Czech Technical University in Prague
Faculty of Electrical Engineering

Doctoral Thesis

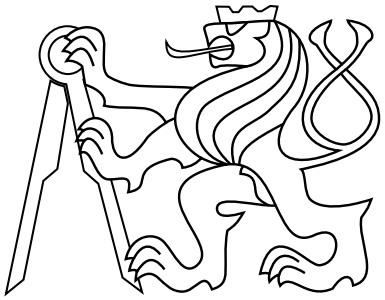
August 2015

Ondřej Nývlt

Doctoral thesis

Risk Management Methods for Industrial Systems

Ondřej Nývlt



Czech Technical University in Prague,
Faculty of Electrical Engineering,
Department of Control Engineering

Prague, August 2015

Supervisor:	doc. Ing. Jan Bílek, CSc.
Supervisor specialist:	doc. Ing. Lukáš Ferkl, Ph.D.
Ph.D. programme:	Electrical engineering and information technology
Study branch:	Control engineering and robotics

Acknowledgement

This Ph.D. thesis would not have been finished without help and support of many great persons, some of which are mentioned lower. So on this place, I would like to say, at least, "thank you very much" to all of them.

First I would like to honour and acknowledge my Ph.D. supervisor Jan Bílek and supervisor specialist Lukáš Ferkl for their support and guidance through my Ph.D. studies.

A big thank belongs to my friends and colleagues from Feramat Cybernetics Ltd. for their help with completing of the thesis, fruitful discussion about the research topics and a trust in my work.

I would like to also thank professor Marvin Rausand and Stein Haugen from NTNU Trondheim for their ideas, supervision, assistance and a chance to spend one very inspiring and unforgettable semester at their department (NTNU IPK).

The biggest thank and honour belongs to my family, because without their continuous support and love, this thesis would not be possible to finish.

This Ph.D. thesis was supported by the internal grants of Czech Technical University in Prague No. CTU0915013, SGS13/209/OHK3/3T/13, SGS10/283/OHK3/3T/13, by the European Union OP RDI projects No. CZ.1.05/2.1.00/03.0091 – *University Centre for Energy Efficient Buildings* and CZ.1.05/3.1.00/13.0283 – *Intelligent Buildings*, by the Czech Ministry of Education, Youth and Sports under the EuSophos project No. 2C06010 and by Norwegian grant by means of financial instruments of EEA and Norway No. B/CZ0046/2/0015.

Prague, August 2015 *Ondřej Nývlt*

Declaration

I declare that I worked out the presented thesis independently and I quoted all used sources of information in accord with Methodical instructions about ethical principles for writing academic thesis.

Abstract

Risk management (RM) is today a commonly used term in many different disciplines (e.g. economy, industry, human resources, IT). Its goal is firstly to identify risks (e.g. of a machine operation, human behaviour or of a whole project) which can cause harm to properties, persons or environment. Secondly the RM should evaluate probabilities and severities of these unwanted events and propose measures for their elimination or a reduction of their impact. This whole process should be periodically repeated to assess influences of the measures of a risk control on detected risks. If the risks are mitigated insufficiently, then there should be additional measures proposed.

This general interdisciplinary approach could be split into three parts or phases. This Ph.D. thesis is focused on the first phase: the risk analysis (RA). There are few commonly used traditional RA methods in the industry area e.g. Fault Tree Analysis (FTA) or Event Tree Analysis (ETA). These methods were developed many years ago, so their original definitions do not meet today's requirements for analysis of large and complex systems or accidental scenarios with different types of dependencies, dynamic changes and other pitfalls. Different industrial areas have developed their own narrowly focused methods during last years, even though there could be, for selected tasks, used some of the mentioned common, but slightly modified methods.

Based on the stated facts, this Ph.D. thesis is focused on an analysis of traditional RA methods, on a detection of their specific problems and mainly on a proposal of new alternative universal methods which are able to solve the mentioned problems. These new methods should integrate more than two phases of the RA together and they have to be practically usable. As a framework for a design of new methods, Petri nets (PN) were chosen. They are often used for a modelling and analysis of discrete event systems (DES), but they are still not common in the area of the RA.

The first part of the thesis shows how advantageous it is to use general (in this case traditional) methods instead of the narrowly focused ones. As an example, a risk analysis of the Strahov city road tunnel is chosen. The goal of the analysis is to select which option of a reconstruction of the tunnel is the best from the point of view of the risk/cost ratio. A slightly modified general analysis called Probabilistic Risk Assessment, which is known from the nuclear and aerospace industry, provides superb results and supports the idea of using non-specialized methods.

The second part of the thesis introduces a concept of the PN as a tool for a solution of selected problems of traditional RA methods. The non-marked PN are used for a theoretical solution of dependencies of pivotal events in the ETA.

The final part of the thesis presents a proposal of a new alternative complex RA method based on stochastic PN, which is able to model the whole accidental scenario without pitfalls of the traditional FTA and ETA. It extends a classical approach with an ability to easily model dependencies and dynamic changes of an event sequence in the scenario. This method is fully usable and is supported by existing commercial software tools.

This doctoral thesis demonstrates that the PN are still a little bit overlooked but powerful framework for risk analysis and management and offer new possibilities for modelling, simulation and analysis.

Keywords

Risk management; Risk analysis; Petri nets; Road tunnels; Fault trees; Event trees

Abstrakt

Rizikový management je dnes již běžným pojmem v mnoha různých oborech (například ekonomie, průmysl, řízení lidských zdrojů nebo IT). Jeho cílem je na prvním místě identifikovat rizika (např. provozu zařízení, lidského chování nebo celého projektu), která mohou mít za následek škody na majetku, osobách nebo životním prostředí. Dále je jeho úkolem vyhodnotit závažnost a pravděpodobnost výskytu nežádoucích situací a navrhnout opatření k jejich úplné eliminaci nebo alespoň snížení jejich vlivu (tzv. řízení rizik). Celý proces je nutné periodicky opakovat, aby se vyhodnotilo, zda nástroje řízení rizika splnily svůj účel, nebo je nutné aplikovat další opatření.

Jde o obecný mezioborový přístup, který můžeme dělit na tři základní části — tato práce se zabývá pouze první z nich: rizikovými analýzami a to v oblasti průmyslu, kde se setkáváme s několika tradičními hojně rozšířenými metodami. Řeč je především o analýze stromů chyb (FTA) a stromů událostí (ETA). Vzhledem k tomu, že tyto metody vznikly před několika desítkami let, tak v klasickém pojetí již často nereflektují potřeby dnešních rozsáhlých a komplikovaných systémů/scénářů obsahujících různé závislosti a další záludnosti. U rozsáhlých a dynamicky se měnících systémů mohou dokonce selhat či poskytovat nepřehledné výsledky. Různé oblasti průmyslu navíc v průběhu let pro svoje potřeby vyvinuly vlastní úzce zaměřené metody a to i v případě, že lze pro ty samé účely využít některých mírně upravených obecných, všeobecně uznávaných a vyzkoušených metod.

