Reliability Engineering and System Safety 95 (2010) 1076–1092

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Hybrid approach for the assessment of PSA models by means of binary decision diagrams

Cristina Ibáñez-Llano [a,*], Antoine Rauzy [b], Enrique Meléndez [c], Francisco Nieto [a]

[a] Instituto de Investigación Tecnológica (IIT), Escuela Técnica Superior de Ingeniería ICAI, Universidad Pontificia Comillas, C/Santa Cruz de Marcenado 26, 28015 Madrid, Spain
[b] Dassault Systèmes, 10 rue Marcel Dassault CS 40501, 78946 Velizy Villacoublay Cedex, France
[c] Consejo de Seguridad Nuclear (CSN), C/Justo Dorado 11, 28040 Madrid, Spain

ARTICLE INFO

Article history:
Received 6 July 2009
Received in revised form
28 April 2010
Accepted 30 April 2010
Available online 1 June 2010

Keywords:
Probabilistic safety assessment
Binary decision diagrams
Event trees
Hybrid approach

ABSTRACT

Binary decision diagrams are a well-known alternative to the minimal cutsets approach to assess the reliability Boolean models. They have been applied successfully to improve the fault trees models assessment. However, its application to solve large models, and in particular the event trees coming from the PSA studies of the nuclear industry, remains to date out of reach of an exact evaluation. For many real PSA models it may be not possible to compute the BDD within reasonable amount of time and memory without considering the truncation or simplification of the model.

This paper presents a new approach to estimate the exact probabilistic quantification results (probability/frequency) based on combining the calculation of the MCS and the truncation limits, with the BDD approach, in order to have a better control on the reduction of the model and to properly account for the success branches. The added value of this methodology is that it is possible to ensure a real confidence interval of the exact value and therefore an explicit knowledge of the error bound. Moreover, it can be used to measure the acceptability of the results obtained with traditional techniques. The new method was applied to a real life PSA study and the results obtained confirm the applicability of the methodology and open a new viewpoint for further developments.

1. Introduction

Probabilistic safety assessment is a well-established technique for integrating various reliability models and to numerically quantify the frequency of damage in nuclear facilities. Its use is now widespread in nuclear regulation as it complements traditional deterministic analysis, providing a comprehensive and structured approach in identifying undesired accident scenarios, computing its likelihood in terms of occurrence frequency, and assessing the consequences and mitigation strategies. In terms of the mathematical tools used, PSA studies rely on the fault tree/event tree (FT/ET) methodology to obtain the response model of the facility.

The majority of computational tools used to assess the FT/ET models have implemented what is called the "classical" approach, namely the kinetic tree theory [1]. This approach, broadly used and accepted, is based on the computation of minimal cutsets (MCSs for short) by means of the Boolean reduction and on the use of probabilistic (frequency) cutoffs, owing to the complexity of the models. Truncation cutoffs on probability (or frequency) and also on the order of the MCS have to be applied to avoid MCS explosion. To avoid computational complexity, success (i.e. negated) logic is avoided in the FT/ET evaluation.

Bryant's binary decision diagrams (BDD) [2,3] are a well-known alternative to the minimal cutsets approach to assess the Boolean models. BDDs have the remarkable property of having complexity that is not related to the number of cutsets of the encoded Boolean formula. Conversely to the classical methodology, the BDD approach involves no approximation in the quantification of the model and is able to handle correctly the negative logic (success branches) at low additional complexity cost. However, BDDs are also subject to combinatorial explosion as the final size of the BDD is very sensitive to the variable ordering needed to convert the model into it.

After more than two decades of application, the BDD methodology has been applied successfully to improve the fault tree assessment and its introduction in the field has permitted renewing its algorithmic framework. In the last years, several works as well have undertaken its application to event tree assessment [4–6]. However, attempts to apply it to very large models, such as the ones coming from the PSA studies of the nuclear industry, which includes several thousand of basic events and logic gates, remain to date out of reach of a full automatic treatment. Although some attempts have been successful [4], for such large models it might not be possible to compute the BDD

* Corresponding autor. Tel.: +34 91 542 2800; fax: +34 91 542 3176.
E-mail addresses: cristina.ibanez@iit.upcomillas.es (C. Ibáñez-Llano), Antoine.RAUZY@3ds.com (A. Rauzy), ema@csn.es (E. Meléndez), nieto@iit.upcomillas.es (F. Nieto).

0951-8320/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2010.04.016

within reasonable amount of time and computer memory without considering truncation or simplification of the model. Consequently, it is necessary to explore new approaches to the problem. A potential solution is to develop a hybrid approach that combines the calculation of the MCS with the BDD approach, which allows obtaining a better and more controllable bound approximation of the model. The motivation and the basis of this new approach are the principal contribution of the work presented in this paper.

The remainder of this paper is organized as follows: Section 2 is devoted to introduce some basic terminology, to describe the particularities of the PSA models and to introduce the case study. Section 3 reviews the existing approaches for the FT/ET assessment, namely the classical and the BDD approaches. Section 4 specifically focused on the problem of model simplification that is performed with the classical approach. Section 5 presents the mathematical foundation of the hybrid approach. Finally, the experimental results and the conclusions are provided in Sections 6 and 7, respectively.

