Chapter 4
Model-Based Functional Safety Analysis and Architecture Optimisation

David Parker
University of Hull, UK

Martin Walker
University of Hull, UK

Yiannis Papadopoulos
University of Hull, UK

ABSTRACT

The scale and complexity of computer-based safety critical systems pose significant challenges in the safety analysis of such systems. In this chapter, the authors discuss two approaches that define the state of the art in this area: failure logic modelling and behavioural modelling safety analyses. They also focus on Hierarchically Performed Hazard Origin and Propagation Studies (HiP-HOPS)—one of the advanced failure logic modelling approaches—and discuss its scientific and practical contributions. These include a language for specification of inheritable and reusable component failure patterns, a temporal logic that enables assessment of sequences of faults in safety analysis as well as algorithms for top-down allocation of safety requirements to components during design, bottom-up verification via automatic synthesis of Fault Trees and Failure Modes and Effects Analyses, and dependability versus cost optimisation of systems via automatic model transformations. The authors summarise these contributions and discuss strengths and limitations in relation to the state of the art.

DOI: 10.4018/978-1-4666-3922-5.ch004

INTRODUCTION

The use of classical safety and reliability analysis and rule-based design techniques has been increasingly challenged in recent years due to the growing scale and complexity of modern engineering systems. New technologies and the subsequent introduction of complex failure modes renders classical manual analyses of safety critical systems, such as Failure Modes & Effects Analysis (FMEA) and Fault Tree Analysis (FTA), increasingly difficult and error prone.

Two distinct strands of work have emerged in an attempt to meet this challenge and enable fast, accurate analyses of modern safety critical systems. The first category includes approaches that are based on formal verification techniques and rely on formal modelling and fault simulation to provide information about the failure behaviour of systems. The second category is based on the concept of compositional component-based safety analysis, enabling analysis to take place hierarchically on the basis of failure information represented at the component level of the system model.

HiP-HOPS (Hierarchically Performed Hazard Origin and Propagation Studies) is an advanced compositional safety analysis approach with software support that has been developed to simplify aspects of the engineering and analysis process. After annotating system components with logic that specifies how those components can cause and react to failures, HiP-HOPS automatically generates and analyses both FMEAs and Fault Trees (FTs) from engineering system models. It has also been extended with many additional capabilities, including automatic architectural optimisation and the allocation of safety integrity levels.

Classical analysis methodologies typically involve not just manual analysis but also manual construction of the analysis model (e.g. an FMEA or a fault tree), requiring substantial expertise and investment even with tool support. By contrast, the manual effort required by modern techniques is generally much more limited; for example, in HiP-HOPS, the only manual effort is the initial annotation of component failure data as part of existing system design modelling. The rest of the process is fully automatic and therefore much faster, drastically reducing the time and effort required to examine the safety of a system.

This automation enables safety analysis to be conducted rapidly as part of an iterative design process and allows safety to become a full, contributing factor to new design evolutions, rather than a hurdle that must be surmounted only at the end of the design, when changes to a mature system model may be much more expensive. By identifying potential safety and reliability issues early in the design process, new ideas and design variations can be proposed and more readily evaluated, potentially leading to safer, cheaper systems. A further benefit arising from the speed and scalability of the underlying algorithms is the ability to analyse large, complex systems that would otherwise be limited to partial or fragmented manual analyses.

In the next section we first describe the classical safety analysis techniques of FMEA and FTA and then go on to discuss the field of modern safety analysis techniques by describing the two main categories of approaches in more detail. Subsequently, we focus on HiP-HOPS in particular as a prominent example of a contemporary safety analysis approach, introducing the core concepts behind its operation, its potential for extensions into new areas, and lastly discussing some of the advantages it presents to designers and analysts of safety critical systems. Finally we take a look at what the future may hold and present a summary of our conclusions.

BACKGROUND

Fault Tree Analysis and Failure Modes and Effects Analysis

FMEA was introduced towards the end of the 1940s (U.S. Military, 1949), and FTA makes its first appearance two decades later in the 1960s for