Z výše zmíněných důvodů se tato dizertační práce zabývá jednak analýzou tradičních metod rizikových analýz, dále pak nalezením jejich problémů a především návrhem alternativních univerzálních (tj. na konkrétním oboru nezávislých) metod bez zmíněných slabých míst. Výsledné metody by v sobě měly sjednocovat více než jednu fázi rizikové analýzy a musí být prakticky použitelné. Jako platforma vhodná pro návrh nových přístupů jsou vybrány Petriho sítě, běžně využívané pro modelování a analýzu systémů diskrétních událostí (DES), ale v praxi méně aplikované v oblasti rizikových analýz.

Práce nejdříve uvádí příklad, jaké výhody přináší využití (stále ještě tradičních) obecných metod místo návrhu nových úzce zaměřených technik. Jako příklad si bere analýzu silničního městského tunelu Strahov v Praze, kdy bylo úkolem vyhodnotit varianty rekonstrukce z pohledu poměru riziko/cena. Mírně upravená univerzální metoda "Probabilistic Risk Assessment", známá z jaderného a leteckého průmyslu, poskytla velmi dobré závěry a ukázala tak výhodu zmíněného přístupu.

V další části práce je představen koncept Petriho sítí jako silného nástroje pro řešení problémů klasických metod rizikových analýz. V tomto případě jsou neznačené Petriho sítě použity pro teoretické řešení specifického problému závislostí v ETA.

Poslední část práce ukazuje návrh komplexní metody rizikové analýzy (tj. od příčin nežádoucích situací až po jejich následky) na bázi stochastických Petriho sítí (s dalšími rozšířeními), která dokáže řešit vybrané nedokonalosti modelování a analýzy scénářů tradičním přístupem (tj. ETA/FTA) a rozšiřuje klasický přístup o možnost dynamického řazení událostí v sekvenci scénáře. Jde o prakticky použitelnou metodiku (jak ukazuje případová studie) podepřenou již existujícím komerčním softwarem.

Tato dizertační práce demonstruje, že Petriho sítě jsou prozatím mírně opomíjenou ale silnou a oborově nezávislou platformou pro rizikové analýzy i rizikový management, která nabízí nové možnosti modelování, simulací i analýz.

Klíčová slova

Management rizik; Rizikové analýzy; Petriho sítě; Silniční tunely; Stromy chyb; Stromy událostí

Contents

Abbreviations

Here is a list of abbreviations that will further be used in the thesis.

BDD	Binary Decision Diagrams
BN	Bayesian Network
CCF	Common Cause Failure
CPN	Coloured Petri Net
CSPN	Coloured Stochastic Petri Net
DES	Discrete Event System
DFT	Dynamic Fault Tree
DSPN	Deterministic and Stochastic Petri Net
ET	Event Tree
ETA	Event Tree Analysis
FT	Fault Tree
FTA	Fault Tree Analysis
GSPN	Generalised Stochastic Petri Net
IEC	International Electrotechnical Commission
IT	Information Technology
MCS	Minimal Cut-set
OOBN	Object-Oriented Bayesian Network
PE	Pivotal Event
PLC	Programmable Logic Controller
PN	Petri Net
PRA	Probabilistic risk assessment
RA	Risk Analysis
RM	Risk Management
SIL	Safety Integrity Levels
SPN	Stochastic Petri Net
SW	Software

1 Introduction

Risk Management (RM) is an important (and in many countries also mandatory) part of any industrial project, because its task is to detect and control risks to achieves project's goals. One of many definitions of the RM is for example: *"A continuous management process with the objective to identify analyse and asses potential hazards in a system or related to an activity, and to identify and introduce risk control measures to eliminate or reduce potential harms to people, the environment or other assets."* [1]. The RM can be divided into three interconnected parts, which are depicted in Figure 1, which is adapted from [1]: **risk analysis (RA), risk evaluation and risk control**. Every of these three parts should be repetitively performed to have all risks under control.

1.1 Motivation

This Ph.D. thesis is focused mainly on the topic of the RA and its methods, because the author sees there potential improvements in a usage of know-how from different disciplines and science sectors. Another reason is an increasing complexity and magnitude of systems/problems, which should be modelled or analysed and also high demands on input data, which lead to uncovering of problems and pitfalls of traditional (often many years old) methods. The main aim of this thesis is to analyse the most important RA methods, search for solutions of their typical problems and propose new methods which do not contain these problems.

The RA can be again divided into three phases:

1. Risk identification
2. Identification and analysis of risk causes
3. Identification and analysis of risk consequences

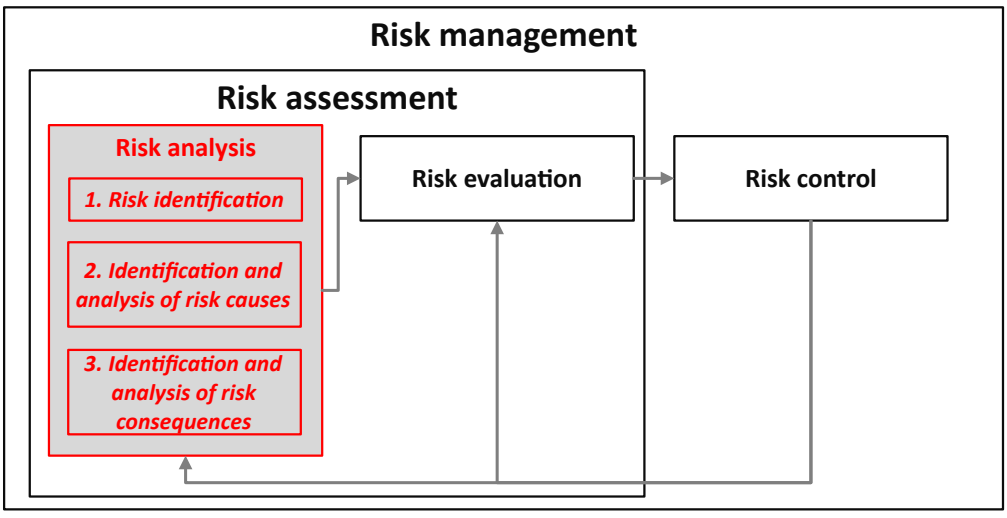


Fig. 1 Risk management parts and Risk analysis phases. Figure adapted from [1].

