

Theoretical and methodological extensions to dynamic reliability analysis

Tero Tyrväinen



Theoretical and methodological extensions to dynamic reliability analysis

Tero Tyrväinen

A doctoral dissertation completed for the degree of Doctor of Science (Technology) to be defended, with the permission of the Aalto University School of Science, at a public examination held at the lecture hall H304 of the school (Otakaari 1, 02150 Espoo, Finland) on 13 October 2017 at 12 noon.

Aalto University
School of Science
Department of Mathematics and Systems Analysis
Systems Analysis Laboratory

Supervising professor

Professor Ahti Salo, Aalto University School of Science, Finland

Thesis advisors

Dr. Jan-Erik Holmberg, Risk Pilot AB, Finland

Professor Ahti Salo, Aalto University School of Science, Finland

Preliminary examiners

Professor Tunc Aldemir, Ohio State University, USA

Professor Lixuan Lu, University of Ontario, Institute of Technology, Canada

Opponent

Professor Tim Bedford, University of Strathclyde, United Kingdom

Aalto University publication series

DOCTORAL DISSERTATIONS 154/2017

VTT SCIENCE 161

© 2017 Tero Tyrväinen

ISBN 978-952-60-7571-6 (printed)

ISBN 978-952-60-7570-9 (pdf)

ISSN-L 1799-4934

ISSN 1799-4934 (printed)

ISSN 1799-4942 (pdf)

<http://urn.fi/URN:ISBN:978-952-60-7570-9>

ISBN 978-951-38-8565-6 (printed)

ISBN 978-951-38-8564-9 (pdf)

ISSN-L 2242-119X

ISSN 2242-119X (printed)

ISSN 2242-1203 (pdf)

<http://urn.fi/URN:ISBN:978-951-38-8564-9>

Unigrafia Oy

Helsinki 2017

Finland



Author

Tero Tyrväinen

Name of the doctoral dissertation

Theoretical and methodological extensions to dynamic reliability analysis

Publisher School of Science

Unit Department of Mathematics and Systems Analysis

Series Aalto University publication series DOCTORAL DISSERTATIONS 154/2017

Field of research Systems and Operations Research

Manuscript submitted 9 June 2017

Date of the defence 13 October 2017

Permission to publish granted (date) 16 August 2017

Language English

Monograph

Article dissertation

Essay dissertation

Abstract

Rigorous analysis of the reliability of a dynamic system calls for modelling of the dynamic behaviour of the system and its interactions. However, traditional and the most frequently used reliability analysis methods, such as fault tree analysis, are static and have only limited capability to represent dynamic systems. Therefore, dynamic reliability analysis methods have been studied since 1990s.

Dynamic flowgraph methodology (DFM) is a method for the reliability analysis of dynamic systems containing feedback loops. A DFM model is a dynamic graph representation of the analysed system. DFM has been most often applied to different digital control systems. One reason for this is that a DFM model can represent the interactions between a control system and the controlled process.

The main goal of DFM analysis is to identify prime implicants, which are minimal combinations of events and conditions that cause the analysed top event, for example, system failure. This dissertation strengthens the mathematical foundation of DFM by developing an improved definition of a prime implicant.

Risk importance measures can be used to identify components and basic events that are most important for the reliability of the system. This dissertation develops new dynamic risk importance measures as generalisations of two traditional risk importance measures for the needs of DFM. Unlike any other importance measure, the dynamic risk importance measures utilise all the information available in prime implicants of DFM. They primarily measure the importances of different states of components and variables of a DFM model. The computation of the dynamic risk importance measures for failure states of components provides significant additional information compared to other importance values.

This dissertation also examines common cause failures (CCFs) in dynamic reliability analysis. Taking CCFs into account is important when modelling systems with redundancies. The dissertation extends the DFM by presenting CCF models that take failure times of components into account.

Keywords Reliability analysis; dynamic system; risk importance measure; common cause failure; prime implicant; digital control system

ISBN (printed) 978-952-60-7571-6

ISBN (pdf) 978-952-60-7570-9

ISSN-L 1799-4934

ISSN (printed) 1799-4934

ISSN (pdf) 1799-4942

Location of publisher Helsinki

Location of printing Helsinki

Year 2017

Pages 111

urn <http://urn.fi/URN:ISBN:978-952-60-7570-9>

Tekijä

Tero Tyrväinen

Väitöskirjan nimi

Teoreettisia ja menetelmällisiä laajennuksia dynaamiseen luotettavuusanalyysiin

Julkaisija Perustieteiden korkeakoulu**Yksikkö** Matematiikan ja systeemianalyysin laitos**Sarja** Aalto University publication series DOCTORAL DISSERTATIONS 154/2017**Tutkimusala** Systeemi- ja operaatiotutkimus**Käsikirjoituksen pvm** 09.06.2017**Väitöspäivä** 13.10.2017**Julkaisuluvan myöntämispäivä** 16.08.2017**Kieli** Englanti **Monografia** **Artikkeliväitöskirja** **Esseeväitöskirja****Tiivistelmä**

Dynaamisen järjestelmän luotettavuuden tarkka analyysi vaatii järjestelmän dynaamisen käyttäytymisen ja vuorovaikutusten mallintamista. Kuitenkin perinteiset ja useimmin käytetyt luotettavuusanalyysimenetelmät, kuten vikapuuanalyysi, ovat staattisia ja niiden sopivuus dynaamisten järjestelmien kuvaamiseen on rajallinen. Siksi dynaamisen luotettavuusanalyysin menetelmiä on tutkittu 1990-luvulta lähtien.

Dynaaminen vuokaaviomallintaminen on menetelmä takaisinkytkentöjä sisältävien dynaamisten järjestelmien luotettavuusanalyysiin. Dynaaminen vuokaaviomalli on dynaaminen verkkoesitys analysoidusta järjestelmästä. Dynaamista vuokaaviomallinnusta on useimmin sovellettu erilaisiin digitaalisiin ohjausjärjestelmiin. Yksi syy tälle on, että dynaaminen vuokaaviomalli pystyy kuvaamaan ohjausjärjestelmän ja ohjattavan prosessin väliset vuorovaikutukset.

Päätavoite dynaamisessa vuokaaviomallinnuksessa on tunnistaa minimitermit (prime implicants), jotka ovat tapahtumien ja tilojen minimaalisia yhdistelmiä, jotka aiheittavat tarkasteltavan huipputapahtuman, esimerkiksi järjestelmän vikaantumisen. Tämä väitöskirja vahvistaa dynaamisen vuokaaviomallintamisen matemaattista perustaa kehittämällä paremman määritelmän minimitermille.

Riskitärkeysmittoja voidaan käyttää järjestelmän luotettavuuden kannalta tärkeimpien komponenttien ja perustapahtumien tunnistamiseen. Tämä väitöskirja kehittää uudet dynaamiset riskitärkeysmitat yleistyksinä kahdesta perinteisestä riskitärkeysmitasta dynaamisen vuokaaviomallinnuksen tarpeisiin. Toisin kuin mikään muu tärkeysmitta, dynaamiset riskitärkeysmitat hyödyntävät kaiken dynaamisen vuokaaviomallinnuksen minimitermeihin sisältyvän tiedon. Ne mittaavat ensisijaisesti dynaamisen vuokaaviomallin komponenttien ja muuttujien eri tilojen tärkeyksiä. Dynaamisten riskitärkeysmittojen laskenta komponenttien vikatiloille antaa merkittävää lisätietoa verrattuna muihin tärkeysarvoihin.

Tämä väitöskirja tutkii myös yhteisvikoja dynaamisessa luotettavuusanalyysissä. Yhteisvikojen huomioiminen on tärkeää redundansseja sisältävien järjestelmien mallinnuksessa. Väitöskirja laajentaa dynaamista vuokaaviomallinnusta esittämällä yhteisvikamalleja, jotka huomioivat komponenttien vikaantumisten ajankohdat.

