Available online at www.sciencedirect.com
SCIENCE DIRECT
Reliability Engineering and System Safety 91 (2006) 292–304
RELIABILITY ENGINEERING & SYSTEM SAFETY
www.elsevier.com/locate/ress

QRAS—the quantitative risk assessment system

Frank J. Groen*, Carol Smidts, Ali Mosleh

Center for Reliability and Risk, University of Maryland, College Park, MD, USA

Received 19 January 2004; accepted 17 January 2005
Available online 7 April 2005

Abstract

This paper presents an overview of QRAS, the Quantitative Risk Assessment System. QRAS is a PC-based software tool for conducting Probabilistic Risk Assessments (PRAs), which was developed to address risk analysis needs held by NASA. QRAS is, however, applicable in a wide range of industries. The philosophy behind the development of QRAS is to bridge communication and skill gaps between managers, engineers, and risk analysts by using representations of the risk model and analysis results that are easy to comprehend by each of those groups. For that purpose, event sequence diagrams (ESD) are being used as a replacement for event trees (ET) to model scenarios, and the quantification of events is possible through a set of quantification models familiar to engineers. An automated common cause failure (CCF) modeling tool further aids the risk modeling. QRAS applies BDD-based algorithms for the accurate and efficient computation of risk results. The paper presents QRAS' modeling and analysis capabilities. The performance of the underlying BDD algorithm is assessed and compared to that of another PRA software tool, using a case study extracted from the International Space Station PRA.

Keywords: PRA; Software tool; Binary decision diagram; Event sequence diagram; Common cause failure

1. Introduction

This paper describes the Quantitative Risk Assessment System (QRAS) [1], which is a PC-based software tool for conducting probabilistic risk assessments (PRA). The tool was originally developed in 1997, in order to provide NASA with a PRA tool responsive to the agency's specific needs in the area of its space mission risk assessment. It is, however, generally applicable as a risk assessment tool. Subsequent to the initial release, and through a series of updates, the capabilities of QRAS were extended, leading to the version released in 2002 [1].

The purpose of this paper is to provide an overview of the software's risk modeling and analysis capabilities. The organization of this paper is as follows. Section 2 describes the modeling tools made available to the risk analyst to specify the risk model. These include descriptions of the system hierarchy, mission timeline, event sequence diagram (ESD) and fault tree (FT) models, completed by the basic event quantification and common cause failure (CCF) models. Section 3 discusses QRAS's analysis capabilities by providing an overview of the analysis procedure as well as the risk measures that are computed. Section 4 describes the organization of the software. An overview of the BDD-based computational engine is provided in Section 5, followed by a discussion of the performance of these algorithms using parts of the International Space Station PRA model [2].

2. QRAS modeling capabilities

Risk models in QRAS consist of representations of risk scenarios in the form of event sequence diagrams and fault trees linked through ESDs. These models are organized based on a structural or functional decomposition of the system, as well as a decomposition of the system's mission timeline into phases and subphases. Details of the risk modeling capabilities are provided in this section.

2.1. System hierarchy and mission timeline decomposition

The construction of a risk model in QRAS starts with the definition of a functional, physical or hybrid system

* Corresponding author. Address: 6525 Belcrest Road #513, Hyattsville, MD 20782, USA. Tel.: +1 301 699 1150; fax: +1 301 699 1151.
E-mail address: fgroen@prediction-technologies.com (F.J. Groen).

0951-8320/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2005.01.008

hierarchy and the mission timeline, which together constitute a high-level model of the system as well as its mission.

The root of the functional or physical hierarchy represents the entire system, e.g. Space Shuttle, or top-level function of that system. Moving down in the system hierarchy, the structure or function is gradually decomposed into smaller systems or functions. Initiating events (IE), which form the starting points for the risk scenario models, form the bottom level of the hierarchy. As such, the system hierarchy provides a mechanism for allocating risk contributions by the initiating events to the different components or functions in the system, analogous to the role typically performed by the Master Logic Diagram [3]. Within the application, the system hierarchy further serves as a navigation tool, allowing the user to navigate through the model.

