

Insights: Publications

An integrated multidomain functional failure and propagation analysis approach for safe system design

Cambridge University Press

April 24, 2013

Written by **Chetan V. Mutha, Ph.D.**

Early system design analysis and fault removal is an important step in the iterative design process to avoid costly repairs in the later stages of system development. System complexity is increasing with increased use of software to control the physical system. There is a dearth of techniques to evaluate inconsistencies, incompatibility, and fault proneness of the system design in an integrated manner. The early design analysis technique presented in this paper aids a designer to understand the interplay between the multifaceted components and evaluate his/her design in an integrated manner. The technique allows simultaneous propagation of different types of faults from various domains and evaluates their functional impact over a period of time. The structure of the technique is explained using domain-specific conceptual metamodels, whereas the execution is based on the event sequence diagram, which is one of the established reliability and safety analysis techniques. One of the notable features of the proposed technique is the object-oriented nature of the system design representation. The technique is demonstrated with the help of a case study, and the execution results of two scenarios are evaluated to demonstrate the analysis capability of the proposed technique.

Related People



Chetan V. Mutha, Ph.D.

t 202.481.9958

cmutha@ktslaw.com