

ITOP 1-1-057

SAFETY CRITICAL SOFTWARE ANALYSIS AND TESTING

SCOPE

This ITOP describes a systematic approach to implement software safety as an integral part of the overall system safety program. A systematic approach to developing and testing safety-critical software is essential in the process of producing reliable software. The ITOP describes the activities necessary to ensure that safety is designed into software that is acquired or developed and that safety is maintained throughout the software life cycle. It provides uniform procedures for developing and implementing a safety-critical software test methodology of sufficient comprehensiveness to identify the software caused hazards of a system and to impose design requirements and management controls to prevent mishaps. The objective is to ensure that the software design takes positive measures to enhance system safety, and that software errors which could reduce system safety have been eliminated or controlled to an acceptable level of risk.