Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 114 (2017) 4–13

Procedia Computer Science

www.elsevier.com/locate/procedia

Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems, CAS
October 30 – November 1, 2017, Chicago, Illinois, USA

Increasing System Failure Analysis Effectiveness Through Architecture Modeling

S. Alex Rambikur, Kristin Giammarco, Bryan O'Halloran

Naval Postgraduate School, Monterey, CA, USA

Abstract

This research demonstrated that the quality of the classic Fault Tree Analysis (FTA) method could be improved through the use of system architecture models. While existing work demonstrates use of simplified system models in FTA using methods that combine existing tools, this research uniquely addresses the value of using a single tool to generate stochastic behavior models of more complex systems, together with their normal and failure mode events, from existing system specification documents. Use of a single tool is desirable for organizations wishing to limit investment and simplify management of architecture data and analysis. The Innoslate tool is used show how classic failure analysis methods such as FTA can be emulated in the Model Based System Engineering (MBSE) design process. For a simple demonstration example, a fault tree is distilled from behavior models captured in action diagrams. A comparison of the classic FTA approach with the model based approach shows potential for increase in failure analysis accuracy and efficiency.

Peer-review under responsibility of the scientific committee of the Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems.

Keywords: FTA; MBSE; Innoslate; Failure Analysis, Behavior Models

1. Introduction

Failure investigations of complex systems require that practitioners understand both the failure analysis methods being employed and the failing system itself. Formal methods of failure analysis such as FTA are often to support the Failure Reporting and Corrective Action System (FRACAS) component of reliability improvement programs for these complex systems. This diagnostic use of such formal methods reduces the amount of no-fault-found analysis results, allowing corrective actions to be implemented that could improve reliability and reduce cost[2]. Despite the formality of the FTA methods, results vary greatly in their accuracy and efficiency based on the system knowledge available to

Peer-review under responsibility of the scientific committee of the Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems.
10.1016/j.procs.2017.09.057

the practitioner and their discipline with the method. The system knowledge required for these tasks is not limited to the failing system alone, but to its environment and systems with which it interacts.

A recent review of common failure analysis methods such as FTA and Failure Modes Effects Analysis (FMEA) has revealed that they share many common elements with system architecture, such as; system elements, logical connections between elements, system redundancies, system context, inputs and outputs of system and its components, system structure through different operation modes, boundary definitions, interface definitions, and triggers[1]. As a result, their integration should present benefit to the accuracy and efficiency of failure analysis for complex systems. Related research in this area spans four different architecture modeling languages and several system architecture types, and demonstrate that fault trees can be generated by and/or extracted from architecture models for direct analysis in reliability tools [1].

This research builds on that previous work by focusing on complex in-service systems where development did not include architecture modeling, conducting integrated analysis in a single tool, and applying the methodology to a real-world system failure investigation. Only failures experienced within normal operating conditions, known as primary failures, are considered within the scope of this research.

1.1. Addressing challenges encountered with classic FTA using behavior modeling

Incorporation of failure modeling into system architecture models seeks to address current challenges with classic FTA and to improve its accuracy and efficiency. Specifically, behavior models will address those challenges presented by availability of system information and FTA method execution.

Failures of in-service complex systems are often difficult to replicate and observe directly. Failure modes based on system interactions are particularly difficult to identify forensically. Often failures not immediately isolated to a particular sub-system or component require the top event (failure) on the fault tree be identified at a high level in the system. Identification of the immediate, necessary, and sufficient events required for the top event to occur requires a detailed understanding of the expected system behavior[3]. Where the expected system behavior is not apparent, or the appropriate system experts are not available, analysts have few options available but to refer to system specification documents or historical data.

Documentation and historical data for in-service systems are often inadequate in presenting the system information in a way that lends itself to FTA of those systems. In the example used in this study, a hierarchy of system specifications was not available. This makes decomposition of system behavior more difficult. In many cases, interface definitions are lacking completeness, not updated during incremental system developments, or totally missing. Without adequate detail available, failures occurring at system interfaces will not be captured completely. Descriptions in the form of diagrams and figures vary greatly in availability and quality from system to system, and even within systems. This variability is possibly a result of differences in frameworks over times and across industries. The authors have also noticed that document-based system specification can lack an integrated perspective, leaving ambiguity in interactions between subsystems or components.

FTA method rules and logic are somewhat conceptual, and sometimes difficult to implement consistently. Common difficulties from the authors' own experience include the following:

- Substitution of the required failure events (verbs) for systems/components (nouns)
- Failure to capture redundancy and cut sets (ANDs/ORs)
- Ignoring quantitative aspect of fault tree for determining probability,
- Failure to consider primary vs secondary vs command failures,
- Failure to capture true immediate cause,
- Failure to capture system state context, as in: what happened and when did it happen?

1.2. Related Research

The methodology applied for the proposed methodology draws on previous work by William Schindel and Rafael Perez[4,5]. Schindel's conceptual approach posits that a systems functional hierarchy implies a complementary failure hierarchy. For each successful system function, there exists the possibility for that function to be unsuccessful[4]. The concept can be applied to physical architecture as well, wherein each physical element provides functionality to the