ETH zürich

ETH Library

Analytical solutions of linked fault tree probabilistic risk assessments using binary decision diagrams with emphasis on nuclear safety applications

Doctoral Thesis

Author(s):
Nusbaumer, Olivier P.M.

Publication date:
2007

Permanent link:
https://doi.org/https://doi.org/10.3929/ethz-a-005506737

Rights / license:
In Copyright - Non-Commercial Use Permitted

This page was generated automatically upon download from the ETH Zurich Research Collection.
For more information, please consult the Terms of use.

DISS. ETH NO. 17286

Analytical Solutions of Linked Fault Tree Probabilistic Risk Assessments using Binary Decision Diagrams with Emphasis on Nuclear Safety Applications

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZURICH

for the degree of
Doctor of Technical Sciences

presented by

OLIVIER P. M. NUSBAUMER

Dipl. Masch. Ing. ETH
born 4th November 1975
citizen of Develier (JU), Switzerland

accepted on the recommendation of

Prof. Dr. Wolfgang Kröger, examiner
Prof. Dr. Enrico Zio, co-examiner

Zurich, 2007

Abstract

This study is concerned with the quantification of Probabilistic Risk Assessment (PRA) using linked Fault Tree (FT) models.

Probabilistic Risk Assessment (PRA) of Nuclear Power Plants (NPPs) complements traditional deterministic analysis; it is widely recognized as a comprehensive and structured approach to identify accident scenarios and to derive numerical estimates of the associated risk levels. PRA models as found in the nuclear industry have evolved rapidly. Increasingly, they have been broadly applied to support numerous applications on various operational and regulatory matters. Regulatory bodies in many countries require that a PRA be performed for licensing purposes. PRA has reached the point where it can considerably influence the design and operation of nuclear power plants.

However, most of the tools available for quantifying large PRA models are unable to produce analytically correct results. The algorithms of such quantifiers are designed to neglect sequences when their likelihood decreases below a predefined cutoff limit. In addition, the rare event approximation (e.g. Moivre's equation) is typically implemented for the first order, ignoring the success paths and the possibility that two or more events can occur simultaneously. This is only justified in assessments where the probabilities of the basic events are low. When the events in question are failures, the first order rare event approximation is always conservative, resulting in wrong interpretation of risk importance measures.

Advanced NPP PRA models typically include human errors, common cause failure groups, seismic and phenomenological basic events, where the failure probabilities may approach unity, leading to questionable results. It is accepted that current quantification tools have reached their limits, and that new quantification techniques should be investigated.

A novel approach using the mathematical concept of Binary Decision Diagram (BDD) is proposed to overcome these deficiencies. BDDs have the remarkable properties of having complexity that is not related to the number of prime implicants of the encoded Boolean formula and of

having polynomial time complexity. Since a BDD analytically encodes a Boolean formula, the failure probability of the top event can be deduced without the need to resort to any numerical approximations. This approach is therefore an interesting technique for fault tree assessment.

However, extended efforts are required when converting a given fault tree structure to its BDD form; the complexity associated with the conversion can be considerably reduced by optimizing the order of the basic events in the BDD. This optimization problem was proved to be of NP-complete complexity.

Heuristics have been developed and investigated as a case study on the full scope PRA model of the Leibstadt Nuclear Power Plant. Several static and dynamic optimization techniques are proposed to optimize large problems.

In order to evaluate these techniques in practice, a software tool (*NeuralSpectrum*) has been developed as part of this study. The software is an integrated fault tree / BDD tool that features a fault tree package, a BDD engine and a minimal cutset engine, with dedicated fault tree to BDD conversion and optimization routines. The optimization routines include global, static (pre-processing), dynamic and local (BDD objects) techniques.

The combination of global, static, dynamic and local optimization techniques proved to be effective when dealing with large models. The Leibstadt PRA model was successfully converted to a BDD form of more than 1'500'000 nodes, for a total of about 3'650 basic events. The BDD covers a complete event tree sequence that includes reactor shutdown and reactor cooling with all Emergency Core Cooling Systems (including all support systems) of the Leibstadt Nuclear Power Plant.

The impact of the different approximations used in the classical approach is evaluated using the Leibstadt PRA model, by comparing the approximated results to exact BDD results. The comparison shows that the classical approach produces accurate results for internal event assessments, but fails for external event assessments or Level 2 PRA, where the probability values are typically much higher.

The analytical quantification of large linked fault tree models using BDDs requires complex algorithms and programming techniques, which have been evaluated for the first time on a fullscope PRA model in this study. This study demonstrated the feasibility of implementing BDDs for the analytical quantification of large fault tree models as found in the nuclear industry. The implementation of BDD turns out to be the most promising approach for analytical fault tree model solving. This important insight should be put in focus when considering the increasing demand on PRA related applications, such as risk-informed decision making in modern industries and services.

Abstract in German

Die vorliegende Studie befasst sich mit der methodisch optimierten Quantifizierung probabilistischer Risikoanalysen (PRA) über die Umwandlung von grossen Fehlerbaummodellen in binäre Entscheidungsdiagramme (BDD).

