Engineering Failure Analysis 18 (2011) 590–608

Contents lists available at ScienceDirect

Engineering Failure Analysis

journal homepage: www.elsevier.com/locate/engfailanal

Engineering failure analysis and design optimisation with HiP-HOPS

Yiannis Papadopoulos [a,*], Martin Walker [a], David Parker [a], Erich Rüde [b], Rainer Hamann [b], Andreas Uhlig [c], Uwe Grätz [c], Rune Lien [d]

[a] University of Hull, Cottingham Road, Hull, HU6 7RX, United Kingdom
[b] Germanischer Lloyd AG, Brooktorkai 18, 20457 Hamburg, Germany
[c] ITI GmbH, Webergasse 1, D-01067 Dresden, Germany
[d] Agito SA, Postbox 792, N-3606 Kongsberg, Norway

ARTICLE INFO

Article history:
Available online 23 October 2010

Keywords:
Failure analysis
Hazards
Safety

ABSTRACT

The scale and complexity of computer-based safety critical systems, like those used in the transport and manufacturing industries, pose significant challenges for failure analysis. Over the last decade, research has focused on automating this task. In one approach, predictive models of system failure are constructed from the topology of the system and local component failure models using a process of composition. An alternative approach employs model-checking of state automata to study the effects of failure and verify system safety properties.

In this paper, we discuss these two approaches to failure analysis. We then focus on Hierarchically Performed Hazard Origin & Propagation Studies (HiP-HOPS) – one of the more advanced compositional approaches – and discuss its capabilities for automatic synthesis of fault trees, combinatorial Failure Modes and Effects Analyses, and reliability versus cost optimisation of systems via application of automatic model transformations.

We summarise these contributions and demonstrate the application of HiP-HOPS on a simplified fuel oil system for a ship engine. In light of this example, we discuss strengths and limitations of the method in relation to other state-of-the-art techniques. In particular, because HiP-HOPS is deductive in nature, relating system failures back to their causes, it is less prone to combinatorial explosion and can more readily be iterated. For this reason, it enables exhaustive assessment of combinations of failures and design optimisation using computationally expensive meta-heuristics.

1. Introduction

Increasing complexity in the design of modern engineering systems challenges the applicability of rule-based design and classical safety and reliability analysis techniques. As new technologies introduce complex failure modes, classical manual analysis of systems becomes increasingly difficult and error prone.

To address these difficulties, we have developed a computerised tool called 'HiP-HOPS' (Hierarchically Performed Hazard Origin & Propagation Studies) that simplifies aspects of the engineering and analysis process. The central capability of this tool is the automatic synthesis of Fault Trees and Failure Modes and Effects Analyses (FMEAs) by interpreting reusable specifications of component failure in the context of a system model. The analysis is largely automated, requiring only the initial component failure data to be provided, therefore reducing the manual effort required to examine safety; at the same time,

* Corresponding author. Tel.: +44 (0)1482 465981.
E-mail address: Y.I.Papadopoulos@hull.ac.uk (Y. Papadopoulos).

1350-6307/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.engfailanal.2010.09.025