Avainsanat Luotettavuusanalyysi; dynaaminen järjestelmä; riskitärkeysmitta; yhteisvika; minimitermi; digitaalinen ohjausjärjestelmä

ISBN (painettu) 978-952-60-7571-6**ISBN (pdf)** 978-952-60-7570-9**ISSN-L** 1799-4934**ISSN (painettu)** 1799-4934**ISSN (pdf)** 1799-4942**Julkaisupaikka** Helsinki**Painopaikka** Helsinki**Vuosi** 2017**Sivumäärä** 111**urn** <http://urn.fi/URN:ISBN:978-952-60-7570-9>

Preface

This dissertation would not have been possible without my instructor Jan-Erik Holmberg. I would like to thank him for the interesting topic and all the guidance during these six years. I would also like to thank professor Ahti Salo for supervising and guiding the work. My co-worker and Master's thesis instructor Kim Björkman also gave me remarkable support, especially at the early phase of the work and concerning software implementations. All in all, our co-operation has been very fruitful throughout the years. In addition, I would like to thank those who have provided useful comments to my manuscripts, notably Antti Toppila and Ilkka Karanta. I would also like to thank my opponent professor Tim Bedford and preliminary examiners professor Tunc Aldemir and professor Lixuan Lu.

Large part of the work of this dissertation was conducted in The Finnish Research Programme on Nuclear Power Plant Safety 2011-2014 (SAFIR-2014) and some of the writing was also performed in SAFIR2018. Most of the work was performed in the SARANA project led by Janne Valkonen. I would finally like to thank SAFIR programme director Jari Hämäläinen and former director Kaisa Simola, because they are actually the persons, along with Jan-Erik Holmberg, who originally gave me this job opportunity at VTT.

Espoo, August 24, 2017,

Tero Tyrväinen

Contents

1. Introduction	1
1.1 Background	1
1.2 Objectives	3
2. Methodological background	5
2.1 Fault tree analysis	5
2.2 Binary decision diagrams	6
2.3 Markov modelling	7
2.4 Dynamic flowgraph methodology	8
2.5 Risk importance measures	12
2.6 Common cause failures	14
3. Results	17
3.1 Prime implicants	17
3.2 Risk importance measures	18
3.3 Common cause failures	19
4. Discussion and conclusions	21
Bibliography	25
Publications	

List of Publications

This thesis consists of an overview and of the following publications which are referred to in the text by their Roman numerals.

I Tyrväinen, T. Prime implicants in dynamic reliability analysis. *Reliability Engineering and System Safety*, Vol. 146, pp. 39-46, doi: 10.1016/j.ress.2015.10.007, February 2016.

II Tyrväinen, T. Risk importance measures in the dynamic flowgraph methodology. *Reliability Engineering and System Safety*, Vol. 118, pp. 35-50, doi: 10.1016/j.ress.2013.04.013, October 2013.

III Tyrväinen, T. Common cause failures in the dynamic flowgraph methodology. *Manuscript*, 19+17 pages, 2017.

Author's Contribution

Tyrväinen is the sole author in all the papers contained in the Dissertation.

1. Introduction

1.1 Background

Comprehensive risk analysis [1] of a complex system calls for a systematic identification of all significant accident scenarios, and assessment of the likelihood and consequences of each accident scenario. Probabilistic risk analysis (PRA) [2] is an approach that has been widely used in the risk analysis of complex facilities, especially nuclear power plants. Compared to qualitative risk analysis methods [3], PRA is more precise and more effective when a large number of complex accident sequences needs to be analysed. Usually, the main purpose of PRA is to support risk-informed decision making and to help fulfil regulatory requirements. PRA can point out the weaknesses of the analysed system, and the system's reliability can be improved effectively on the basis of the results of PRA.

PRA modelling is generally performed using fault trees [4, 5] and event trees [2]. An event tree models how an accident can progress from an initiating event to different consequences depending on a set of nodal questions e.g. about which safety systems fail. The probabilities of different event tree branches can be calculated using fault trees. A fault tree typically represents the failure logic of the analysed system and thus helps to determine which component failure and event combinations can cause the system to fail. The probability of the system's failure can be calculated from the fault tree if the probabilities of its basic events (e.g. component failures) are known. This computation is usually based on minimal cut sets [4], which are minimal combinations of basic events that can cause the top event, such as failure of the system. The probabilities can be estimated on the basis of operational data or determined by expert judgement.

Fault tree analysis is currently the leading method for risk and reliability analysis of complex systems. However, fault trees are static and have only limited capability to represent dynamic systems such as digital control systems. Dynamic interactions between software and hardware or interactions between the control system and the controlled process cannot be modelled properly using fault trees. In addition, fault trees do not support non-binary logic or modelling of the system's evolution in time. This has motivated the extensive development of dynamic reliability analysis methods since the 1990s [6].

Dynamic flowgraph methodology (DFM) is a method for the reliability analysis of dynamic systems containing feedback loops [7, 8, 9]. As in fault tree analysis, the aim of DFM is to identify which conditions can cause a top event, which can be e.g. system failure. A DFM model is a graph representation of the analysed system. The components of DFM models are analysed at discrete time points, and they can have multiple states. DFM has most often been applied to different digital control systems that include both hardware and software components. One reason for this is that a DFM model can represent the interactions between a control system and the controlled process.

The main alternative to DFM is the methodology that combines Markov modelling and cell-to-cell mapping (CTCM) technique [10, 11, 12]. Markov models can represent the dynamic and multi-state logic of a system to a degree of accuracy that is comparable to DFM. The main difference is that every state transition is associated with a probability in Markov models. Other dynamic reliability and risk analysis methods include dynamic event trees [13, 14, 15], Petri nets [16], event sequence diagrams [17], GO-FLOW methodology [18] and dynamic fault trees [19]. In addition, there are some Monte Carlo simulation based methods for the reliability analysis of digital instrumentation and control systems [20, 21, 22].

Broadly viewed, there are two main approaches to analyse the reliability of a dynamic system:

1. to simulate the system (inductive analysis),
2. to identify different ways in which the system can fail, e.g. minimal cut sets, and to determine the system's failure probability based on this kind of logical analysis (deductive analysis).

Some dynamic models, such as DFM and Markov models, can be solved in both ways. Markov models have been used more for inductive analysis,

whereas DFM has been considered more suitable for deductive analysis.

Although risk importance measures [23] and common cause failures [24] are important areas of reliability theory, they have not been studied much in the context of DFM. Risk importance measures can be used to identify components and basic events that are most important with regard to the system's reliability. The importance of a component depends both on the reliability of the component and the consequences that its failure would have on the system's reliability. Risk importance values help to determine how the system's reliability can best be improved.

A common cause failure (CCF) means that multiple components fail due to a common cause [25]. A CCF can occur between components that share some failure mechanism which can cause them to fail simultaneously or during a relatively short time window, for instance during the PRA mission time which is usually 24 hours. Modelling CCFs is an important part of the reliability analysis of complex systems including redundant components. If CCFs are not taken into account, the risk of the system's failure can be underestimated.

1.2 Objectives

This dissertation develops new risk importance measures for DFM. Traditional risk importance measures have been developed for binary and static logic, meaning that they cannot directly be applied in DFM. Some risk importance measures have previously been developed for DFM [26, 27], but they have limitations. For example, they cannot fully measure the importances of different failure modes of components, because they are not formulated for the states of nodes of DFM. Neither do they consider information about the timings of events and conditions properly. This motivates the development of new risk importance measures for measuring the importances of states of components and for taking the time aspect of DFM into account. The new importance measures also need to support the interpretation of results.

Another objective of this dissertation is to study CCFs in the DFM context, which has not been addressed in the earlier literature. Model in [28] included CCFs, but they were not really discussed in the paper. Approaches for the modelling of CCFs as well as the computation of CCF probabilities are developed. Compared to static analysis, DFM introduces a new dimension in that it considers the failure times of components. It

needs to be considered how the failure times should be taken into account in the CCF modelling and the calculation of probabilities.

One important basis for risk importance measure calculation and CCF modelling is the interpretation of DFM results. The primary result of DFM analysis is a set of prime implicants [29], which are minimal combinations of events and conditions that are sufficient to cause the top event. The interpretation of prime implicants is not always completely clear and unambiguous, for example when non-repairable components are considered as identified in the author's MSc thesis [30]. Therefore, the definition and interpretation of prime implicants are also studied in this dissertation.

