Fault Tree Analysis

Several investigations are presently addressing the recent failures of the Mars Climate Orbiter and the Mars Polar Lander. NASA is certainly looking forward to the full results of these assessments. Meanwhile, we can improve the potential for success of NASA programs as we await the lessons these teams will report.

I would like to suggest some actions we need to take during the formulation phase of any new program development effort. A few simple steps can increase our chances for preventing failures in our future launches and projects.

In our work, we tend to focus on ways to make things "go right." This confident optimism is an important characteristic that helps us pursue the challenges of invention and exploration. However, to make things "go right," we also need to understand and control the things that can "go wrong." This beneficial pessimism is sometimes a bit more difficult to apply to our own creations, but is needed to increase the likelihood of future successes. Therefore, I ask that we put more effort into analyzing "what can go wrong."

There are a number of engineering tools and techniques that can help us understand the vulnerabilities to our systems. These include the bottom-up analytical approach, known as the Failure Modes and Effects Analysis (FMEA), and the top-down approach, known as the Fault Tree Analysis. A third assessment, the Probabilistic Risk Assessment, integrates information from these two approaches and other sources to assess the potential for failure and help find ways to reduce risk. These analyses constitute a three-pronged approach to help program/project managers assess and mitigate risk and to increase the likelihood for safe and successful missions. This week, I would like to talk in more detail about Fault Tree Analysis.

Fault Tree Analysis is not a new method. The Boeing Corporation first applied it in 1964 to analyze "what could go wrong" with the Minuteman ICBM. It remains, however, one of the best methods for systematically identifying and graphically displaying the many ways something can go wrong. It is "best" in the sense that it is the easiest to use and can be used by anyone, not just safety or reliability experts. It is the easiest in that one begins with a top-level undesired event and works down to identify the subordinate events that could cause such an unwanted outcome. Moreover, in most cases, quantification is not needed to obtain valuable insight into the weaknesses of a design.

At NASA, a Fault Tree Analysis is a methodical review of a system’s hardware and software that begins by envisioning an undesired end state, such as mission failure or loss of crew or vehicle. The project team identifies, in a logical manner, the sequences and combinations of events that could lead to the undesired event. Fault Tree Analysis is most cost-effective when performed early in a project and updated as the project develops. When applied early in the life cycle, it is cheaper to modify a requirement or a drawing than it is to modify hardware or software code later on.

Fault Tree Analysis should also be used to evaluate possible system engineering changes that could eliminate or reduce potential failure paths. As one part of the three-pronged approach, it is a very effective way to find and graphically communicate to engineers and managers a design’s potential "Achilles Heel," should one exist.

Application of Fault Tree Analysis can be beneficial even if initiated late in a program. Questions, doubts, or a late need for additional assurance may sometimes arise. After the Mars Climate Orbiter mishap, a Fault Tree Analysis was done on the Mars Polar Lander, even as it was nearing the end of its long journey to Mars. This analysis was ordered to quickly assess whether the spacecraft might contain latent, but correctable, problems. Ironically, the ability for Fault Tree Analysis to identify what "could" go wrong creates an ancillary capability for helping to find what "did" go wrong after a mishap.

As we prepare for future missions, it is increasingly important that we apply tools such as the Fault Tree Analysis during the formulation and development of a project to ferret out design faults long before any mishap occurs. Think of it as a form of mishap investigation conducted BEFORE there is a mishap.

For our complex and expensive systems, we should not be questioning "why" we should be using Fault Tree Analysis or the other two parts of our three-pronged analysis to ensure our mission’s safety and success. On the contrary, we should be questioning "why not" before we elect to forgo these safeguards. I urge you to understand and employ Fault Tree Analysis to learn "what" can go wrong and to help prevent it when it really counts.

For more information on Fault Tree Analysis, you may contact the Agency’s Office of Safety and Mission Assurance at Headquarters or any Center’s Safety and Mission Assurance organization.

NASA Actions

NASA Program/Project Managers

- Use Fault Tree Analysis as early as possible in your programs and projects to analyze "what" could go wrong.
- Use the results of Fault Tree Analysis to eliminate potential causes of mishap or mission failure-preferably through engineering design.

NASA Center Directors

- Check that assurance tools, such as Fault Tree Analysis, are being conducted on programs and projects at your Center.
- Provide training and assistance in Fault Tree Analysis to program and project offices.

An excellent reference manual for learning the technique of Fault Tree Analysis: "Fault Tree Handbook", NUREG-0492, by W. E. Vesely, U. S. Nuclear Regulatory Commission, January 1981, GPO Stock Number 052-010-02012-9, $14.00