Each of these three phases has its own analytic and modelling methods, which are usually primarily focused on only one phase and the results must be (somehow) transferred between the phases. This could be quite bothering for example in a case, where some risk reducing measure is implemented and the risk must be recalculated by a sequence of methods. One of the goals of the thesis is to propose a new method, which is complex, so it can be used for more than one phase (and in different industrial sectors). The most logical way is to connect the causal-frequency analysis together with the consequence analysis of hazardous/undesired events into one modular model, which would be able to produce qualitative and quantitative results for both phases. To integrate these two phases into one means to model the whole accident scenario from its roots till its impacts. The new method should also manage various dependencies and complex model interconnections, which are one of the pitfalls of the traditional Fault Trees Analysis (FTA) and the Event Tree Analysis (ETA). This method should not be only theoretical, but it has to be practically usable, so it must be supported by existing software tools.

Industrial systems, their tasks or FTA/ETA models are usually Discrete Event Systems (DES), so there can be used modelling/simulation languages and frameworks, which are known from different science areas (e.g. scheduling or automation). One of the most promising candidate are Petri nets (PN) [2], which are common in engineering, scheduling or automation sectors. The PN offer graphical and mathematical interface, modularity for large and complicated cases, a dynamic behaviour modelling or simulation tools (e.g. Monte-Carlo), which are very usable in the case of analysis of complex problems, where exact equations are impossible to solve. A massive application of the PN in the RM sector is still missing, which could be several reasons e.g. a complexity of the PN or the fact that there exist tens of different classes of the PN with different features and not every class is supported by appropriate software tool. So the one of the tasks is to check them and find the most suitable class for needs of proposed method.

The main motivation of this thesis are mentioned imperfections and pitfalls of traditional methods (i.e. the FTA, the ETA) and unused potential of analytical tools (i.e. the PN) commonly used in different science sectors but not in the area of the RM. Another source of the motivation is a fact that many RM/RA methods can be used for a lot of tasks in different industrial areas (as well as non-industrial sectors) but they are not. Every area has its own specific RM/RA methods, which can be substituted in some cases by the universal ones. The situation vary from sector to sector – for example in the area of the RM/RA of road tunnels, there exist many specific methods, but also several suitable commonly used approaches known for example from chemical or aerospace industry, which are not applied in the RA of road tunnels. The author would like to show, that there is a big benefit in a preference of the universal RM/RA methods to designing of new specialized ones.

1.2 Organization of the Thesis

The thesis is organized as follows: Chapter 2 states the goals which should the thesis achieve. Chapter 3 gives an introduction to the state of the art in the topic of risk management and risk analysis of industrial systems. The results of the thesis are shown in Chapter 4. This chapter contains three main published papers of the author with a commentary and a description of their interconnection with the topics of the thesis. Chapter 5 documents the fulfilment of the goals of the thesis together. The thesis is concluded by Chapter 6 which summarizes the results and suggests possible future steps and topics to be explored.

2 Goals of the Doctoral Thesis

The main goals of the thesis are to review essential methods for the causal/frequency, consequences, reliability and accidental scenario analysis (e.g. the FTA and the ETA), find out and describe their main problems (e.g. dependencies, dynamic behaviour) and propose new approaches, which are able to solve detected imperfections and would be usable in different industrial sectors. A search for a new framework should be focused on the Petri nets and their classes as the best candidates so far. Another aim is to show that an application of known universal RA/RM methods from various science areas instead of developing new specialized ones is advantageous.

The main goals of the thesis can be briefly described as follows:

1. **Perform a survey of the main methods for risk and reliability analysis (and also in selected industrial sector).**
2. **Select the most important traditional RA/RM approaches and find out their potential problems and pitfalls (based on case studies).**
3. **Propose alternative universal methods, which are able to solve problems from the previous point, integrate more types of analysis together and make them practically usable. Test them on case studies.**

3 State of the Art

This chapter presents a literature overview of selected work connected with the topics of the thesis. The first part is focused on chosen traditional risk and reliability analysis methods – the Fault Tree Analysis and the Event Tree Analysis. These two methods represent the most popular and the most frequently used approaches, but they suffer know problems. This is the reason why there is also presented a survey of their alternatives. The most promising alternative, from the point of view of this thesis, are the Petri nets, which are a topic of the second part of this chapter.

3.1 Main Approaches

3.1.1 Fault Tree Analysis

The Fault tree analysis is a deductive or a top-down analysis, which has its origins in the Bell Laboratories. The method was developed in 1962 for an evaluation of a launch control system of the Minuteman missile project. Today is the FTA one of the most frequently used reliability/risk analysis methods and it is also covered by an international standard *IEC 61025 Fault tree analysis* [3]. The analysis itself begins with a *specific undesired or potential critical event* so-called *top event* and ends up with a structured tree which describes all causes of an occurrence of the top event. The top event often represents a *pivotal event* in an event tree (see below). The events on the lowest level of a tree are called *basic events*. The numerical output of an analysis is a probability of the occurrence of the top event. Other important results are minimal cut-sets (MCS), which represent minimal combinations of basic events, which cause occurrence of the top event. A basic FTA is a binary analysis with binary events (i.e. an event either occurs or does not occur), which are connected together using simple Boolean/logic gates (i.e. OR, AND). Besides these essential elements, there exist also advanced events (e.g. external events) and gates (e.g. priority gate, inhibit gate). All these concepts are described in the *Fault tree handbook* [4] and in its extension for aerospace applications [5]. Very good introduction to the FTA is given in books [1] and [6], which contain both theory and practical examples.

The classical FTA has known problems which some of them are mentioned in [Dis-D1] and [Dis-D2] – e.g. the FT provides only a static image of a situation, a processing of dependencies is complicated or impossible or uncertainty processing. There exist approaches alternative to the FTA, which try to solve some of these issues in one of two ways: they only "translate" a FT to different language or they define new methodologies and bring new views on situations.

A typical alternative method is the **Bayesian network approach** (BN), which offer advanced dependencies modelling, using of dynamic probabilities or coping with uncertainties and more flexible structures. A comparison of these two methods can be found in [7]. In the BN, event probabilities can be automatically updated whenever any new information has come – so this is not a static image as in the case of the FT. There exist also some disadvantages of the BN approach e.g. a problematic modelling of temporal dependencies or that the BN are very general and there does not exist any fundamental guide how to prepare a good reliability/dependability model (opposite to the FT). The FT can be used as a pattern for a structure of a corresponding BN. The FT model is mapped to the BN model which contains some new features (some of them were mentioned earlier). This approach is shown in [8] and together with the method described in [7] is a typical example of the mapping of FTs to BNs. The BN are not only the FTA or the ETA

substitution, but it also has a lot of applications in general risk, dependability and maintenance analysis as is shown in [9], which contains a very interesting summary of a BN usage.

From other concepts that enhance the FT methodology or add new features, **Binary decision diagrams** (BDD) [10] can be mentioned, which can be used for an efficient and exact computation of probabilities in a FT (as a alternative to the MCS) and for its analysis [11] or **Dynamic fault trees** (DFT) [12] which are an extension of ordinary/static FTs. The DFT contain new dynamic gates (e.g. priority-AND, functional dependency, cold-spare or sequential enforcing)[12], which offer a modelling of complex system behaviour and system components interactions (e.g. the order of an occurring of events can be taken into account during an analysis) and are often connected with Markov chains. Another alternative concept to the FT are **Petri nets**, which are mentioned in Chapter 3.2.