PRA von Kernkraftwerken bieten einen umfassenden und strukturierten Ansatz zur Identifizierung von Störfallszenarien und Ableitung numerischer Grössen der damit verbundenen Risiken. Sie ergänzen damit die üblichen deterministischen Analysen zum Nachweis ausreichender Vorsorge gegen Störfälle in Kernkraftwerken. In vielen Ländern verlangen die zuständigen Aufsichtsbehörden, dass eine PRA für die Lizenzierung und den Dauerbetrieb von Kernkraftwerken vorliegt. Die PRA sind damit an einem Punkt angelangt, wo sie bedeutende Beiträge zur Auslegung und zum Betrieb von Kernkraftwerken liefern müssen.

Allerdings sind die heute zur Verfügung stehenden Quantifizierungswerkzeuge umfassender PRA-Modelle nicht in der Lage, analytisch korrekte Resultate zu liefern. Die üblichen Algorithmen solcher Werkzeuge sind so ausgelegt, dass Unfallsequenzen vernachlässigt werden, falls ihre Wahrscheinlichkeit unter ein festgelegtes Abschneidekriterium fällt. Eine Näherung erster Ordnung (nach der Gleichung von Moivre) ist üblich, so dass Erfolgspfade und das mögliche gleichzeitige Auftreten mehrerer Ereignisse ignoriert werden. Dies ist methodisch aber nur dann gerechtfertigt, wenn die Wahrscheinlichkeiten der Basisereignisse sehr klein sind. Sind die modellierten Ereignisse Ausfälle, werden immer konservative Ergebnisse geliefert, was letztlich zu einer falschen Beurteilung der Importanzwerte der Basisereignisse führt.

Fortgeschrittene PRA-Modelle für Kernkraftwerke beinhalten menschliche Fehlhandlungen, Gruppen von Fehlern gemeinsamer Ursache, seismische und phänomenologische Basisereignisse, für die sich die entsprechenden Ausfallswahrscheinlichkeiten näherungsweise Eins annähern können, was bei den etablierten Methoden zu fraglichen Ergebnissen führen muss. Es ist allgemein anerkannt, dass die zurzeit verwendeten Quantifizierungswerkzeuge ihre Grenzen erreicht haben. Neue Quantifizierungsmethoden müssen somit erforscht und entwickelt werden.

Ein neuartiger Denkansatz zur Überwindung der beschriebenen Defizite ist die Anwendung

binärer Entscheidungsdiagramme (BDD). BDDs besitzen die Vorteile, dass ihre Komplexität unabhängig von der Anzahl der Primimplikanten der zu Grunde liegenden Booleschen Funktionen ist, und dass sie polynomische Zeitkomplexität aufweisen. Da BDDs Boolesche Funktionen analytisch darstellen, lässt sich die Ausfallwahrscheinlichkeit eines Top-Ereignisses ohne numerische Näherungen ableiten. Der BDD-Ansatz wird dadurch zu einer interessanten Methodik zur realitätsnahen Bewertung von Fehlerbäumen.

Allerdings sind grosse Anstrengungen für die Umwandlung vorhandener Fehlerbäume in ein BDD-Format notwendig. Die mit der Umwandlung verbundene Komplexität kann durch die Optimierung der Reihenfolge der Basisereignisse in der BDD-Darstellung beträchtlich reduziert werden. Dieses Optimierungsproblem erwies sich als Bestandteil der Komplexitätsklasse "NP-Komplett". Heuristische Methoden wurden anhand einer Fallstudie mit dem PRA-Gesamtanlagemodell des Kernkraftwerkes Leibstadt (KKL) entwickelt und untersucht. Statische und dynamische Optimierungstechniken werden vorgeschlagen und angewendet.

Um diese Methoden bezüglich ihrer Praxistauglichkeit zu beurteilen, wurde eine Software-Anwendung (*NeuralSpectrum*) als Teil der vorliegenden Studie entwickelt, die über eine integrierte Fehlerbaum/BDD-Engine verfügt. Diese Engine besteht aus einem Fehlerbaum-, einem BDD- und einem Minimal-Cutset-Modul sowie aus Routinen zur Umwandlung von Fehlerbäumen zu BDD und zur Optimierung. Letztere beinhalten globale, statische (pre-processing), dynamische und lokale (BDD-Objekte) Methoden.

Die Kombination dieser Optimierungsmethoden hat sich im Zusammenhang mit grossen PRA-Modellen als leistungsfähig erwiesen: das PRA-Modell des KKL liess sich erfolgreich in ein BDD mit mehr als 1'500'000 Knoten konvertieren, bei einem Total von ungefähr 3'650 Basisereignissen. Das BDD deckt dabei eine komplette, relevante Unfallsequenz mit Reaktorabschaltung und Reaktorkühlung, mit allen Kernnotkühlsystemen und zugehörigen Hilfssystemen, ab.

Die analytische Quantifizierung von grossen verknüpften Fehlerbaummodellen mit BDDs benötigt komplexe Algorithmen und Programmiertechniken, welche zum ersten Mal mit einem PRA-Gesamtanlagemodell untersucht wurden. Die Studie hat die Einsetzbarkeit von BDDs zur analytischen Quantifizierung grosser Fehlerbaummodelle, wie sie in der Nuklearindustrie vorkommen, nachgewiesen. Diese wichtige Einsicht muss im Hinblick auf die zunehmenden PRA-Anforderungen, wie "Risikoinformierte Entscheidungsfindung" in modernen Industrie- und Dienstleistungsbetrieben, hervorgehoben werden.