2. Methodological background

The most often used reliability analysis method, fault tree analysis, is summarised in Section 2.1. Section 2.2 presents binary decision diagrams, because they are a commonly used method to solve a reliability model and they have been applied to DFM analysis. Markov modelling is described briefly in Section 2.3 because it is the most often used dynamic reliability analysis method and the main alternative to DFM. Sections 2.4-2.6 present DFM, risk importance measures and CCFs as the main background for the results of the dissertation, presented in Chapter 3.

2.1 Fault tree analysis

Fault tree analysis [4, 5] is a widely used method to estimate the failure probability of a system. A fault tree represents the ways in which the system can fail. It is a graphical tree structure in which basic events (component failures and other events that can cause the system to fail) are connected using logical gates, such as OR and AND; there are equivalent Boolean operations [31] (+ and \cdot).

A fault tree is typically used to identify minimal cut sets [4]. A cut set is a set of basic events that causes the top event which represents the system's failure. A minimal cut set is a cut set that contains the minimal number of basic events. Thus if one of the basic events is removed from the minimal cut set, it is not a cut set any more and the system does not fail.

The probability of the top event can be calculated on the basis of minimal cut sets and the probabilities of basic events [32]. It is also possible to calculate the top event probability directly from the fault tree without the identification of minimal cut sets. On the other hand, the analysis can also focus only on the identification of minimal cut sets if the probability

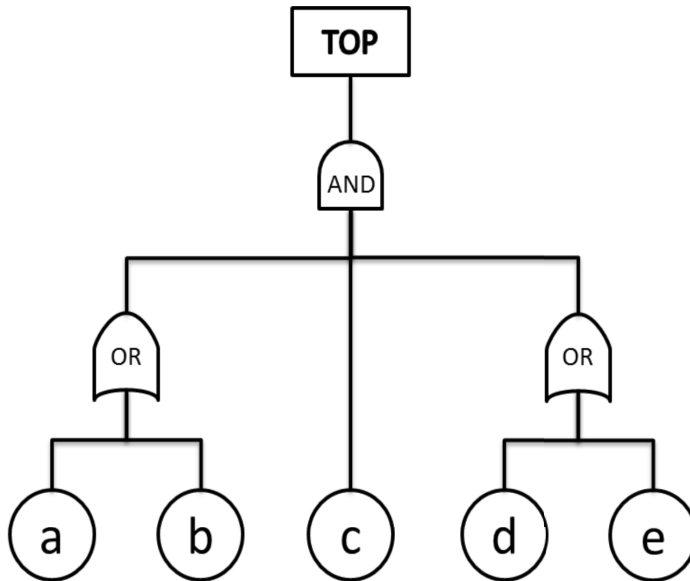


Figure 2.1. A fault tree with five basic events.

estimates of basic events are not available. Minimal cut sets themselves are useful qualitative information.

An example of a fault tree is presented in Figure 2.1. Boolean formula representation of the fault tree is $F = (a+b) \cdot c \cdot (d+e) = acd + ace + bcd + bce$. The minimal cut sets of the fault tree are acd , ace , bcd and bce .

2.2 Binary decision diagrams

A binary decision diagram (BDD) [33, 34] is an efficient data structure for symbolic Boolean manipulation. It is a directed acyclic graph that consists of decision nodes, two kinds of edges, 0-edges and 1-edges, and terminal nodes, 1-terminal and 0-terminal. In a BDD, each decision node, representing a Boolean variable, has a 0-edge and a 1-edge. When a BDD represents a Boolean formula, each path from the root node to the 0-terminal or the 1-terminal represents a Boolean assignment.

BDDs are based on repeated application of the Shannon expansion formula [34]

$$F = x \cdot F|_{x=1} + \bar{x} \cdot F|_{x=0}, \quad (2.1)$$

where F is a Boolean formula, x is a Boolean variable, \bar{x} is the negation of variable x , $F|_{x=1}$ is Boolean formula F with condition that $x = 1$, and $F|_{x=0}$ is Boolean formula F with condition that $x = 0$. For example, if

$F = abc + ad$, F can be presented in form

$$\begin{aligned} F &= a \cdot (bc + d) \\ &= a \cdot (b \cdot (c + d) + \bar{b} \cdot d) \\ &= a \cdot (b \cdot (c + \bar{c} \cdot d) + \bar{b} \cdot d). \end{aligned}$$

Reliability analysis has been one application area of BDDs [35, 36, 37]. For example, a fault tree can be transformed into a BDD. Minimal cut sets can be generated from a BDD representing a fault tree, or the top event probability can directly be calculated from the BDD. In a BDD, each path ending in the 1-terminal also corresponds to a cut set, and these cut sets are mutually exclusive, which is an advantage compared to fault trees.

2.3 Markov modelling

Markov modelling is described briefly in this section because it is the most often used dynamic reliability analysis method and the main alternative to DFM. A Markov model consists of a set of system states, and transition rates between the states [38]. A Markov model is usually analysed in discrete time steps. The probabilities of different system states at a time step can be calculated on the basis of the probabilities of the states at the previous time step and the state transition rates. Typically, initial probabilities are defined for the system states, whereafter probabilities for how the states evolve in time are calculated.

The methodology of Markov/CTCM [10, 11, 12] has been applied to the reliability analysis of dynamic systems. In CTCM, the variables of the analysed system are discretised to a finite number of states. The variables can, for example, be physical variables such as water level or represent states of components such as a valve. States of different variables are combined to form state combinations called *cells*. These cells are then used as system states in a Markov model. The transition rates between the cells are determined e.g. on the basis of physical equations, system design and estimated failure rates of components. From the model, it is possible to analyse the ways in which some postulated top event can occur [12, 39] and how probable this event is or, alternatively, how the system evolves on the basis of some initial conditions [8, 11].

2.4 Dynamic flowgraph methodology

A DFM model [7, 8, 9, 40, 41, 42, 43, 44] is a graph representation of the analysed system. Nodes in the model represent the components and variables of the system, and edges connecting the nodes represent causal and other dependencies between the nodes. These dependencies can involve time delays, and nodes can have two or more states. If a node does not depend on any other node, it is a stochastic node, the state of which is determined by a discrete probability distribution at each time step. The state of a deterministic node is determined on the basis of the states of input nodes. Each deterministic node has a decision table which specifies the output state for each state combination of the input nodes. Decision tables can be constructed on the basis of empirical knowledge about the system, physical equations, simulations, expert judgement, software design or software code.

Figure 2.2 shows a simple DFM model of a tank system with a valve that is controlled on the basis of water level measurement, and Table 2.1 gives the decision table of node V as an example. In the model, node V represents the functional state of a valve (state 0 for closed and 1 for open), L represents the water level and M represents the water level measurement value. Nodes M and L have three states $-1, 0$ and 1 indicating water levels low, medium and high. Nodes S and F are stochastic nodes determining whether the water level measurement and the valve have failed. A row in the decision table specifies a combination of states of the input nodes, and the corresponding state of the output node. Delays in the dependencies are shown in the time lag row. Table 2.1 can be interpreted so that the valve is stuck in its previous state if it has failed (F is 1). Otherwise, the valve is opened if the water level measurement has a high value and closed if the water level measurement has a low value.