3.1.2 Event Tree Analysis

The Event tree analysis (ETA) is a very popular risk assessment method which is usually strongly connected with the FTA. It is a typical tool for accidental scenario modelling and analysis. This method was developed during late 1960s and the first important successful application was the WASH 1400 study from 1975, which is also known as the Rasmussen Report [13]. This risk assessment technique was standardized in 2010 by international standard *IEC 62502 Analysis techniques for dependability - Event tree analysis (ETA)* [14]. The books [6] and [1] can be used as guidelines how to use the ETA in practice and also present theoretical background of the analysis.

The ETA is (opposite to the FTA) an inductive/forward-looking method. The analysis starts with one specific *initiating/hazardous event* and ends up with *end-states/events*, which represent possible consequences of this initiating event. Between the initiating event and the spectre of end states, there is one or more other events which branch the tree and stand for barriers, which should mitigate or prevent unwanted consequences, or they represent some environmental conditions and other influences. These branching events are called *pivotal events* and they are usually modelled and analysed by a FT. A combination of the ETA and the FTA is often called a "bowtie" technique and it is an essential part of a risk evaluation methodology *Probabilistic Risk Assessment* (PRA) [15]. The ETA is common in many different application fields – from aerospace applications or nuclear power plants to chemical/offshore engineering. In the area of road tunnels risk analysis, there exist also several methods based on the ETA technique (e.g. Austrian TuRisMo model [16], Italian IRAM [17] [18]) or on the combination of the ETA and the FTA (e.g. Dutch TUNprim model [19], German BAST methodology [20]).

A typical problem with an analysis of probabilities/frequencies of end-states is an assumption that the pivotal events (i.e. their fault trees) are independent of each other, which is generally not correct. There could be temporal/logic dependencies between the pivotal events in the event chain or between the events in the fault trees (e.g. shared basic events, common cause failures). The dependencies between branches can be further divided into two basic types [21] – implicit and explicit. According to [22] and [23], the ET which contain dependencies between their branches are non-coherent systems. When all the events and branches are independent of each other, calculations of probabilities or frequencies of all end states are trivial and they are based on a simple multiplication of probabilities of the pivotal events. The topic of dependencies in the ETA is mentioned in the ETA standard [14]. There are several approaches, that introduce solutions of the problem of dependencies using different techniques: [22] presents a method based on binary decision diagrams and [23] shows an example of dependencies in the ET solved using the DFT and Markov analysis. The method presented in [21] uses the ETA with FTA as a modelling pattern for a construction of a BN, which is then capable to handle the dependencies (i.e. implicit weak s-dependencies) and present exact numerical results. The authors also

mention, that the BN approach has one deficiency, because the computational complexity of the BN increases quickly with the size of a model.

There can be found more examples of the BN applications as an alternative approach to the ETA – e.g. [24] where the ETA is translated onto BN. The main feature of this transformation is that factors, which influence an evolution of an event chain (e.g. a state of the system or its environment) and which cannot be modelled in ordinary ETA, can be explicitly added to the BN model. The authors also present some other similar approaches. The classical BN suffer the same problem as the ETA with a modelling of large systems and scenarios, because they produce large models. One of possible solutions of this issue is to use an object-oriented approach known from the computer programming combined with the BN, which is presented in [25]. This new technique is called **Object-Oriented Bayesian Networks** (OOBN) and it provides better readability and more effective modelling and probabilistic calculation for large-scale tasks. Another possible alternative method to the ETA are Petri Nets, which are mentioned in Chapter 3.2.

3.2 Petri Nets as an Alternative to Classical Methods

Beside mentioned BNs or BDDs, there exist another promising method alternative to classical risk analysis approaches (i.e. the FTA and the ETA) – **the Petri nets**, which are a very general modelling and analysis tool used in many different science, engineering and industrial applications (e.g. automation, communication, chemistry, economy, reliability theory, management). The Petri nets (PN) were conceived in early 1960s by Carl Adam Petri in his PhD thesis [2]. It is a mathematical tool with a convenient graphical interpretation for modelling and analysis of Discrete event systems (DES). Many reliability/risk models are typically Discrete Event Systems (DES), so they are good objects for the PN modelling and analysis.

The PN can be employed in the area of dependability, reliability and risk analysis and evaluation, but they are used less frequently than the classical, above mentioned approaches. One of the reason could be, that they are more complicated to understand. During the last years, the topics of the PN application in these areas have became more discussed, which culminated with a publishing of an international standard *IEC 62551 Analysis techniques for dependability – Petri net techniques* [26], where the most interesting and successful PN approaches are summarized (e.g. a structured modular PN model or High-level PN). The PNs are also mentioned in other international standards: *IEC 61508* [27] and *IEC 60300-3-1* [28]. A thorough introduction to a basic PN theory is given by [29]. Special classes of the PN which are suitable for dependability modelling are *Stochastic Petri Nets* (SPN), *Deterministic and Stochastic Petri Nets* (DSPN) [30], *Generalised Stochastic Petri Nets* (GSPN) [31] or *Stochastic Petri Nets with Predicates and Assertions* [32]. A general introduction into basic risk and reliability analysis using the PN can be found in the book [33], which is focused primarily on reliability modelling and qualitative analyses. A comprehensive study of possible applications of different PN classes (e.g. coloured, timed, SPN, GSPN, object-oriented) in the field of risk modelling and analysis is presented in [34]. The authors also included a list of interesting research papers and discuss some disadvantages of the PN (e.g. missing SW tools and PN complexity).

There are several interesting works that show the PN as an alternative to the FTA, ETA or BN, which can add new features and solve some of their typical issues and deficiencies (e.g. dynamic behaviour, dependencies). A basic comparison of the FTA, ETA and the PN approach for the accident scenario analysis is shown in [35] where the author also compares their efficiency and demanded resources. As in the case of the BN, there are two main ways how to use the PN in the area of risk analysis – the first approach is to use some other method as a pattern (i.e. to "copy" it) and add new properties to it or simply translate an existing model (e.g. a FT) to a PN

model. These two options usually do not use all the power of the PN framework and suffer some disadvantages of the original method, which they copy. The first approach can be presented by these works: The FT can be very easily translated to the PN using simple rules presented in [36] and [37]. This transformation extends classical FTA by new features connected mainly with dynamics of the PN. Similar topic of the simple mapping of a FT on a basic PN is analysed in [38] and [39]. This method does not utilize the full power of the PN. More complex rules and effective transformation of a FT to a GSPN model is introduced in [40], where also qualitative and quantitative analysis of obtained GSPN model are presented. The GSPN can be combined with the FT structure to build an extended FT, which offer modelling of multi-state components or stochastic dependencies between FT's basic events [41]. The next example of translation of classical methods on the PN is [42], where an ET model of a human reliability is transformed onto a SPN model and the numerical results are compared. A transformation of another common concept – Markov chains, which are used for reliability and maintainability analysis, to the SPN is discussed in [43]. [44] translates FTA operators onto PN and uses the PN instead of the FTA in connection with the fuzzy approach for a complete reliability analysis of repairable systems. The PN are used because their possibilities of asynchronous and concurrent processing. Another method based on the simple translation of the FT model to the PN model connected with fuzzy reasoning (i.e. fuzzy reasoning Petri nets) is shown in [45].

