PREFERRED RELIABILITY PRACTICES

THE TEAM APPROACH TO FAULT-TREE ANALYSIS

Practice:

Use a multi-disciplinary approach to investigations using fault-tree analysis for complex systems to derive maximum benefit from fault-tree methodology. Adhere to proven principles in the scheduling, generation, and recording of fault-tree analysis results.

Benefits:

The use of the team approach to fault-tree analysis permits a rapid, intensive, and thorough investigation of space hardware and software anomalies. This approach is specifically applicable when the solution of engineering problems is urgent and when they must be resolved expeditiously to prevent further delays in program schedules. The systematic, focused, highly participative methodology permits quick and accurate identification, recording, and solution of problems. The resulting benefits of the use of this methodology are reduction of analysis time, and precision in identifying and correcting deficiencies. The ultimate result is improved overall system reliability and safety.

Programs That Certified Usage:

Space Shuttle Solid Rocket Motor (SRM), Space Shuttle Main Engine (SSME), Space Shuttle External Tank (ET).

Center to Contact for More Information:

Marshall Space Flight Center (MSFC)

Implementation Method:

***Determination that a Team Approach to Fault-Tree Analysis is Required*:**

In situations where program hardware or software anomalies are uncovered which could potentially reduce the possibility of mission success or cause harm to personnel, and where the pressure of schedules requires a rapid and accurate solution of problems, the team approach to fault-tree analysis should be strongly considered. Fault-trees are useful necessary when the system in question is complex and has many potential contributors to the problem that solution defies simple intuition, engineering judgement, or easy elimination of the events that contributed to the

MARSHALL SPACE FLIGHT CENTER

THE TEAM APPROACH TO FAULT-TREE ANALYSIS

problem. The team approach to fault-tree analysis brings all disciplines to bear simultaneously in an interactive but controlled environment.

A fault-tree is defined as, “a graphic depiction or model of the rationally conceivable sequences of events within a complex system that could lead ultimately to the observed failure or potential failure.” It is a systematic approach to fault prevention achieved by postulating potential high level faults, and identifying the primary and secondary causes, down to the lowest piece-part, that could induce the high level fault. A typical arrangement of a fault-tree showing the potential types of "gates” containing Boolean logic is shown on Figure 1. In situations of high urgency and cost or schedule sensitivity, it is often desirable to apply a team approach to development and use of the fault-tree methodology.