The primary target of DFM is usually to identify prime implicants of the top event [29]. An implicant is a combination of conditions that causes the top event, and a prime implicant is a minimal combination of conditions that is sufficient to cause the top event. In DFM, these conditions are represented by literals. In this context, a literal is a triplet consisting of a variable V , state s and time point $-t$, and denoted as $V_s(-t)$. A literal can, for example, represent a value of a physical variable or a state of a component, or indicate the occurrence of some event at a particular time step. Prime implicants of DFM can be interpreted as multi-state and

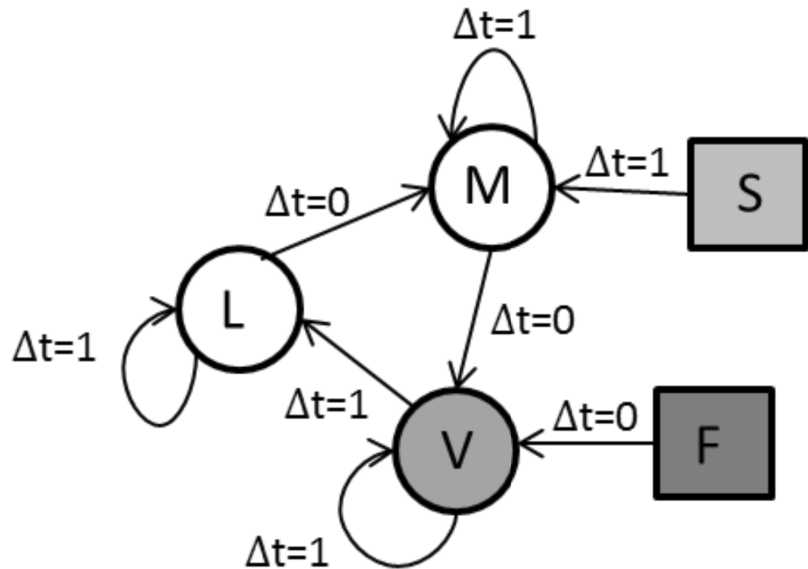


Figure 2.2. A DFM model.

Table 2.1. The decision table of node V.

	Output	Inputs		
Node	V	F	M	V
Time lag		0	0	1
	0	0	-1	0
	0	1	-1	0
	0	0	0	0
	0	1	0	0
	1	0	1	0
	0	1	1	0
	0	0	-1	1
	1	1	-1	1
	1	0	0	1
	1	1	0	1
	1	0	1	1
	1	1	1	1

timed minimal cut sets. Generally, prime implicants are an extension of minimal cut sets for non-coherent logic [35]. Paper I of this dissertation concerns the mathematical definition of a prime implicant.

The top event is also defined as a set of literals. The analyst can freely

choose any top event. Therefore, it is possible to analyse several top events in parallel, and both success and failure scenarios can be analysed.

A DFM model is typically analysed by tracing event sequences backwards from effects to causes [7]. Deductive analysis starts from the top event. The model is traced backwards in the cause-and-effect flow to identify what states of variables produce the top event. The process ends when the initial time step is reached. Prime implicants of a top event can contain initial states of deterministic nodes and states of stochastic nodes at any time step.

DFM analysis does not always have an unambiguous solution, because there are different ways to interpret some literals, prime implicants and constraints related to literals, and to handle the initial time step. Issues related to the interpretation of prime implicants, literals and literal constraints are studied in Paper I of this dissertation.

DFM models can also be analysed inductively by simulating the model with particular initial conditions [45]. All the possible consequences of the system's initial or boundary conditions are generated. The initial or boundary conditions can either be desired or undesired states. If these conditions are desired states, inductive analysis can be used to verify system requirements with the aim of ensuring that operation under normal conditions does not lead to undesired states. If these conditions are undesired states, inductive analysis can be used to verify the system's safety behaviour. Inductive analysis can be used, for example, to analyse the prime implicants identified in deductive analysis in more detail, and to examine the effects of mitigation actions.

DFM involves key concepts such as process node, condition node, causality edge, condition edge, transfer box and transition box (see e.g. [40]). The difference between process nodes and condition nodes is largely based on the modelling philosophy. From a technical point of view, there is no difference. Transfer boxes correspond to decision tables without time lags, and transition boxes correspond to decision tables with time lags. Causality edges connect process nodes, and condition edges connect condition nodes to process nodes via transfer or transition boxes.

The two most frequently cited DFM software tools are Dymonda [46] and Yadrat [41]. Dymonda has been developed by the original developers of DFM. It solves the graph model by transferring it to a set of timed fault trees representing different time steps, or alternatively combining the decision tables of the model into one critical transition table [29]. Dy-

monda solves an initial set of prime implicants directly from the timed fault trees or the critical transition table, and then applies the method of generalized consensus [47, 48] to solve the complete set of prime implicants. Yadrat has been developed by VTT. It transforms the DFM model into a BDD from which the prime implicants are solved. The prime implicant solving methods of the tools have not been compared properly with regard to computation times. A benefit of a BDD is that the non-coherent logic of the model is naturally present in the BDD structure. Because of this, the BDD approach requires less prime implicant processing after initial identification, whereas the Dymonda's approach of using the method of generalized consensus relies heavily on the comparisons between initial prime implicants. On the other hand, multi-state nodes have to be converted into binary variables when a BDD is used, and the prime implicants of the BDD have to be converted back to represent the multi-state logic.

Dymonda and Yadrat use slightly different specifications and terminology. Dymonda follows the official DFM specifications [49]. Yadrat can be considered as an alternative interpretation of the methodology. Despite their differences, the same deductive analyses can be performed using both tools. Yadrat does not provide support for inductive analysis.

In the computation of the top event probability in DFM, the basic idea is similar to the computation of the top event probability in fault tree analysis [32]. In DFM, the top event probability is calculated on the basis of the prime implicants and the probabilities of the literals. Determination of the probabilities of literals has not been addressed much in the literature. Probabilities have been presented mainly considering one time step, whereas time-dependent probability models have not been presented. However, DFM specifications [49] do mention that Dymonda contains time-dependent probability models. In this dissertation (see Paper III), an exponential model with a constant failure rate is used for the computation of failure probabilities. For computation of the top event probability, the usual upper bound algorithms [32] used in fault tree analysis can also be applied in DFM. More accurate top event probability algorithms have also been developed, such as the algorithm presented in [50] and the algorithm cited in [49].

The application areas of DFM have included digital control and safety systems in nuclear power plants [8, 45, 51], space systems [28, 52, 53], hydrogen production plants [40, 54], human performance [55], networked

control systems [9] and field programmable gate arrays (FPGAs) [44, 56]. The reliability analysis of digital systems is considered to be one of the greatest challenges in modern nuclear power plant PRA. Traditional static methods, such as fault trees, cannot capture the dynamic interactions of digital systems very well. NUREG/CR-6901 [57] has identified DFM as one of the promising methods for the reliability analysis of digital I&C systems. DFM has been considered effective in modelling dynamic interactions, such as delays, memories, logic loops and system states [51]. Interactions can, for example, lead to the coupling of events, such as opening of a valve and starting of a pump, and therefore, have a significant effect on the reliability of the system. Multi-state logic is advantageous, because the behaviour of software controlled systems is usually non-binary.

Most DFM models reported in the literature are rather small. To the author's knowledge, the largest model found in the literature represents the FPGA-based reactor trip logic loop in a detailed manner and contains 396 nodes [44]. The complexity of DFM analysis depends on the number of nodes and states of nodes, the complexity of decision tables, and the number of time steps used in the analysis. The computation times are rather sensitive to increase in any of these factors. The model in [44] was traced backwards only one time step, because the computation with multiple time steps would have lasted too long.

Aldemir et al. [8] compared DFM to Markov/CTCM methodology in modelling a digital feedwater control system. The results of the methodologies were consistent. An approach utilising both DFM and Markov analysis was proposed. The authors suggested that DFM could first be used to identify prime implicants. Thereafter, inductive Markov analysis could be performed to validate the prime implicants and to examine their sensitivity to variations of initial conditions.

2.5 Risk importance measures

Risk importance measures [23, 58] are used to analyse which components contribute most to a system's failure probability. This information helps to determine how the system's reliability can be improved effectively, e.g. where to add redundancy, which components to upgrade and how to allocate testing activities. The importance of a component depends on the reliability of the component itself, its position in the system's structure, and the need for the component in the system. The failure probability

of the component is a significant factor, but if the failure of component does not jeopardise the functioning of the system, it is not very important. At least two different importance measures should be used in the importance analysis, because one measure is usually limited to describing the component's influence over the system's reliability from one point of view only.

