The techniques to achieve and guarantee high and ultra high software reliability, needed for applications in avionics, process control and other high assurance domains, have been actively pursued in software engineering research for several decades. Two rather distinct approaches emerged. In one, state space exploration tools search for the existence of states and their combinations that, if reached during program execution, would violate some of the required safety properties. Model checking tools have become mature and are being used for verification of critical program sections in critical domains. The other approach exploits statistical testing for demonstration of the absence of faults. This approach suffers from well known theoretical and practical limitations: imprecise nature of operational distributions, difficulty in the construction of test oracles, massive testing requirements and ensuing statistical significance. Both approaches impose severe limitations on the cost effectiveness of software verification and validation in practice.

In this talk, we will analyze the verification and validation techniques that improve the effectiveness of software verification. Empirical analysis of formal modeling approaches indicates that combinations of diverse tools can expose faults not detected by any of these tools in isolation. Further, using examples from biometric recognition, we will demonstrate that domain specific model based analysis can lead to meaningful ultra high reliability assessment. We will further outline the most promising research directions for streamlining software verification and validation activities and emerging research challenges.