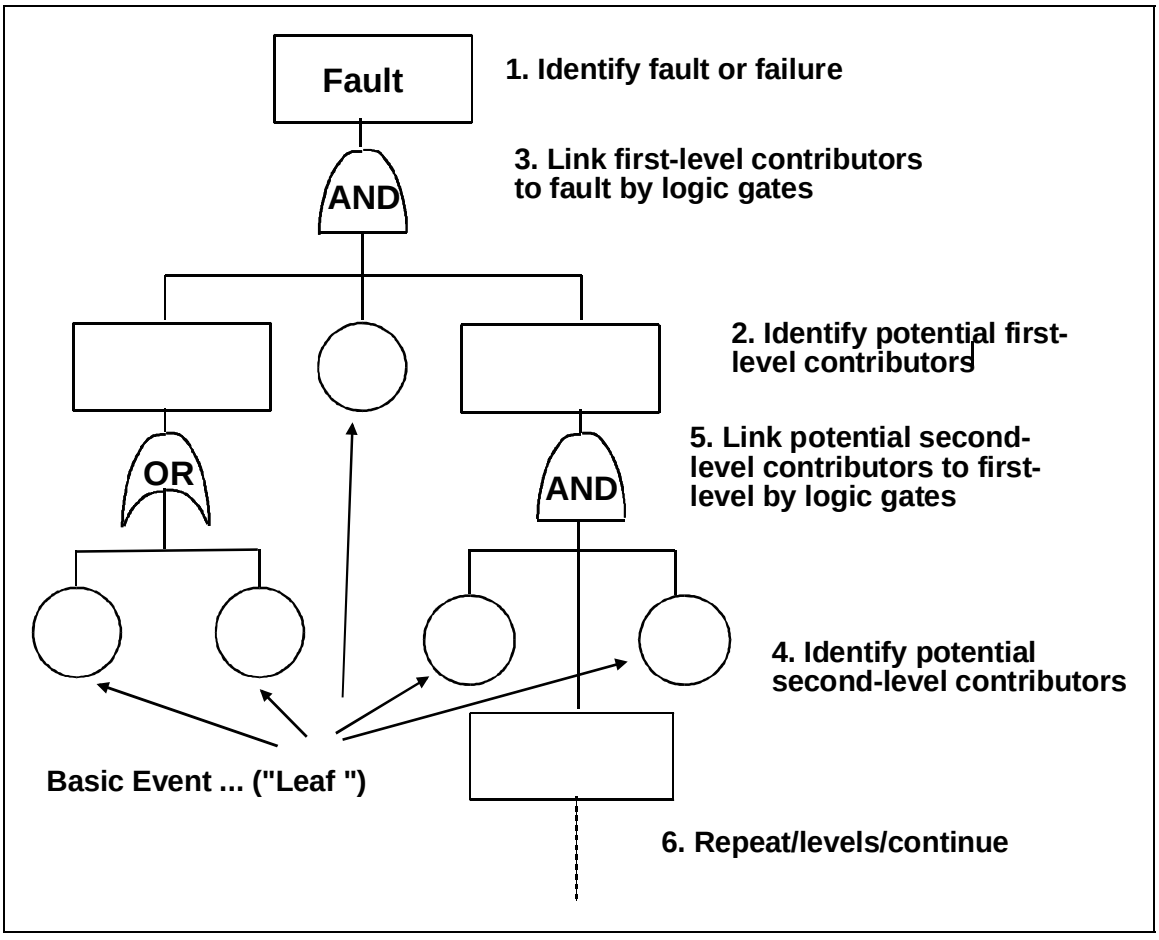

Figure 1. Fault Tree Analysis

THE TEAM APPROACH TO FAULT-TREE ANALYSIS

Fault-Tree Team Methodology:

The keys to a successful team approach to a fault-tree analysis are: (1) selection of the right people to participate in the analysis; (2) interactive meetings of these people in a creative but focused environment; (3) thorough documentation of objectives, fault-tree structure, and action items; (4) parallel (but not redundant) participation by all team members; and (5) careful attention to general ground rules for effective team dynamics. All of the preceding must be backed up by a data base containing the hardware/software configuration, operational time lines, potential failure causes, and exonerating or indicting data. Logic flow networks are built based on the system's design, then laboratory test results, hardware/software test results, and modeling are based on deterministic and/or probabilistic statistical analyses. These logic flow networks also feed into the information data base that is used by the fault-tree team.

An integral part of successful fault-tree methodology is the selection of an orderly structure on which to base the fault-tree and the team participation. The Work Breakdown Structure (WBS) is an ideal starting point for the team as well as for the design. Each event or activity in the WBS is subdivided into its main contributing events or activities, then the tree is subdivided again until the smallest activity that cannot be further subdivided is reached. These final events or activities are the "leaves" on the fault-tree.

Team Composition:

Given the nature of the failure or anomaly being investigated, people should be assembled who have both an intimate disciplinary knowledge and a knowledge of the overall system. Elements heads and subteam leaders should be established for major investigative elements of the work breakdown structure. Important administrative functions to support the team are: (1) the maintenance of a current address, phone, and fax listing of all persons involved; (2) recording daily team meeting minutes; (3) preparation of agenda for the next day, (prepared at the end of the current day); (4) recording of all action items including the name of the person responsible, suspense dates, and the specific action required; and (5) the maintenance of a master schedule of major planned events, based in part on the suspense dates.

Team Dynamics and Work Strategy:

The entire team should meet together in one location in a meeting to expose all known data related to the anomaly or failure, then the team should meet at least once per day thereafter. Action items should be assigned and as much work as possible should be done in parallel without undue redundancy. Series activities of the team should be avoided. Team interaction is important because the fault-tree is built in a dynamic, contributory fashion.

