failures by accounting for possible redundancy or work-arounds. Again design alterations may be invoked. Those remaining up to the system level are reported as single points of failure (SPFs), and the project makes a conscious decision to either retain them or to initiate corrective action.

Technical Rationale:

Every technical mission carries with it a degree of risk. A mechanism is needed to identify and quantify the risk to permit decisions to be made which will ultimately reduce the risk to the minimum permissible level within the project cost, schedule, and performance constraints. Because most spacecraft systems are extremely complex, a method of risk identification must be used which has total visibility into the system. The FMECA has been recognized as such an approach and, if implemented rigorously, will provide the necessary visibility.

The process requires the assumption of a failure of each part of each unit. The credible failure modes are identified for each part (e.g., capacitors can short or open). If a piece part level FMECA is required by project definition, a line item must be entered for each identified mode of each part, e.g., "C23 shorts". If a

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

project employs a high degree of redundancy, the complexity of a part level FMECA is unnecessary because a presumably redundant element will perform the function. Thus a functional level FMECA is adequate, e.g., "the amplifier chain formed by Q14, Q15, and Q16 and their associated parts has very low gain". This failure may have many root part failure causes but if all possible failure modes of the block are identified, e.g., "low gain, oscillation, high gain, high harmonic distortion", there is no value in recording the individual part causes. The most essential analysis in a design which uses redundancy is that of the cross-strapping networks. For this reason, a parts level FMECA is considered mandatory for all cross-strapped redundant elements, either inside an assembly or at an external interface.

Impact of Non-Compliance:

Without a formal FMECA process, the system design integrity would be determined by the experience and rigor of a large number of individual design engineers. There would be no means of verifying that design risk has been minimized to a degree which yields a high confidence in achieving the mission goals.