

MESSAGE FROM THE ADMINISTRATOR

Health & Safety Topic—Design for Safety

No one can deny that reaching for the stars is a risky venture, but we should be committed to doing it as safely as possible. We must think safety throughout a program or system life cycle and focus on identifying failure modes and effects in our hardware and software along the way.

A Design for Safety program -- a total systems approach addressing safety issues as they are discovered -- would help us meet this goal. It would allow us to continuously search for problems and assess risk and solution options from concept through operations. Designing for safety would also include the verification processes to insure the development of safe life designs.

Design for Safety tools would essentially cut the fault tree off at the roots and not allow it to grow. To do this we would depend heavily on learning and knowledge-based tools that will be developed under the Intelligent Systems program. This technology will enable us to create systems that learn and reason for themselves and extract information and knowledge from complex distributed databases. They will also allow us to develop the means to virtually capture the experience and insight of experts. We would use this capability to build high-level "safety oriented" supervisory tools. We would integrate them into the Intelligent Synthesis Environment's life cycle analysis and design tools to develop and institutionalize a smart design process oriented on safety.

How might such a system work?

Design for Safety should start in the concept design phase and continue through the entire life cycle of the project. Design for Safety applies to all project phases -- design and development, test and verification, certification, and maintenance and operation. During the design and development phases, Design for Safety tools would conduct automated "what if" studies to evaluate system hazards and their impact on the life and operation of systems. As failure modes are discovered, these tools would quantitatively evaluate safety issues and assess the cost and risk of redundancy versus robustness to minimize risk. And once a system is operational, Design for Safety tools would use the "what if" results and advanced information technology methods to discover patterns and trends and to identify and analyze possible failures throughout the system's life cycle. They would also track problem reports and maintenance actions to assure our systems were kept in top operating condition. Additionally, operational experience would be used to update analytical models and legacy data/knowledge bases to better predict future system performance and risk. The more experience we gain with our systems, the safer they would be.

We could also use Design for Safety tools and techniques to create a more effective workforce. We could use case studies as educational tools and let people do mock designs under the supervision of a Design for Safety intelligent agent. No tool will replace smart people, but smart tools can create even smarter people and an even stronger NASA.

While this vision requires a long-term commitment to conduct the necessary research and technology development, NASA is prepared to start making it a reality today.