The second way searches for new modelling and analysis possibilities using the PN – it can be called a "free" modelling, without any defined rules or patterns. There could be a problem with a verification, that the created model is correct and useful. Some examples of the second approach include: [46] (a SPN dependability modelling and SIL calculations), [47] (another example of the SPN dependability modelling), [48] (a safety requirements and performance analysis of a hot standby using the CPN), [49] (a reliability/availability assessment of mechanical systems using the SPN), [50] (CCF modelling using CPN), [51] (a modular motorway model for risk evaluation of transportation of hazardous materials based on Coloured Timed Petri Nets), [52] (a combination of the PN and a Markov chain forms a method for vulnerability analysis of interdependent infrastructures (e.g. power and water distribution nets) against an earthquake), [53] (a CPN model for a risk assessment of IT identity management systems), [54] (a dependability SPN model of a smart grid control networks). The paper [55] presents an approach for reliability and safety analysis of manufacturing system, which is based on an example of free modelling of PN and also shows that the classical FTA can be used as a first step (for an identification of potential failures) of the method. The PN can be also used for a calculation of Safety Integrity Levels (SIL) [56]. This paper shows a comparison of a complex PN model with a simpler FTA model combined with the BDD approach. Coloured Stochastic Petri Nets (CSPN) are used for a modelling of a dynamic behaviour of a repairable system in [57], which is compared to the Monte Carlo approach for dynamic process systems. The CSPN are applied in [58] for a quantitative assessment of domino effects.

This short enumeration confirms that almost every research team uses different class of the PN, which is one of the problem why the PN are not known more broadly and employed in the area of risk and dependability analysis.

3.2.1 Software Tools

One of the often mentioned disadvantages, which causes the PN less frequent application, is an insufficient number of available comprehensive SW for the PN modelling and analysis (especially with regard to risk and reliability analysis). The existing software is mainly focused on academical or research applications – not on the professional commercial usage. The PN tools do not usually offer an advanced structure, a behaviour analysis or a stochastic modelling.

Basic PN tools (e.g. Platform Independent Petri net Editor 2 [59][60] `http://pipe2.`

sourceforge.net/ or Netlab [61]) are free and provide some basic structure analyses, but they are usable only for a basic PN class modelling and analysis. An interesting platform is Snoopy [62] http://www-dssz.informatik.tu-cottbus.de/DSSZ/Software/Snoopy, which is able to model and animate many different classes of the PN and also the FT, but it is not capable to do any analysis, which has to be done in external tools e.g. Charlie [63] (a PN structure analysis, invariants calculations, model checking) and Marcie [64] (the qualitative and quantitative analysis of GSPN). This SW triptych could be interesting for reliability and risk analysis. The TimeNET tool [65][66] https://www.tu-ilmenau.de/sse/timenet/ is a very promising platform, because it offers advanced stochastic modelling and analysis connected with coloured PN, but it has still some issues. It could be used for commercial purposes, but it is still more oriented on academic/research applications. Maybe the only commercial complex PN tool suitable for risk/reliability analysis is GRIF [32] http://grif-workshop.com/, which was originally developed in ELF Aquitaine and TOTAL laboratories. This SW package provides 10 modules focused on the PN, the FTA, the ETA, a SIL computation or Markov graphs analysis. The PN module is based on *Stochastic Petri Nets with Predicates and Assertions* and offers a hierarchic modelling, complex firing conditions or deterministic/stochastic delays with many types of probability distributions. The disadvantage of this approach is that only simulations can be used for an assessment of firing frequencies – not exact calculations.

4 Results and Papers

This chapter presents the results of the author's research related to the topic of this thesis in the form of three main author's papers relevant to the topic in combination with integrating text[1]. Every paper has a short commentary: a summary of the paper and its contribution to the thesis goals. The order of the papers presented here follows the development of author's ideas. Each of these papers is presented in the original formatting in this chapter.

[1] This format of the thesis is approved on the Faculty of Electrical Engineering of the Czech Technical University by the directive of the dean from 1.11.2014

4.1 Probabilistic Risk Assessment of Highway Tunnels

Full citation:
O. Nývlt, S. Prívara, and L. Ferkl. "Probabilistic risk assessment of highway tunnels". In: *Tunnelling and Underground Space Technology* 26 (2011). (co-authorship: Nývlt: 50%; Prívara: 30%; Ferkl: 20%), pp. 71–82. ISSN: 0886-7798. DOI: `http://dx.doi.org/10.1016/j.tust.2010.06.010`

Co-authorship (according to VVVS): Nývlt: 50 % (main author) Prívara: 30 % Ferkl: 30 %

Citations (August 2015):

- Web of Science: 10
- Google Scholar: 23

Journal statistics according to the Journal Citation Report® (August 2015)

Total Cites:	2204
Impact Factor:	1.490
5-Year Impact Factor:	1.833
Immediacy Index:	0.247
Citable Items:	158
Cited Half-life:	6.9
Citing Half-life:	9.3

Annotation:

This paper summarizes a situation of the RA methods for road, highway and city tunnels. The authors have found that many of these specialized methods suffer problems and that some universal RA methods, known from different industrial sectors, can substitute them and solve some of their issues. The paper also includes a proposal of an adapted PRA method [15], whose original version is common in the aerospace, nuclear or chemical industry. This method can be easily used for a fulfilment of needs of the RA of road tunnels. A practical application of the proposed method is shown on a real case-study, which was prepared for a planned reconstruction of one of the main city road tunnels in Prague, Czech Republic.

Contribution to the thesis:

This paper contributes to all three points of the goals of the thesis. The contribution to the first point is the survey of the methods for the risk analysis and the risk management in the selected industrial sector i.e. in the area of road/highway tunnels. These methods are analysed and some of their disadvantages are pointed out – this part of the paper contributes to the second point of the goals. The proposed adapted version of the PRA, used for a specific analysis of the real road tunnel project, represents the contribution to the last point.