In the reliability analysis of nuclear power plants, the Fussell-Vesely measure of importance [59, 60] and the risk increase factor [61, 62] (also known as the risk achievement worth) are frequently used risk importance measures. Fussell-Vesely takes into account both the failure probability of the component and the system's capability to survive without the component. Therefore, Fussell-Vesely is typically used as the primary risk importance measure. The risk increase factor measures how much the failure of the component increases the probability of the system's failure. It is a good complement to Fussell-Vesely and it is useful, e.g. when the repairing order of failed components must be decided.

Although the previous paragraphs discussed component failures, risk importance measures can be calculated for any basic event. The Fussell-Vesely measure of importance $I^{FV}(i)$ for basic event i is defined as the probability that at least one minimal cut set containing basic event i has been realised assuming that the system has failed.

Definition 1 *Fussell-Vesely:*

$$I^{FV}(i) := \frac{Q_{TOP}^i}{Q_{TOP}}, \quad (2.2)$$

where Q_{TOP} is the probability that the system fails and Q_{TOP}^i is the probability that a minimal cut set including basic event i causes the system to fail.

The risk increase factor $I^I(i)$ for basic event i is defined as the system's failure probability with the condition that basic event i has occurred divided by the system's failure probability (without any conditions).

Definition 2 *The risk increase factor:*

$$I^I(i) := \frac{Q_{TOP}(i=1)}{Q_{TOP}}, \quad (2.3)$$

where $Q_{TOP}(i=1)$ is the failure probability of the system, given that basic event i has occurred.

2.6 Common cause failures

CCFs [24, 63] are an important part of the reliability analysis of complex systems including redundant components. If CCFs are not taken into account, the risk of the system's failure is likely to be underestimated. In [25], a CCF is defined using the following criteria:

- “1. Two or more individual components fail, are degraded (including failures during demand or in-service testing), or have deficiencies that would result in component failures if a demand signal had been received.
2. Components fail within a selected period of time such that success of the probabilistic risk assessment (PRA) mission would be uncertain.
3. Components fail because of a single shared cause and coupling mechanism.
4. Components fail within the established component boundary.”

There are different ways to model CCFs. In nuclear power plant PRA, parametric models [64] are used most often. In parametric models, the CCF probability is calculated by multiplying individual component failure probability with some CCF parameters. Another option is to estimate the CCF probability independently without considering the failure probabilities of individual components.

Two parametric models, β - and α -factor models, have been used in this dissertation. They are introduced in the following.

Consider a group of m identical components with a common failure mechanism. When CCFs are modelled using the β -factor model, it is assumed that a component can either fail independently or in a CCF of all m components. If a component fails, the failure is a CCF with probability β . Hence, if the component fails with probability Q , the probability of independent failure is $Q^1 = (1 - \beta) \cdot Q$, and the probability of a CCF of all m components is $Q^m = \beta \cdot Q$.

The α -factor model considers the possibility that a subset of m components can fail due to a common cause, i.e. CCFs between different component combinations are possible. The formulas for the α -factor model are

$$Q^k = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_{tot}} Q, \quad (2.4)$$

$$\alpha_{tot} = \sum_{k=1}^m k \alpha_k, \quad (2.5)$$

where the factors $\alpha_1, \dots, \alpha_m$ are determined by the analyst.

If an α -factor group includes four components, the failure probability of

a component is 0.001, $\alpha_1 = 0.935$, $\alpha_2 = 0.05$, $\alpha_3 = 0.01$ and $\alpha_4 = 0.005$, it follows that

$$\alpha_{tot} = 0.935 + 2 \cdot 0.05 + 3 \cdot 0.01 + 4 \cdot 0.005 = 1.085,$$

$$Q^1 = \frac{1}{\binom{3}{0}} \frac{0.935}{1.085} \cdot 0.001 \approx 8.62 \cdot 10^{-4},$$

$$Q^2 = \frac{2}{\binom{3}{1}} \frac{0.05}{1.085} \cdot 0.001 \approx 3.07 \cdot 10^{-5},$$

$$Q^3 = \frac{3}{\binom{3}{2}} \frac{0.01}{1.085} \cdot 0.001 \approx 9.22 \cdot 10^{-6}$$

and

$$Q^4 = \frac{4}{\binom{3}{3}} \frac{0.005}{1.085} \cdot 0.001 \approx 1.84 \cdot 10^{-5}.$$

3. Results

3.1 Prime implicants

Paper I presents a new definition of a prime implicant that is applicable in time-dependent dynamic reliability analysis. The basis for the definition is a reliability model that consists of a top function and a set of additional constraints. The analysis of non-repairable components in the DFM was the case that revealed the need for the new definition, because the results contained prime implicants that implied some other prime implicants. For example, according to the traditional definition [35],

$$\{V_1(-4), VF_0(-3), WL_0(-4), WLM_{-1}(-4), MF_1(-1)\}$$

and

$$\{V_1(-4), VF_0(-3), WL_0(-4), WLM_{-1}(-4), MF_1(-2)\}$$

are prime implicants of the example model presented in Paper I. However, since MF represents the failure of a non-repairable component, implicant

$$\{V_1(-4), VF_0(-3), WL_0(-4), WLM_{-1}(-4), MF_1(-2)\}$$

implies

$$\{V_1(-4), VF_0(-3), WL_0(-4), WLM_{-1}(-4), MF_1(-1)\}.$$

The new definition was developed with the idea that an implicant that implies some other length-minimal implicant is not a prime implicant, because it is not a minimal condition for causing the top event.

The new definition provides solid mathematical foundation for DFM. It takes time-related minimality into account. For example, assume that a top event occurs if a non-repairable component fails during a particular time frame. The component can fail at different time points to cause the

top event, but it does not need to fail until a specific time point. Therefore, the condition that the component is failed at the latest possible time point is minimal, and the condition that the component fails earlier is non-minimal. The new definition also supports the calculation of the top event probability better than the traditional definition [35], and conveniently a smaller number of prime implicants can represent the root causes of the top event. These claims are demonstrated by simple examples in Paper I. The definition and interpretation of prime implicants affect the modelling of the component's time-dependent behaviour and dependent events, and the computation of failure probabilities, the top event probability and risk importance measures. Hence, the new definition is an important basis for further research.

3.2 Risk importance measures

Paper II develops new dynamic risk importance measures as generalisations of traditional risk importance measures: the dynamic Fussell-Vesely (DFV) and the dynamic risk increase factor (DRIF). These risk importance measures map information from prime implicants to values that represent the significances of different events and conditions. The dynamic risk importance measures are calculated for the states of nodes. It is logical to separate different states of a node in the analysis because they represent completely different conditions. Furthermore, the information about time steps is taken into account in the computation of the dynamic risk importance measures.

Fussell-Vesely measures the portion of the top event probability coming from the minimal cut sets that include the analysed basic event. Correspondingly, the DFV measures the portion of the top event probability coming from the prime implicants that include a particular node in a particular state before or at a particular time step. If the analysed system is coherent with regard to the analysed state of the node, the DFV can be interpreted as the relative decrease in the top event probability caused by the condition that the node is not in the considered state until a particular time step. The DFV is presented in its basic form in Definition 3. In addition to the basic form, the DFV is formulated for failure states of components that are modelled with two nodes: one that determines whether the component has failed or not, and one that represents the functional state of a component. Another form of the DFV is also developed to mea-

sure the incoherency of a component.

Definition 3 *The dynamic Fussell-Vesely measure of state s of node i at time step $-t$ is*

$$I^{DFV}(i_s(-t)) := \frac{Q_{TOP}^{i_s(-t)}}{Q_{TOP}}, \quad (3.1)$$

where Q_{TOP} is the top event probability and $Q_{TOP}^{i_s(-t)}$ is the probability that a prime implicant including node i in state s before or at time step $-t$ causes the top event.

The DRIF measures how much the top event probability would relatively increase if the analysed node was in the considered state at all time steps of the DFM analysis time frame. The DRIF is presented in Definition 4. It can also be calculated for failure states of components.