2. Description of the PSA models

This section is devoted to introduce the basic terminology and concepts needed to describe the Boolean models used in the PSA studies and to present the case study.

2.1. Terminology

Let $X=\{x_1,x_2,\ldots,x_n\}$ be a set of Boolean variables. We will briefly review some basic definitions concerning Boolean algebra.

A Boolean formula, F, denoted here by upper case letters, is a term inductively constructed over the two Boolean constants, 0 and 1, a denumerable set of variables X, and the usual logic connectives: the disjunction, equivalent to the OR operator and denoted by + or $\vee$, the conjunction equivalent to the AND operator and denoted by • or $\wedge$, and the negation or NOT operator, represented by the arithmetic symbol – or $\neg$. A literal is either a variable v or its negation $\overline{v}$. A product π is a set of literals that does not contain a literal and its opposite. Typically, it is assimilated with the conjunction of its elements.

A miniterm on a set of variables X is a product that contains a literal built over each variable of X. For n variables, there exist 2^n miniterms that can be constructed on X.

An assignment σ of a set of variables X is a mapping from X to $\{0,1\}$ that assign a value to each variable of X (true=1/false=0). There is a one to one correspondence between miniterms over a finite set of variables X and assignments. An assignment (equivalently a miniterm) satisfies a formula F if $\sigma(F)=1$. In this case we say that σ belongs to F, i.e., $\sigma\in F$, and that σ is a solution of F.

There exist a natural order over literals: $\overline{v}<v$. This order can be an extender to miniterms: $\pi\leq\rho$ if for each variable of X, $\pi(v)\leq\rho(v)$. A formula F is monotone if for any pair of miniterms σ, ρ that satisfy F such that $\sigma\leq\rho$, then $\rho\in F$ implies that $\pi\in F$. The monotonic Boolean functions are precisely those functions, which can be defined only with AND, OR, and K/N operators and do not contain negations.

A product σ that satisfies a function F is also called an implicant of F. An implicant of F is prime if no proper subset of it is an implicant of F. In the general case, if the function in not monotone, prime implicants may contain negated variables. Any formula is equivalent to the disjunction of its prime implicants, or equivalently to a set of miniterms that satisfy it, leading to a representation in terms of a disjunction of conjunctions also called the sum of products.

For any two formulae F and G, we say that F implies G if for any assignment satisfying F $\sigma\in F$, then it satisfies G as well. This is denoted by $F\models G$.

We denote by $F_{v\leftarrow e}$ the function in which the value of v is substituted by the constant $e\in\{0,1\}$. $F_{v\leftarrow 1}$ and $F_{v\leftarrow 0}$ are the positive and the negative cofactors of F w.r.t. the variable v.

2.2. Boolean models

Boolean models are commonly used in risk analysis of industrial facilities to develop a representation of the overall system in terms of logic diagrams. In the case of PSA studies, the technique used for the schematic representation of the facility is a combination of fault trees and event trees.

Fault Trees are deductive models used to identify the causes of failures of a system in terms of its subsystems and basic component failures. The basic events represent component failures and unavailabilities or human errors, to which a probability distribution is associated (i.e. events for which data are available). From a mathematical point of view, a fault tree is a Boolean formula. Variables correspond to basic events of the tree, internal tree nodes, or gates corresponding to formula connectives, and the final equation of the formula represents the top event of the tree.

Fault trees are classified according to their logic into coherent and non-coherent categories. In a coherent fault tree, each component in the system is relevant, and the structure function is monotonically increasing. A fault tree that contains only AND gates, OR gates, and/or independent events is always coherent. Whenever a NOT logic gate is introduced or directly implied into a fault tree, the latter is likely to become non-coherent. In non-coherent fault trees, the working or success states of components as well as their failures (negative and positive events, respectively) contribute to the failure of the system. If the NOT logic can be eliminated from the fault tree, the fault tree is coherent. If the NOT logic cannot be eliminated from the fault tree, the fault tree is non-coherent. For a more precise definition of coherency based on the structure function of the fault tree, see [7].

Traditional solution of coherent fault trees involves the determination of the so-called minimal cutsets (MCSs). They represent the minimal combinations of component failures leading to a failure. For coherent fault trees, this definition matches the formal notion of prime implicant and so the function can be expressed as a disjunction of all its MCSs. However, this is not the case for non-coherent fault trees because these no longer have the monotone properties. For this later case, the notion of MCS should be replaced by the notion of prime implicants. The mathematical details of these concepts are expounded in [8].

Event Trees constitute an inductive technique used to examine all possible responses to a potential hazardous initiating event (called the initiator). It works forward in time considering all possible subsequent events until the consequences are known—either the system reaches a stable state or some level of failure or damage occurs. Branch points on the tree structure represent the success or failure of the systems and operator actions designed to respond in order to mitigate the initiating event. In its graphical representation, upper branches represent successes of the corresponding safety system or event, while lower branches represent its failure. Note that the existence of the success branches makes the Event Trees intrinsically non-coherent.

Concerning the integration of the fault trees and event trees models, in the nuclear PSA studies, there has been traditionally two different modelling approaches: the fault trees and the event tree linking approaches [9]. They both utilize a combination of fault trees and event trees to represent the model, although they