A second high-level decomposition concerns a representation of the various operational phases the system goes through during its mission. The mission time-line decomposition is done in two levels. At the system-level, the user can specify so-called mission phases to represent the major stages in the operation of the system. For example, in case of the Space Shuttle, mission phases typically included are Ascent, Orbit, and Descent. Each of the mission phases is defined in terms of a name, as well as a start and an end time. The mission phase start and end times serve as a reference clock for the specification of event timing during the mission phases. The definition of mission phases applies to the entire model.

In addition, QRAS allows the user to define operational time intervals (OTIs) which consist of specific time intervals within a given mission phase, and which are defined for individual subsystems in the system hierarchy. Operational time intervals are used to represent time periods during the mission phase within which the subsystem is thought to be in a particular mode of operation, or under a particular type of load, and, therefore, subject to particular modes of failure.

The user then has the option to specify during which OTIs the initiating events associated with the subsystem are possible. This results in a high-level model structure shown in Fig. 1. The system hierarchy is shown along the vertical axis, and the mission timeline is shown along the horizontal axis. The rectangles in Fig. 1 represent the OTIs during which the initiating events are considered relevant, and thus require further analysis.

2.2. Event sequence diagrams and fault trees

Initiating events form the starting point for the modeling of the risk scenarios, i.e. the combination of events leading to various ‘end states’ of the system. QRAS allows the system failure logic to be modeled in the form of event sequence diagrams [4] and fault trees [5]. ESDs are representations of sets of possible risk scenarios originating from an initiating event. Each scenario in an ESD consists of a unique sequence of occurrences and non-occurrences of ‘pivotal events’. Each scenario eventually leads to an end state, which designates the severity of the outcome of the particular scenario.

ESDs are used rather than event trees (ET) to model risk scenarios for two reasons. First, they are considered to be more easily understood, and therefore, facilitate a greater involvement of managers and engineers in the PRA process.

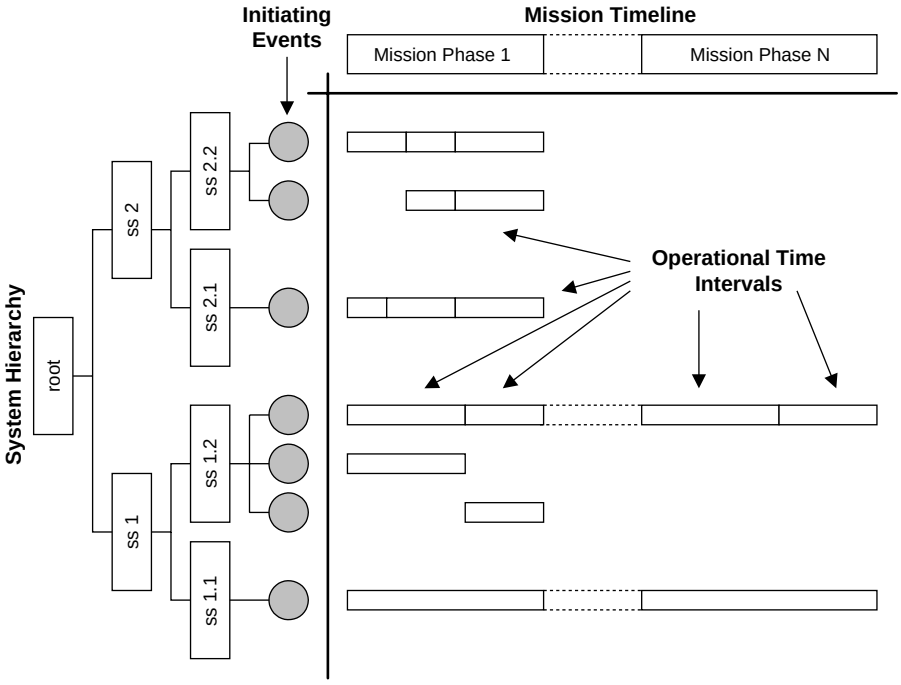

Fig. 1. High-level model structure based on system hierarchy and mission timeline. Root means the system, and ss means subsystem.