Gregor GOESSLER  
INRIA Grenoble (France)  

A General Trace-Based Framework for Blaming in Component-based Systems

Abstract: In component-based safety-critical embedded systems it is crucial to determine the cause(s) of the violation of a safety property, be it to issue a precise alert or to determine liability of component providers. In this paper we present an approach to blame components based on a single execution trace violating a safety property $P$. The diagnosis relies on counterfactual reasoning (what would have been the outcome if component $C$ had behaved correctly?) to distinguish component failures that actually contributed to the outcome from failures that had little or no impact on the violation of $P$. 