World Academy of Science, Engineering and Technology
International Journal of Mechanical and Industrial Engineering
Vol:13, No:10, 2019

Failure Analysis and Verification Using an Integrated Method for Automotive Electric/Electronic Systems

Authors : Lei Chen, Jian Jiao, Tingdi Zhao

Abstract : Failures of automotive electric/electronic systems, which are universally considered to be safety-critical and software-intensive, may cause catastrophic accidents. Analysis and verification of failures in these kinds of systems is a big challenge with increasing system complexity. Model-checking is often employed to allow formal verification by ensuring that the system model conforms to specified safety properties. The system-level effects of failures are established, and the effects on system behavior are observed through the formal verification. A hazard analysis technique, called Systems-Theoretic Process Analysis, is capable of identifying design flaws which may cause potential failure hazardous, including software and system design errors and unsafe interactions among multiple system components. This paper provides a concept on how to use model-checking integrated with Systems-Theoretic Process Analysis to perform failure analysis and verification of automotive electric/electronic systems. As a result, safety requirements are optimized, and failure propagation paths are found. Finally, an automotive electric/electronic system case study is used to verify the effectiveness and practicability of the method.

Keywords : failure analysis and verification, model checking, system-theoretic process analysis, automotive electric/electronic system
Conference Title : ICEFA 2019 : International Conference on Engineering Failure Analysis
Conference Location : Paris, France
Conference Dates : October 29-30, 2019