Building Safer Systems With SpecTRM

System safety, an integral component in software development, often poses a challenge to engineers designing computer-based systems. While the relaxed constraints on software design allow for increased power and flexibility, this flexibility introduces more possibilities for error. As a result, system engineers must identify the design constraints necessary to maintain safety and ensure that the system and software design enforces them.

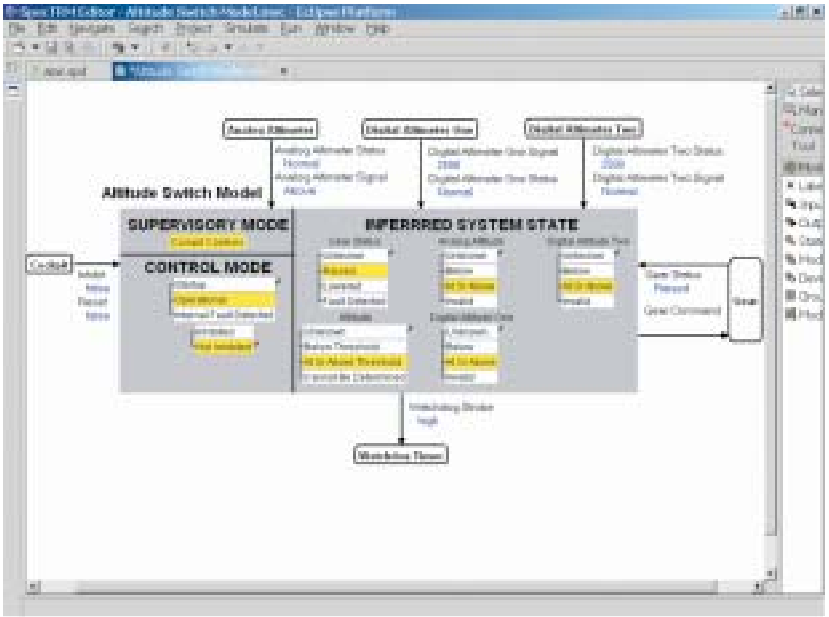
Safeware Engineering Corporation, of Seattle, Washington, provides the information, tools, and techniques to accomplish this task with its Specification Tools and Requirements Methodology (SpecTRM). NASA assisted in developing this engineering toolset by awarding the company several **Small Business Innovation Research (SBIR)** contracts with Ames Research Center and Langley Research Center. The technology benefits NASA through its applications for Space Station rendezvous and docking.

SpecTRM aids system and software engineers in developing specifications for large, complex safety-critical systems. The product enables engineers to find errors early in development so that they can be fixed with the lowest cost and impact on the system design. SpecTRM traces both the requirements and design rationale (including safety constraints) throughout the system design and documentation, allowing engineers to build required system properties into the design from the beginning, rather than emphasizing assessment at the end of the development process when changes are limited and costly.

Engineers ensure that software specifications possess desired safety properties through manual inspection, formal analysis, simulation, and testing. SpecTRM provides support for all of these activities. The simulation of specifications in SpecTRM graphically illustrates the behavior of software from the requirements model, allowing the software requirements to be tested and validated before the costly process of generating design and code. SpecTRM's specification slicing tool cuts through even the most complex systems to assist reviewers in validating requirements by making the most important system behavior stand out.

As a bridge among diverse groups of system, software, and safety engineers, SpecTRM facilitates communication and the coordinated design of components and interfaces. The product's executable requirements specification language can be easily read and reviewed by all system engineering disciplines, helping to provide seamless transitions and mappings between the various development and maintenance stages.

SpecTRM is based on proven research methods in flight management systems, air traffic control systems, and the Traffic Alert and Collision Avoidance System. The tool ensures these methods and analyses are robust, user-friendly, and automated to the point that they can be used in an industrial setting, benefiting the aerospace and transportation industries. SpecTRM can also be applied to designs for automotive systems, defense systems, and medical devices. Safeware Engineering Corporation offers comprehensive consulting and training services to new and existing SpecTRM users, helping customers to meet their system specification and design needs.



The Specification Tools and Requirements Methodology provides the information, tools, and techniques engineers need to identify design constraints for system safety during software development.