Definition 4 *The dynamic risk increase factor of state s of node i is*

$$I^{DI}(i_s) := \frac{Q_{TOP}(i_s(-t) = 1, \forall t \in \{0, 1, \dots, l-1, l\})}{Q_{TOP}}, \quad (3.2)$$

where $Q_{TOP}(i_s(-t) = 1, \forall t \in \{0, 1, \dots, l-1, l\})$ is the probability that the top event occurs, assuming that node i is in state s at every time step starting from $-l$ which is the earliest possible time step for node i to be in state s considering the initial conditions. The last time step of the analysis is assumed to be 0 in this formula.

Paper II also presents how failure states of components can be tracked, because the information on failure states (as defined in Paper II) does not directly appear in prime implicants. The failure states provide useful information even without risk importance measures, because the failure state is an important factor when analysing the causes of a top event. Moreover, more information is obtained if it is known that a component fails to a particular state than if it is only known that the component fails somehow.

3.3 Common cause failures

One special characteristic of DFM is that components can fail at different time points but still contribute to the same top event. Even though a CCF event is often interpreted as a simultaneous failure of similar components, NUREG/CR-6268 [25] defines that components need to fail only during the PRA mission time, which is typically 24 hours. This definition is used

both in data collection and PRA analysis. In data collection, if multiple failures occur within 24 hours, they are interpreted as a CCF. In addition, 50% of such events where the time between failures is 24-48 hours are counted as CCFs, i.e. a timing factor of 0.5 is used [25]. For traditional fault tree analysis, it is irrelevant whether the components fail simultaneously or not during the mission time, but in DFM non-simultaneous CCFs can be considered, because DFM divides the mission time into smaller time intervals. Paper III takes the possibility of such CCFs into account.

Two parametric CCF models, β - and α -factor models, are used in CCF probability computation. The CCF probability is calculated on the basis of the average of the probabilities of individual component failures in (3.3) for the β -factor model.

$$P_{\pi}(C_1(-t_1, -t_2, \dots, -t_m)) = \beta \cdot \frac{1}{m} \sum_{i=1}^m P_{\pi}(F_1^i(-t_i)), \quad (3.3)$$

where $-t_1, -t_2, \dots, -t_m$ are the failure times of components, π is the prime implicant that contains the CCF, and $P_{\pi}(F_1^i(-t_i))$ is the probability that the i :th component is failed at time step $-t_i$ in the prime implicant π . The probabilities can depend on other literals included in the prime implicant as presented in Paper III.

The method is simple and, in most cases, conservative, because simultaneous CCFs are more likely. If non-simultaneous CCFs are ignored in the analysis, some CCF probabilities are underestimated assuming that non-simultaneous CCFs are possible, and some prime implicants are also left out. It is advantageous that the same β and α parameters can be used as in the traditional case so that ordinary CCF data [65] can be used in DFM analysis.

Paper III also presents how CCFs can be incorporated into DFM results. CCFs do not need to be accounted for when the prime implicants are first solved. All the prime implicants with CCFs can be created on the basis of the original prime implicants that contain individual failures. This approach was chosen so that the graph model would not become excessively complex, which would increase the computational demands significantly and make the analysis time-consuming.

4. Discussion and conclusions

This Dissertation has extended dynamic reliability analysis theory in the following ways. First, the mathematical foundation of DFM was strengthened by developing an improved definition of a prime implicant in Paper I (Section 3.1 in the Dissertation). Second, the DFM analysis was improved by defining and analysing new risk importance measures in Paper II (Section 3.2 in the Dissertation). Third, CCF modelling was developed in the DFM context in Paper III (Section 3.3 in the Dissertation).

Unlike any other importance measure, the dynamic risk importance measures utilise all the information available in prime implicants of DFM. They measure primarily the importances of different states of components and variables. The computation of the dynamic risk importance measures for failure states of components provides significant additional information compared to other importance values. On the basis of DFV results, it is possible to judge at which time points particular failures and conditions contribute to the top event.

The dynamic risk importance measures were developed for the needs of DFM, but their applicability to other dynamic risk analysis methodologies could also be studied. The DRIF could quite easily be applied in some different methodologies because it only measures the change in the top event probability caused by the analysed event, but the DFV relies heavily on prime implicants. In methods that do not solve prime implicants, some alternative way of calculating the DFV should be found or some other importance measure could be used instead. For example, dynamic simulation based methods are often applied in level 2 PRA [15, 66]. Timings of events are important in severe reactor accidents. Hence, the application of the dynamic risk importance measures could be studied in that area. Actually, some dynamic importance measures have already been developed for level 2 PRA [67].

Usually, the essential task in DFM analysis is to identify the prime implicants of the top event. Prime implicant identification should be studied considering the definition presented in Paper I. Previously, e.g. non-repairable components have been handled using case-specific treatments in the identification process. A goal for future research could be to develop a prime implicant identification algorithm that would take additional constraints of any type into account. The decomposition theorem from [68] could possibly be generalised to take the multi-state logic and additional constraints into account.

Computational efficiency is a key issue in the development of DFM for practical reliability analysis. There is a need both to identify prime implicants and to perform quantification in a reasonable time. If a new prime implicant identification algorithm is developed as discussed in the previous paragraph, the implementation of the algorithm should also be efficient enough to be used in practice. Correspondingly, the computation of the top event probability and the risk importance measures should be reasonably fast, but also accurate enough. Approximations can be calculated rapidly, but the computation of accurate values can be demanding if the analysed model is not small. Approximate values are usually sufficient in most reliability analyses as long as they are accurate enough. The quantification of DFM could be studied in greater depth so that an optimal balance between accuracy and computation times could be achieved in the computation of the top event probability and the risk importance measures.

Despite its importance, quantification of individual literals and prime implicants has not been much addressed in the literature. Paper III presented how to calculate the failure probabilities of non-repairable components and CCF probabilities, but different component reliability models, the determination of the probabilities of the initial states of variables, and quantification of cascading failures and other dependent events could also be studied. One factor that adds complexity is that the same literal can have different probabilities in different prime implicants if its probability depends on other literals. Non-repairable components are a simple example of this, as presented in Paper III. Probabilistic analysis depends on the modelling decisions, and the modelling of components and variables should therefore also be considered from the quantification point of view. An interesting and challenging topic for future research is to define good practices in the DFM modelling and quantification.

The CCF probability computation could be made more accurate by developing time-dependent CCF models. The assumption of simultaneous failures is not realistic in many cases. Timing related CCF parameters could be estimated, for example the probability that the difference between failure times lies within a specific interval. Data about failure times is actually already collected [25], but is only utilised in the classification of events. Data analyses would be needed to study to which failure modes time-dependent models should be applied.

DFM has been considered to be too complex to be applied to large systems, and most applications found in the literature are rather small. However, more efficient DFM tools and prime implicant solving technologies, such as BDDs, are being developed, and computers are becoming more and more powerful. Recent DFM models have been larger [28, 44], and this development will probably continue in the future. With larger models, the ability to analyse results efficiently becomes even more important. Therefore, suitable risk importance measures are needed. CCFs are also more important when larger systems with redundancies are analysed.

Bibliography

- [1] Häring, I. Risk analysis and management: Engineering resilience. Singapore: Springer, 2015. 397 p. ISBN: 978-981-10-0015-7.
- [2] Bedford, T. & Cooke, R. Probabilistic risk analysis: Foundation and methods. Cambridge: Cambridge University Press, 2001. 393 p. ISBN: 0521773202, 9780521773201.
- [3] Emblemsvåg, J. & Kjølstad, L.E. Qualitative risk analysis: Some problems and remedies. *Management Decision*, Vol. 44 (2006) 3, pp. 395-408.
- [4] Vesely, W.E., Goldberg, F.F., Roberts, N.H. & Haasl, D.F. Fault tree handbook. Washington D.C.: U.S. Nuclear Regulatory Commission, 1981. 202 p. NUREG-0492.
- [5] Clements, P.L. Fault tree analysis, 4th edition. Massachusetts: Sverdrup Technology, Inc., 1993. 96 p.
- [6] Labeau, P.E., Smidts, C. & Swaminathan, S. Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering and System Safety*, Vol. 68 (2000) 3, pp. 219-254.
- [7] Garrett, C.J., Guarro, S.B. & Apostolakis, G.E. The dynamic flowgraph methodology for assessing the dependability of embedded software systems. *Systems, Man and Cybernetics*, Vol. 25 (1995) 5, pp. 824-840.
- [8] Aldemir, T., Guarro, S., Mandelli, D., Kirschenbaum, J., Mangan, L.A., Bucci, P., Yau, M., Ekici, E., Miller, D.W., Sun, X. & Arndt, S.A. Probabilistic risk assessment modeling of digital instrumentation and control systems using two dynamic methodologies. *Reliability Engineering and System Safety*, Vol. 95 (2010), pp. 1011-1039.

