Safety Science 105 (2018) 55–70

Contents lists available at ScienceDirect

Safety Science

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

Dynamic system safety analysis in HiP-HOPS with Petri Nets and Bayesian Networks

Sohag Kabir*, Martin Walker, Yiannis Papadopoulos

School of Engineering and Computer Science, University of Hull, Hull HU6 7RX, UK

ARTICLE INFO

Keywords:
Fault tree analysis
Reliability analysis
Model-based safety analysis
Dynamic fault trees
Temporal fault trees
HiP-HOPS
Petri Nets
Bayesian Networks

ABSTRACT

Dynamic systems exhibit time-dependent behaviours and complex functional dependencies amongst their components. Therefore, to capture the full system failure behaviour, it is not enough to simply determine the consequences of different combinations of failure events: it is also necessary to understand the order in which they fail. Pandora temporal fault trees (TFTs) increase the expressive power of fault trees and allow modelling of sequence-dependent failure behaviour of systems. However, like classical fault tree analysis, TFT analysis requires a lot of manual effort, which makes it time consuming and expensive. This in turn makes it less viable for use in modern, iterated system design processes, which requires a quicker turnaround and consistency across evolutions. In this paper, we propose for a model-based analysis of temporal fault trees via HiP-HOPS, which is a state-of-the-art model-based dependability analysis method supported by tools that largely automate analysis and optimisation of systems. The proposal extends HiP-HOPS with Pandora, Petri Nets and Bayesian Networks and results to dynamic dependability analysis that is more readily integrated into modern design processes. The effectiveness is demonstrated via application to an aircraft fuel distribution system.

1. Introduction

Safety-critical systems underpin many of the advances in modern society and have become an integral part of our life. However, our reliance upon them also means the failure of such systems has the potential to cause great harm, both to people and environment. For this reason, development of such systems requires a rigorous assessment of system behaviour to ensure that they possess a high level of reliability: the ability to perform their intended functions satisfactorily for a prescribed time and under stipulated environmental conditions (Leveson, 1995). Many classical system analysis techniques such as Fault tree analysis (FTA) and Failure modes effects and criticality analysis (FMECA) are available to evaluate system reliability.

Among these techniques, FTA is one of the most common approaches for probabilistic reliability evaluation of a wide range of systems. It is a graphical method which helps determine how a system failure (or "top event") can arise from combinations of component faults and other contributing factors (known as "basic events"). FTA usually has two aspects: a qualitative aspect and a quantitative aspect. Qualitative analysis is performed by transforming fault trees into the minimal cut sets (MCS), which are the smallest combinations of basic events that are necessary and sufficient to cause the top event. In quantitative analysis, the probability of the occurrence of the top event and other quantitative reliability indexes such as importance measures are mathematically calculated, given the failure rate or probability of individual basic events.

Although FTA is widely used for system analysis, it has some known limitations. One of such limitations is that it can only evaluate reliability of static systems. Static systems are those which exhibit a single mode of operation throughout their lifetimes. However, modern large-scale and complex systems frequently operate in multiple modes or phases, making them dynamic systems. This gives rise to a variety of dynamic failure characteristics such as functional dependencies between events and priorities of failure events. To overcome this limitation, a number of extensions to static fault trees such as dynamic fault trees (DFTs) (Dugan et al., 1992), Boolean logic Driven Markov Processes (BDMP) (Bouissou and Bon, 2003) and Pandora temporal fault trees (TFTs) (Walker, 2009) have been proposed.

In addition, even where software tool support exists, both classical and dynamic fault tree analyses can require a lot of manual effort, meaning the system analyses process is time consuming and expensive. Moreover, given the rapid iterative nature of modern system design, by the time a manual analysis is complete it may already be out of date (Kabir, 2017). These inconsistencies and discrepancies can lead to inaccurate evaluation of system reliability. Therefore, over the past two decades, there has been a lot of research on how to minimise manual

* Corresponding author.
E-mail addresses: s.kabir@hull.ac.uk (S. Kabir), martin.walker@hull.ac.uk (M. Walker), y.i.papadopoulos@hull.ac.uk (Y. Papadopoulos).

https://doi.org/10.1016/j.ssci.2018.02.001
Received 30 August 2017; Received in revised form 15 January 2018; Accepted 1 February 2018

effort by automatically synthesise reliability related data from formal system models. This has led to the emergence of model-based dependability analysis (MBDA). Over the years, several tools & approaches such as Hierarchically Performed Hazard Origin and Propagation Studies (HiP-HOPS) (Papadopoulos et al., 2016), Failure Propagation and Transformation Notation (FPTN) (Fenelon and McDermid, 1993), AltaRica (Arnold et al., 2000), and xSAP (Bittner et al., 2016; Bozzano et al., 2015; Bozzano and Villafiorita, 2007) etc. have been developed to support MBDA of systems.

Among these approaches, HiP-HOPS offers advanced compositional MBDA techniques with state-of-the-art tool support. System level analysis and assessment are broken down via composition into more manageable tasks, applied to individual components. A system-level failure model is then produced by composing the failure models of individual components, typically by connecting output deviations of one component to the input deviations of another. The system-level failure model is then automatically analysed to obtain dependability artefacts such fault trees and FMEA. Although HiP-HOPS primarily uses static FTA, it has also been demonstrated that HiP-HOPS can perform dynamic analysis of systems by using Pandora temporal fault trees (Kabir et al., 2017; Walker et al., 2007; Walker and Papadopoulos, 2009).