This paper is available at `http://dx.doi.org/10.1016/j.tust.2010.06.010`

4.2 Dependencies in Event Trees Analyzed by Petri Nets

Full citation:
O. Nývlt and M. Rausand. "Dependencies in event trees analyzed by Petri nets". In: *Reliability Engineering & System Safety* 104 (2012). (co-authorship: Nývlt: 80%; Rausand: 20%), pp. 45–57. ISSN: 0951-8320. DOI: 10.1016/j.ress.2012.03.013

Co-authorship (according to VVVS): Nývlt: 80 % (main author) Rausand: 20 %

Citations (August 2015):

- Web of Science: 7 (out of which 1 is self-citation)
- Google Scholar: 12 (out of which 1 is self-citation)

Journal statistics according to the Journal Citation Report® (August 2015)

Total Cites:	6527
Impact Factor:	2.410
5-Year Impact Factor:	2.693
Immediacy Index:	0.559
Citable Items:	220
Cited Half-life:	7.6
Citing Half-life:	>10.0

Annotation:

This paper continuous with the topic which was mentioned in the previous work [Dis-D3], i.e. with the topic of the ETA. The first part of the paper contains a description of detected potential issues of the ETA in combination with the FTA. The selected problem is dependencies between the pivotal events of the ET. A possible solution of this problem is described in the second part of the paper and is based on a formal analysis of a non-marked PN model and its properties. This model is obtained by a transformation of the the whole ET, including all pivotal events represented by the FT, to a PN. This solution is then tested on a slightly simplified version of the case-study from [Dis-D3]. This paper is a starting point of the author's research focused on the use of the PN in the RM/RA field and is followed by papers [Dis-E1], [Dis-E2] and [Dis-D4]. This effort is concluded by the work [Dis-D2], which is described lower.

Contribution to the thesis:

This paper contributes mainly to the second and the third point of the thesis objectives because it contains a description of problems of the selected RA/RM methods, i.e. the problem of dependencies in the traditional ETA/FTA (the goal No.2). It also proposes a solution of this problem based on the non-marked PN, which contributes to the goal No.3.

This paper is available at http://dx.doi.org/10.1016/j.ress.2012.03.013

4.3 Complex Accident Scenarios Modelled and Analysed by Stochastic Petri Nets

Full citation:
O. Nývlt, S. Haugen, and L. Ferkl. "Complex accident scenarios modelled and analysed by Stochastic Petri Nets". In: *Reliability Engineering & System Safety* 142 (2015). (co-authorship: Nývlt: 80%; Haugen: 15%; Ferkl: 5%), pp. 539–555. ISSN: 0951-8320. DOI: http://dx.doi.org/10.1016/j.ress.2015.06.015. URL: http://www.sciencedirect.com/science/article/pii/S0951832015001908

Co-authorship (according to VVVS): Nývlt: 80 % (main author) Haugen: 15 % Ferkl: 5 %

Citations (August 2015):

- Web of Science: 0
- Google Scholar: 0

Journal statistics according to the Journal Citation Report® (August 2015)

Total Cites:	6527
Impact Factor:	2.410
5-Year Impact Factor:	2.693
Immediacy Index:	0.559
Citable Items:	220
Cited Half-life:	7.6
Citing Half-life:	>10.0

Annotation: The discussion about the disadvantages of the classical RM/RA approaches (especially the standard ETA) and their possible extensions continues in this paper, where the problems of the modelling and analysis of accidental scenario with a dynamic behaviour and events which can change their positions in an event chain or which can be repeated are addressed. The main outcome of the paper is a complex modelling and analysis method for complicated scenarios, where a scenario is modelled from its base causes to all consequences of the undesired event by an advanced class of the PN, i.e. the Stochastic Petri Nets with Predicates and Assertions. The method is hierarchical, modular and is inspired by a programming of a Programmable Logic Controller (PLC). It is fully compatible with the GRIF professional SW tool, which offers numerical results based on a Monte Carlo simulation. The proposed approach application is presented on a real case-study from the offshore industry.

Contribution to the thesis:
The first point of the thesis objectives is mentioned in the first part of the paper, where a basic summary of some scenario analysis methods and a large scale scenario problematic is discussed. The paper also contributes to the second point of the goals, because it addresses problems with modelling of dynamic, large and complicated accident scenarios by the traditional RM/RA methods i.e. the ETA. The proposed complex method for the modelling of the complex accident scenarios based on advanced class of the PN contributes to the last point of the thesis objectives. This complex PN based RM/RA method is the main outcome of this thesis.

This paper is available at http://dx.doi.org/10.1016/j.ress.2015.06.015

5 Fulfilment of the goals

This chapter presents a short summary of the fulfilment of the thesis objectives, which were described in Chapter 2:

1. The main and most frequently used universal and specialized RM/RA methods for selected industrial sectors (i.e. road tunnels, machine tools, ventilation systems, offshore installations) are discussed in the state-of-the-art chapters of the papers [Dis-D3],[Dis-D1],[Dis-D2] and they are also mentioned in the papers [Dis-E1],[Dis-B1],[Dis-D4].

2. The main RM/RA methods (i.e. the FTA and the ETA) were selected from the survey prepared in the previous point and some of their interesting pitfalls and disadvantages (e.g. a dynamic behaviour, dependencies, events which can change their position in an event chain) were selected, described and further analysed mainly in papers [Dis-D3],[Dis-D1] and [Dis-D2].

3. The paper [Dis-D3] shows how advantageous is to use universal RM/RA methods, which are common in some industrial sectors and can be easily adapted for needs of another industrial areas, instead of using of highly specialized methods focused on one task. The alternative methods proposed in this thesis are also generally applicable and they are based on the framework of the Petri nets. This modelling and analysis framework was selected because of its mathematical formulation, a possibility of an extension and other features help to solve problems mentioned in the second point of the thesis goals. The evolution of author's ideas with an application of the PN for the RM/RA as an alternative to the classical ETA/FTA can be seen in papers [Dis-E1], [Dis-D1],[Dis-E2],[Dis-D4] and finally in the paper [Dis-D2], which concludes the author's effort with the most complex and sophisticated methodology. Every of these papers also contains a case study, which shows how to use the proposed method.

6 Conclusions and Future Work

6.1 Summary

Risk management in the industrial area is an extensive topic which can be divided into few fundamental parts (i.e. risk analysis, risk evaluation, risk control) and which is covered by many specialized and universal methods. An objective of this thesis was not to analyse all of them, but to focus on a topic of the risk analysis part and select the most important and frequently used RA methods for a further study. A survey has shown, that instead of using universal well-known interdisciplinary methods, new highly specialized ones are developed, which is in some cases unnecessary and time consuming. The survey has also selected the FTA and the ETA as the main RA methods on which should be the thesis focused, because they are a basis of an accidental scenario analysis. An analysis, based on experiences from real applications and case studies, of these two approaches has shown that there exist some non-trivial problems and pitfalls – e.g. dependencies of the PE in the ET, when the FT contain common base events or a lack of ability to model and analyse dynamic systems and event chains with dynamic changes in an order of events. These methods may also fail or produce unclear results in cases of large systems/scenarios or when some of the PE are repeated in an event chain. This thesis contains examples of the mentioned problems.