- [9] Al-Dabbagh, A.W. & Lu, L. Reliability modeling of networked control systems using dynamic flowgraph methodology. *Reliability Engineering and System Safety*, Vol. 95 (2010), pp. 1202-1209.
- [10] Bucci, P., Kirschenbaum, J., Mangan, L.A., Aldemir, T., Smith, C. & Wood, T. Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. *Reliability Engineering and System Safety*, Vol. 93 (2008), pp. 1616-1627.
- [11] Gomes, I.B., Saldanha, P.L.C. & Frutuoso e Melo, P.F.F. A cell-to-cell Markovian model for the reliability of a digital control system of a steam generator. Proceedings of the 2013 International Nuclear Atlantic Conference - INAC 2013, Recife, Brazil, 24-29 November 2013. ISBN: 978-85-99141-05-2.
- [12] Yang, J. & Aldemir, T. An algorithm for the computationally efficient deductive implementation of the Markov/cell-to-cell-mapping technique for risk significant scenario identification. *Reliability Engineering and System Safety*, Vol. 145 (2016), pp. 1-8.
- [13] Acosta, C.G. & Siu, N.O. Dynamic event tree analysis method (DETAM) for accident sequence analysis. Cambridge (USA): Massachusetts Institute of Technology Nuclear Engineering Department, 1991. 138+23 p. MITNE-295.
- [14] Karanki, D.R., Kim, T.-W. & Dang, V.N. A dynamic event tree informed approach to probabilistic accident sequence modeling: Dynamics and variabilities in medium LOCA. *Reliability Engineering and System Safety*, Vol. 142 (2015), pp. 78-91.
- [15] Tyrväinen, T., Silvonen, T. & Mätäsniemi, T. Computing source terms with dynamic containment event trees. Proceedings of the 13th International Probabilistic Safety Assessment and Management Conference; 2016 Oct 2-7; Seoul, Korea.
- [16] Sadou, N. & Demmou, H. Reliability analysis of discrete event dynamic systems with Petri nets. *Reliability Engineering and System Safety*, Vol. 94 (2009) 11, pp. 1848-1861.
- [17] Swaminathan, S. & Smidts, C. The mathematical formulation for the event sequence diagram framework. *Reliability Engineering and System Safety*, Vol. 65 (1999) 2, pp. 103-118.

- [18] Zhao, J., Liu, T. Zhao, Y., Liu, D., Yang, X., Lin, J., Lin, Z. & Lei, Y. Reliability evaluation of NPP's power supply system based on improved GO-FLOW method. *Science and Technology of Nuclear Installations*, Vol. 2016 (2016), 10 p.
- [19] Cepin, M. & Mavko, B. A dynamic fault tree. *Reliability Engineering and System Safety*, Vol. 75 (2002) 1, pp. 83-91.
- [20] Huang, H.W., Shih, C., Yih, S. & Chen, M.H. Integrated software safety analysis method for digital I&C systems. *Annals of Nuclear Energy*, Vol. 35 (2008) 8, pp. 1471-1483.
- [21] Wang, W., Di Maio, F. & Zio, E. Component- and system-level degradation modeling of digital instrumentation and control systems based on a multi-state physics modeling approach. *Annals of Nuclear Energy*, Vol. 95 (2016), pp. 135-147.
- [22] Zio, E. & Di Maio, F. Processing dynamic scenarios from a reliability analysis of a nuclear power plant digital instrumentation and control system. *Annals of Nuclear Energy*, Vol. 36 (2009) 9, pp. 1386-1399.
- [23] Van Der Borst, M. & Schoonakker, H. An overview of PSA importance measures. *Reliability Engineering and System Safety*, Vol. 72 (2001) 3, pp. 241-245.
- [24] Mosleh, A., Fleming, K.N., Parry, G.W., Paula, H.M., Worledge, D.H. & Rasmuson, D.M. Procedures for treating common cause failures in safety and reliability studies: Procedural framework and examples. Washington D.C.: U.S. Nuclear Regulatory Commission, Division of Reactor and Plant Systems, 1988. 202 p. NUREG/CR-4780 EPRI NP-5613 Vol. 1.
- [25] Wierman, T.E., Rasmuson, D.M. & Mosleh, A. Common-cause failure database and analysis system: Event data collection, classification, and coding. Washington D.C.: U.S. Nuclear Regulatory Commission, Division of Risk Assessment and Special Projects, 2007. NUREG/CR-6268, Rev. 1 INL/EXT-07-12969.
- [26] Karanta, I. Importance measures for the dynamic flowgraph methodology. Espoo (Finland): VTT Technical Research Centre of Finland, Systems Research, 2011. VTT-R-00525-11.
- [27] Houtermans, M.J.M. A method for dynamic process hazard analysis and integrated process safety management [doctoral thesis].

- Eindhoven (Netherlands): Technische Universiteit Eindhoven, 2001.
<http://alexandria.tue.nl/extra2/200111699.pdf>.
- [28] Yau, M., Dixon, S. & Guarro, S. Application of the dynamic flowgraph methodology to the space propulsion system benchmark problem. Proceedings of the 12th International Probabilistic Safety Assessment and Management Conference; 2014 Jun 22-27; Sheraton Waikiki, Honolulu, Hawaii, USA.
- [29] Yau, M., Apostolakis, G. & Guarro, S. The use of prime implicants in dependability analysis of software controlled systems. *Reliability Engineering and Systems Safety*, Vol. 62 (1998), pp. 23-32.
- [30] Tyrväinen, T. Risk importance measures and common cause failures in dynamic flowgraph methodology [master's thesis]. Espoo (Finland): Aalto University, School of Science, 2011.
- [31] Halmos, P. & Givant, S. Introduction to Boolean algebras. New York: Springer, Undergraduate Texts in Mathematics, 2009. 446 p. ISBN: 978-0-387-40293-2.
- [32] Jung, W.S. A method to improve cutset probability calculation in probabilistic safety assessment of nuclear power plants. *Reliability Engineering and System Safety*, Vol. 134 (2015), pp. 134-142.
- [33] Bryant, R.E. Graph-based algorithms for Boolean function manipulation. *Computers*, Vol. C-35 (1986) 8, pp. 677-691.
- [34] Bryant, R.E. Symbolic Boolean manipulation with ordered binary-decision diagrams. *ACM Computing Surveys*, Vol. 24 (1992) 3, pp. 293-318.
- [35] Rauzy, A. Mathematical foundation of minimal cutsets. *IEEE transactions on Reliability*, Vol. 50 (2001) 4, pp. 389-396.
- [36] Contini, S., Cojazzi, G.G.M. & Renda, G. On the use of non-coherent fault trees in safety and security studies. *Reliability Engineering and System Safety*, Vol. 93 (2008) 12, pp. 1886-1895.
- [37] Rauzy, A. Binary decision diagrams for reliability studies. In: Misra, K.B. *Handbook of performance engineering*. London: Springer London, 2008. pp. 381-396.