Pandora is a dynamic extension of static fault trees and defines three temporal gates in addition to the existing Boolean gates. It also provides a set of temporal laws to perform dependability analysis of dynamic systems. Qualitative analysis using Pandora can create useful insight into dynamic system failure and its basis in traditional FTA means it can be integrated into model-based design and analysis processes and tools. Pandora's temporal logic is capable of describing the local failure behaviour of components, enabling compositional synthesis of TFTs from systems models using popular modelling languages such as Matlab Simulink (MathWorks, 2017), EAST-ADL (EAST-ADL Association, 2014), or AADL (Feiler and Rugina, 2007). However, the use of Pandora in the context of HiP-HOPS was only for qualitative analysis. Although qualitative analysis can produce useful information about system reliability, it is advantageous (and sometimes necessary) to have quantitative information about the reliability of the system as well.

In the past, methodologies have been proposed to quantify Pandora temporal fault trees. For example, an analytical method has been developed (Edifor et al., 2012; Kabir et al., 2016), which uses algebraic expressions to probabilistically evaluate the temporal gates of Pandora TFTs. This approach is only applicable to systems with exponentially distributed lifetime data and works by considering the events (both basic and intermediate events) in the TFTs as statistically independent. However, in real life systems, not all events are statistically independent, and in such situations this can lead to an inappropriate estimation of system reliability. Recently, to overcome these limitations, some preliminary ideas on Petri Nets and Bayesian Networks based quantification methods for Pandora TFT were presented by the authors in (Kabir et al., 2015) and (Kabir et al., 2014) respectively and the approaches were applied to a small system. Further research is required to integrate this work with compositional MBDA so that they can be evaluated by applying them to larger systems.

1.1. Contributions

Given the advantages offered by MBDA and the potential benefits of Pandora for dynamic dependability analysis, integrating these capabilities will open many possibilities. In this paper, we focus on integrating dynamic quantitative analysis using Pandora with compositional model-based dependability analysis via HiP-HOPS. Within this broader context smaller contributions include:

- Consolidation of the ideas presented in (Kabir et al., 2015, 2014) providing two methodologies for probabilistic analysis of Pandora TFTs. In this paper, we move forward to show how the two new proposals for analysis of TFTs can work with a technique that can compositionally produce these TFTs from smaller fragments of analysis and annotations of system models. The paper contains a much larger case study than those used in (Kabir et al., 2015, 2014). Both BN and PN analysis techniques are applied on the same system models and results are compared.
- The processes of calculating importance measures of dynamic system components using the Petri Net- and Bayesian Network-based methods.
- A method for performing diagnostic analysis of dynamic systems using the BN-based approach.

The value of the paper is mostly in the synthesis of several fragments of earlier work, application of the resultant method, comparison between two techniques for quantitative analysis and reflection on results. This work contributes to improved quantitative analysis of dynamic systems in the context of HiP-HOPS method. In addition, the model transformations described in this paper may have a more general value and could be exploited by other work on dynamic and temporal fault trees.

2. Background

2.1. Introduction to HiP-HOPS and Pandora

HiP-HOPS has a long history that goes back twenty years and it is contributing to the state-of-the-art in model-based dependability analysis. It can automatically generate fault trees and FMEA tables from system models, as well as perform quantitative analysis on the fault trees. It can semi-automatically allocate safety requirements to the system components in the form of Safety Integrity Levels (SILs). It also has the ability to perform multi-objective optimisation of the architecture of system models, automating for example decisions about the location and level of replication of components. System analysis using HiP-HOPS is done in three main steps:

1. system modelling and failure annotation
2. fault tree synthesis
3. fault tree analysis and FMEA synthesis

In the first step, a system architecture is created showing the interconnections between system components. The architecture can be arranged hierarchically, i.e., components comprising the system can themselves contain subsystems with their own components. Afterwards, failure annotations are added to the system components to define how they may fail. This dependability related information includes component failure modes and expressions for output deviations, which describe how a component can fail and how it responds to failures that occur in other parts of the system. The expression for the output deviations show how the deviations in the component outputs can be caused either by the internal failure of that component or by corresponding deviations in the component's input. Such deviations can be user defined but typically include omission (O) of output, unexpected commission (C) of output, incorrect output, or too late or early arrival of output (Papadopoulos et al., 2001). Quantitative data can also be entered to facilitate quantitative analysis in a later phase through parametric distribution functions (e.g. failure rate or scale and shape parameters of exponential and Weibull distributions, respectively). Modelling and annotation of the system with dependability information can be done using popular modelling tools like Matlab Simulink or SimulationX (ESI ITI GmbH, 2017).

In the second step, the annotated system model is synthesised to obtain fault trees. The process of constructing fault trees starts with a deviation of system output (top event) and traverses the system architecture deductively, i.e., from the system level outputs to the component level failures, to examine the propagation of failures through connections between components. In this way the process traverses the