The first part of the thesis demonstrates how advantageous it is to use adapted universal RA/RM methods. The idea is demonstrated on the case of the risk cost-effective analysis of the reconstruction of the Strahov highway tunnel in Prague, Czech republic. Instead of designing a new approach, adjusted PRA is applied. This method provides results, which are usable for a decision making about the reconstruction of the tunnel. The outputs advise to cut almost 67 % of the originally calculated costs while the level of the risk remains in required interval.

The middle part of the thesis comments a problem of the ETA where the PE (and their underlying FT) are dependent by explicit dependencies. Other types of the dependencies are also described there. The discussed solution is based on a simple transformation of both the FT and the ET onto non-marked PN, which can contain and handle mentioned dependencies. The end-states probabilities of the ET can be determined by establishment of end-sate structure functions. The method is the first step on the way to a complex RA/RM method based on the PN – the next step, which describes a (sometimes troublesome) search for an ideal PN class, is shown in papers [Dis-E1], [Dis-E2] and [Dis-D4]. These approaches show attempts how to model mechanisms of failures and repairs together in one system PN model and analyse their mutual relationships and dependencies or how to model a system state machine. The evolution starts with the class of the non-marked PN, continues with the Generalized stochastic PN, Deterministic stochastic PN, Stochastic coloured PN and finishes with the framework based on the Stochastic and deterministic PN with predicates and assertions.

The last part of the thesis proposes the most sophisticated PN based RA/RM method, which integrates causal and consequence analysis in one model – this model covers whole accident scenario. The presented approach, which is compatible with the GRIF commercial professional software tool [32], is shown on two case studies to prove its abilities and positive features. This method is able to solve problems of the ETA when a scenario or a system to analyse is large, contains repeated PE, has PE with not fixed position in an event chain or has some type of dependencies. A system or a scenario is divided into sufficiently small modules, which are built

only once, even though they can be repeated in the event sequence, and their inputs/outputs are independent on their inner structure, so it can be easily changed. These modules are connected by minimal amount of arcs and variables, so the model is easy to understand even for a non-expert.

This thesis has shown that the Petri nets can be successfully used as an universal method for both reliability analysis and risk management. The PN are not only academic tool but they are very powerful and flexible in addressing problems, which are difficult to solve by standard approaches, such as the FTA/ETA.

6.2 Future Research

The subsequent research and development should be focused mainly on improving and extending the complex method presented in the last part of the thesis [Dis-D2] to utilize the full power and potential of the PN framework. This approach is very promising, provides good results, but still suffers some disadvantages (e.g. a less readable model for a large accidental scenario). So there exist a lot of tasks and topics to discuss and solve:

- Prepare a complex user manual for the presented method. This manual should contain a basic introduction to the PN for non-experts, a description of every method element, a detailed step-by-step guide for the method and examples of basic structures.
- Run an intensive testing of the method on real industrial cases.
- One of the steps, which are needed for a better usability of the method (especially by a non-expert), is to improve the readability of the model. In a case of an extensive scenario, the corresponding model can became large and unclear (i.e. a large-scale challenge). This is a motivation for a research about more efficient representation and simplification of the model. One of possible inspiration is an object oriented approach known from computer programming (e.g. classes or inheritance), which was also applied in the case of the BN [25].
- Incorporate new features into the method and expand its abilities. There are some possible extensions:
  - Different types of dependencies e.g. time dependencies, dependencies between events, CCF, shared common events between modules etc. The time dependencies are connected with another interesting topic – a dynamically transforming event chain of a modelled scenario, where an exact sequence of events is dependent on appearance of some other events. The classical ET has a fixed order of the PE. Some events/modules can be also repeated in the sequence.
  - Risk influencing factors, which are close to dependencies and to the BN.
  - To allow events with static and non-static probabilities in one model.
  - Implement simultaneously processed blocks, which are connected to the mentioned idea of time dependent behaviour and event ordering (and which are much more close to the real life cases).
- A long-term task is to explore possibilities of an interconnection of the method with other promising approaches e.g. the BN, which can lower the number of model elements and add new features connected with conditional probabilities (e.g. uncertain input values).

Bibliography

[1] M. Rausand. *Risk Assessment: Theory, Methods, and Applications*. Wiley, 2011, p. 672. ISBN: 978-0-470-63764-7.

[2] C. A. Petri. "Kommunikation mit Automaten". PhD thesis. Bonn: Institut für instrumentelle Mathematik, 1962.

[3] IEC. *IEC 61025 Fault tree analysis (FTA)*. Tech. rep. International Electrotechnical Commission, 2006.

[4] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl. *Fault Tree Handbook*. Washington, DC: U.S. Nuclear Regulatory Commission, 1981.

[5] W. Vesely, J. Dugan, J. Fragola, Minarick, and J. Railsback. *Fault Tree Handbook with Aerospace Applications*. Handbook. Washington, DC: National Aeronautics and Space Administration, 2002.

[6] M. Rausand and A. Høyland. *System Reliability Theory, Models, Statistical Methods, and Applications*. Hoboken, NJ, USA: John Wiley & Sons, Inc, 2004.

[7] N. Khakzad, F. Khan, and P. Amyotte. "Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches". In: *Reliability Engineering and System Safety* 96.8 (2011). cited By 72, pp. 925–932. DOI: 10.1016/j.ress.2011.03.012.

[8] A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla. "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks". In: *Reliability Engineering & System Safety* 71.3 (2001), pp. 249–260. ISSN: 0951-8320. DOI: 10.1016/S0951-8320(00)00077-6.

[9] P. Weber, G. Medina-Oliva, C. Simon, and B. Iung. "Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas". In: *Engineering Applications of Artificial Intelligence* 25.4 (2012). Special Section: Dependable System Modelling and Analysis, pp. 671–682. ISSN: 0952-1976. DOI: http://dx.doi.org/10.1016/j.engappai.2010.06.002. URL: http://www.sciencedirect.com/science/article/pii/S095219761000117X.

[10] C. Ibáñez-Llano, A. Rauzy, E. Meléndez, and F. Nieto. "Minimal cutsets-based reduction approach for the use of binary decision diagrams on probabilistic safety assessment fault tree models". In: *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 223.4 (Dec. 1, 2009), pp. 301–311. DOI: 10.1243/1748006XJRR259. URL: http://dx.doi.org/10.1243/1748006XJRR259.

[11] R. Sinnamon and J. Andrews. "Fault tree analysis and binary decision diagrams". In: *Reliability and Maintainability Symposium, 1996 Proceedings. International Symposium on Product Quality and Integrity., Annual*. Jan. 1996, pp. 215–222. DOI: 10.1109/RAMS.1996.500665.