- [38] Ching, W.-K., Huang, X., Ng, M.K. & Siu, T.-K. Markov chains: Models, algorithms and applications. New York: Springer US, 2013. 258 p. ISBN: 978-1-4614-6312-2.
- [39] Hejase, M., Kurt, A., Aldemir, T., Ozguner, U., Guarro, S.B., Yau, M.K. & Knudson, M.D. A quantitative and risk based framework for UAS control system assurance. AIAA Information Systems-AIAA Infotech @ Aerospace; 2017 Jan 9-13; Grapevine, Texas, USA. AIAA 2017-0882.
- [40] Al-Dabbagh, A.W. & Lu, L. Dynamic flowgraph modeling of process and control systems of a nuclear-based hydrogen production plant. International Journal of Hydrogen Energy, Vol. 35 (2010), pp. 9569-9580.
- [41] Björkman, K. Solving dynamic flowgraph methodology models using binary decision diagrams. Reliability Engineering and System Safety, Vol. 111 (2013), pp. 206-216.
- [42] Guarro, S., Yau, M. & Dixon, S. Applications of the dynamic flowgraph methodology to dynamic modeling and analysis. Proceedings of the 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference; 2012 Jun 25-29; Helsinki, Finland.
- [43] Guarro, S., Yau, M. & Dixon, S. Advanced risk modeling and risk-informed testing of digital instrumentation and control systems. Proceedings of the Probabilistic Safety Assessment Conference (PSA-11); 2011 Mar 13-17; Wilmington, NC.
- [44] McNelles P., Zeng, Z.C., Renganathan, G., Lamarre, G., Akl, Y. & Lu, L. A comparison of fault trees and the dynamic flowgraph methodology for the analysis of FPGA-based safety systems part 1: Reactor trip logic loop reliability analysis. Reliability Engineering and System Safety, Vol. 153 (2016), pp. 135-150.
- [45] Houtermans, M., Apostolakis, G., Brombacher, A. & Karydas, D. The dynamic flowgraph methodology as a safety analysis tool: Programmable electronic system design and verification. Safety Science, Vol. 40 (2002), pp. 813-833.
- [46] ASCA Inc. Dymonda. 2010. www.ascainc.com/dymonda/dymonda.html [Referred 17.8.2017].

- [47] Quine, W.V. A way to simplify truth functions. *American Mathematical Monthly*, Vol. 62 (1955), pp. 627-631.
- [48] Cepek, O., Kucera, P. & Kurik, S. Boolean functions with long prime implicants. *Information Processing Letters*, Vol. 113 (2013), 698-703.
- [49] ASCA Inc. DFM specifications. 2010. www.ascainc.com/dfm/dfm_specs.html [Referred 17.8.2017].
- [50] Karanta, I. Implementing dynamic flowgraph methodology models with logic programs. *Journal of Risk and Reliability*, Vol. 227 (2013), pp. 302-314.
- [51] Pinto, J.M.O., Frutuoso e Melo, P.F. & Saldanha, P.L.C. A dynamic failure evaluation of a simplified digital control system of a nuclear power plant pressurizer. *Proceedings of the 13th Brazilian Congress of Thermal Sciences and Engineering; 2010 Dec 5-10; Uberlandia, MG, Brazil. Rio de Janeiro: ABCM; 2010.*
- [52] Yau, M., Guarro, S. & Apostolakis, G. Demonstration of the dynamic flowgraph methodology using the Titan II space launch vehicle digital flight control system. *Reliability Engineering and System Safety*, Vol. 49 (1995), pp. 335-353.
- [53] Shi, J., Wang, G. & Tong, T. The integrated health monitoring design using the dynamic flowgraph methodology for thermal control systems of payloads. *Chemical Engineering Transactions*, Vol. 33 (2013), pp. 211-216.
- [54] Ahmed, F. Probabilistic risk assessment using dynamic flowgraph methodology for copper chloride CANDU-SCWR hydrogen production. *Procedia Computer Science*, Vol. 19 (2013), pp. 777-785.
- [55] Milici, A., Mulvihill, R. & Guarro, S. Extending the dynamic flowgraph methodology (DFM) to model human performance and team effects. Washington D.C.: U.S. Nuclear Regulatory Commission, Division of System Analysis and Regulatory Effectiveness, 2001. NUREG/CR-6710.
- [56] McNelles, P. & Lu, L. Field programmable gate array reliability analysis using the dynamic flowgraph methodology. *Nuclear Engineering and Technology*, Vol. 48 (2016) 5, pp. 1192-1205.

- [57] Aldemir, T., Miller, D.W., Stovsky, M.P., Kirschenbaum, J., Bucci, P., Fentiman, A.W. & Mangan L.T. Current state of reliability modeling methodologies for digital systems and their acceptance criteria for nuclear power plant assessments. Washington D.C.: U.S. Nuclear Regulatory Commission, Division of Fuel, Engineering, and Radiological Research, 2006. NUREG/CR-6901.
- [58] Zio, E. Risk importance measures. In: Pham, H. Safety and risk modeling and its applications. London: Springer-Verlag, 2011. pp. 151-195.
- [59] Meng, F.C. Relationships of Fussell-Vesely and Birnbaum importance to structural importance in coherent systems. *Reliability Engineering and System Safety*, Vol. 67 (2000) 1, pp. 55-60.
- [60] Laitonen, J. & Niemelä, I. Analyzing system changes with importance measure pairs: Risk increase factor and Fussell-Vesely compared to Birnbaum and failure probability. Proceedings of the 12th International Probabilistic Safety Assessment and Management Conference; 2014 Jun 22-27; Sheraton Waikiki, Honolulu, Hawaii, USA.
- [61] Bäckström, O., Krcal, P. & Wang, W. Two interpretations of the risk increase factor definition. In: Walls, S., Revie, M. & Bedford, T. Risk, reliability and safety: Innovating theory and practice. London: Taylor & Francis Group, 2017. pp. 2816-2822. ISBN: 978-1-138-02997-2.
- [62] Martorell, S., Marton, I., Martorell, P., Carlos, S. & Sanchez, A.I. RAM based metrics for safety assessment of safety systems with application to ageing management. In: Podofilini, L., Sudret, B., Stojadinovic, B., Zio, E. & Kröger, W. Safety and reliability of complex engineered systems. London: Taylor & Francis Group, 2015. pp. 1645-1650. ISBN: 978-1-138-02879-1.
- [63] Høyland, A. & Rausand, M. Dependent failures. In: System reliability theory: Models and statistical methods. New York: Wiley Series in Probability and mathematical statistics: Applied probability and statistics section, 1994. pp. 325-354. ISBN: 0-471-59397-4.
- [64] Chebila, M. & Innal, F. Unification of common cause failures' parametric models using a generic Markovian model. *Journal of Failure Analysis and Prevention*, Vol. 14 (2014), pp. 426-434.

- [65] Mosleh, A., Rasmuson, D.M. & Marshall, F.M. Guidelines on modelling common-cause failures in probabilistic risk assessment. Washington D.C.: U.S. Nuclear Regulatory Commission, Safety Programs Division, 1998. NUREG/CR-5485, INEEL/EXT-97-01327.

- [66] Guigueno, Y., Raimond, E., Dufлот, N., Tanchoux, V., Rahni, N., Laurent, B. & Kioseyan, G. Severe accident risk assessment for NPPs - Software tools and methodologies for level 2 PSA development available at IRSN. Proceedings of the 13th International Probabilistic Safety Assessment and Management Conference; 2016 Oct 2-7; Seoul, Korea.

- [67] Jankovsky, Z.K., Denman, M.R. & Aldemir, T. Dynamic importance measures in the ADAPT framework. Transactions of the American Nuclear Society, Vol. 115 (2016), pp. 799-802.

- [68] Rauzy A & Dutuit Y. Exact and truncated computation of prime implicants of coherent and non-coherent fault trees within Aralia. Reliability Engineering and System Safety, Vol. 58 (1997), pp. 127-144.



ISBN 978-952-60-7571-6 (printed)
ISBN 978-952-60-7570-9 (pdf)
ISSN-L 1799-4934
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)

978-951-38-8565-6 (printed)
978-951-38-8564-9 (pdf)
2242-119X
2242-119X (printed)
2242-1203 (pdf)

Aalto University
School of Science
Department of Mathematics and Systems Analysis
www.aalto.fi

**BUSINESS +
ECONOMY**

**ART +
DESIGN +
ARCHITECTURE**

**SCIENCE +
TECHNOLOGY**

CROSSOVER

**DOCTORAL
DISSERTATIONS**