During the fault-tree team activities, the team leader and scribe should keep files of action items, agendas, technical data related to development of the fault-tree, correspondence, administrative

reports, the master fault-tree diagram, and the team's schedule. Top management and other related organizations should be kept informed as to the progress of the team. Hand written notes to the key players from the team leader "en route," at key milestones and critical junctures, and on successful completion of the investigation are particularly helpful. Rambling discourses should be avoided. Meetings and discussions must be diplomatically kept on track. The leader should be as democratic as possible in team meetings. No one should be affronted, but in case of an impasse, the team leader must make the decision. Refreshments should be provided occasionally, especially on Saturday or Sunday and after hours. This will boost morale and provide an atmosphere conducive to free discussion.

Other General Techniques and Methods:

The purpose of the team approach is to provide multidisciplinary perspectives that will uncover details and to resolve cause/effect relationships which may not be apparent in more narrowly focused detailed engineering analytical and design methods. Therefore, each element of the fault-tree must be doggedly and systematically analyzed, persistently subdivided into it's smallest elements, and pursued to the lowest level.

The history of these types of investigations has indicated that a methodical, vigorous assessment is needed to develop and to utilize a fault-tree of sufficient depth. This vigorous assessment will eliminate illogical assumption, identify or eliminate synergistic effects, help to avoid partial fixes and reduce intuitive or random approaches that cannot be substantiated. The team should resist the temptation to preconceive a conclusion or take on a "pet theory" to the exclusion of a systematic, orderly, and vigorous treatment of all elements in the decision tree. The team should avoid any tendency to slow down the analysis process or to assume that a conclusion has been reached when a likely cause candidate has been identified, because this potential candidate could mask the true cause or divert the team's attention from a more fruitful path.

Probability and statistics are important disciplines to use in the fault-tree analysis process. The team should have an appreciation of the fact that if it is necessary to stack too many possible events together to eventually postulate the occurrence of the failure, then it is improbable that it occurred in that manner. The references list several computer-aided fault-tree analysis software packages that will aid in performing the statistical analysis and informing the decision tree graphics required to document a fault-tree analysis.

Technical Rationale:

The team approach to fault-tree analysis described in this practice was used very successfully in a number of in-depth investigations of problems that occurred in propulsion elements of the Space Shuttle, and related facilities and equipment. The procedure was first used in full measure in the investigation of a fire in the casting pit of the Space Shuttle Solid Rocket Motor (SRM) in 1984. It was also used in identifying causes of problems in the SRM propellant mix facility.

THE TEAM APPROACH TO FAULT-TREE ANALYSIS

Several problems and potential problems with the Space Shuttle Main Engine (SSME) were successfully investigated using the team approach to fault-tree analysis. These investigations involved the bearings for the alternate turbopump, and a synchronous vibration problem. Hydrogen leaks in the Space Shuttle Columbia were investigated and successfully resolved in an in-depth and intensive three-month team approach to fault-tree analysis.

Impact of Nonpractice:

Failure to adhere to the guidance provided in this preferred reliability practice could result in: (1) prolonged investigations yielding either marginal or no fruitful results; (2) expenditure of the valuable time and efforts of engineering personnel with less than optimum performance; and (3) failure to pinpoint problem causes and corrective actions with precision. Overall results could be slippage of the schedule, increased costs, unidentified hazards to the crew and other personnel, and nonperformance of the mission.

Other Related Practices:

PD-ED-1208 - "Static Cryogenic Seals for Launch Vehicle Applications"

References:

1. Dhillon, Balbir S: "Fault-Tree Analyses," (Chapter 20 of "Mechanical Engineers Handbook") John Wiley & Sons, New York, NY, 1986.
2. Koren, James: "Computer-Aided Fault-Tree Analysis (CAFTA) User's Manual," Science Applications International Corporation, Los Altos, CA, 1993.
3. Van Fleet, Kevin: "Risk Spectrum Fault-Tree Software," User's Manual, Innovative Software Designs, Inc., Baltimore, MD, 1993.
4. Wild, Tony, Ph.D.: "Tree Master Software," User's Manual, Management Sciences Incorporated, Albuquerque, NM, 1994.
5. Schwinghamer, Robert: "Leak Team's Final Eureka Anthem" Hydrogen Leak Investigation Team Final Report (Presentation), NASA, Marshall Space Flight Center, A-L, November 8, 1990.