[12] J. Bechta Dugan, S. J. Bavuso, and M. Boyd. "Dynamic fault-tree models for fault-tolerant computer systems". In: *Reliability, IEEE Transactions on* 41.3 (Sept. 1992), pp. 363–377. ISSN: 0018-9529. DOI: 10.1109/24.159800.

[13] USNRC. *Reactor Safety Study, An Assessment of Accident Risk in US Commercial Nuclear Power Plants, USNRC WASH 1400 (NUREG 75/014)*. Tech. rep. 1975.

[14] IEC. *IEC 62502 Analysis techniques for dependability -– Event tree analysis*. Tech. rep. International Electrotechnical Commission, 2010.

[15] M. Stamatelatos and H. Dezfuli. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. Ed. by M. Stamatelatos and H. Dezfuli. Version 1.1. Washington, DC: NASA Office of Safety and Mission Assurance, Aug. 2002.

[16] FSV (Austria Research Association Road-Rail-Traffic). *Guideline RVS 09.03.11 "Tunnel Risk Model – TuRisMo"*. Tech. rep. 2008.

[17] ANAS S.P.A – Azienda Nazionale Autonoma Delle Strade. *Guidelines on Road Tunnel Safety Design*. Tech. rep. 2009.

[18] A. Focaracci. "Italian Risk Analysis Method (IRAM)". In: *Proceedings of the ITA Conference: "Transportation and City Tunnels"*. 2010.

[19] D. de Weger, M. Kruiskamp, and J. Hoeksma. "Road Tunnel Risk Assessment in the Netherlands , TUNprim: A Spreadsheet Model for the Calculation of Risks in Road Tunnels". In: *European Safety & Reliability International Conference ESREL 2001 - Towards a Safer World*. 2001.

[20] C. Zulauf, P. Locher, B. Steinauer, G. Mayer, U. Zimmermann, W. Baltzer, W. Riepe, and P. Kündig. *B 66: Berichte der Bundesanstalt für Straßenwesen*. Tech. rep. Bundesanstalt für Straßenwesen, 2009.

[21] S. Hosseini and M. Takahashi. "Combining Static/Dynamic Fault Trees and Event Trees Using Bayesian Networks". In: *Computer Safety, Reliability, and Security*. Ed. by F. Saglietti and N. Oster. Vol. 4680. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, pp. 93–99. ISBN: 978-3-540-75100-7. DOI: 10.1007/978-3-540-75101-4_10. URL: http://dx.doi.org/10.1007/978-3-540-75101-4_10.

[22] J. D. Andrews and S. J. Dunnett. "Event-tree analysis using binary decision diagrams". In: *IEEE Transactions on Reliability* 49.2 (2000), pp. 230–238. ISSN: 0018-9529. DOI: 10.1109/24.877343.

[23] H. Xu and J. Bechta Dugan. "Combining dynamic fault trees and event trees for probabilistic risk assessment". In: *Reliability and Maintainability, 2004 Annual Symposium - RAMS*. Jan. 2004, pp. 214–219. DOI: 10.1109/RAMS.2004.1285450.

[24] G. Bearfield and W. Marsh. "Generalising Event Trees Using Bayesian Networks with a Case Study of Train Derailment". In: *Computer Safety, Reliability, and Security*. Ed. by R. Winther, B. A. Gran, and G. Dahll. Vol. 3688. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2005, pp. 52–66. ISBN: 978-3-540-29200-5. DOI: 10.1007/11563228_5.

[25] D. Koller and A. Pfeffer. "Object-Oriented Bayesian Networks". In: *Proceedings of the 13th Annual Conference on Uncertainty in AI (UAI)*. 1997, pp. 302–313.

[26] IEC. *IEC 62551 Analysis techniques for dependability – Petri net techniques*. Tech. rep. International Electrotechnical Commission, 2012.

[27] IEC. *IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems (Part 0-7)*. Tech. rep. International Electrotechnical Commission, 1998-2000.

[28] IEC. *IEC 60300-3-1 Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*. Tech. rep. International Electrotechnical Commission, 2003.

[29] R. David and H. Alla. *Discrete, Continuous, and Hybrid Petri Nets*. Ed. by R. David and H. Alla. Springer Berlin Heidelberg, 2005. DOI: 10.1007/b138130.

[30] M. A. Marsan and G. Chiola. "On Petri nets with deterministic and exponentially distributed firing times". In: *European Workshop on Applications and Theory of Petri Nets*. 1986, pp. 132–145.

[31] M. Ajmone Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis. *Modelling With Generalised Stochastic Petri Nets*. John Wiley and Sons, 2004.

[32] SATODEV. *GRIF version 2.0*. Oct. 25th, 2013. URL: http://grif-workshop.com.

[33] W. G. Schneeweiss. *Petri Nets for Reliability Modeling*. LiLoLe-Verlag, 1999.

[34] D. Vernez, D. Buchs, and G. Pierrehumbert. "Perspectives in the use of coloured Petri nets for risk analysis and accident modelling". In: *Safety Science* 41.5 (2003), pp. 445–463. ISSN: 0925-7535. DOI: 10.1016/S0925-7535(01)00078-9.

[35] Z. Nivolianitou, V. Leopoulos, and M. Konstantinidou. "Comparison of techniques for accident scenario analysis in hazardous systems". In: *Journal of Loss Prevention in the Process Industries* 17.6 (2004), pp. 467–475.

[36] T. Liu and S. Chiou. "The application of Petri nets to failure analysis". English. In: *Reliability Engineering & System Safety* 57.2 (AUG 1997), 129–142. ISSN: 0951-8320.

[37] S. Yang and T. Liu. "Failure analysis for an airbag inflator by Petri nets". English. In: *Quality and Reliability Engineering International* 13.3 (MAY-JUN 1997), 139–151. ISSN: 0748-8017.

[38] A. Lee. "Petri net modeling of fault analysis for probabilistic risk assesment". MA thesis. University of Ontario Institute of Technology, 2013. URL: https://ir.library.dc-uoit.ca/handle/10155/334.

[39] A. Lee and L. Lu. "Petri Net Modeling for Probabilistic Safety Assessment and its Application in the Air Lock System of a CANDU Nuclear Power Plant". In: *Procedia Engineering* 45 (2012). 2012 International Symposium on Safety Science and Technology, pp. 11–20. ISSN: 1877-7058. DOI: http://dx.doi.org/10.1016/j.proeng.2012.08.113. URL: http://www.sciencedirect.com/science/article/pii/S1877705812031256.

[40] A. Bobbio, G. Franceschinis, R. Gaeta, and L. Portinale. "Exploiting Petri nets to support fault tree based dependability analysis". In: *Petri Nets and Performance Models, 1999. Proceedings. The 8th International Workshop on*. 1999, pp. 146–155. DOI: 10.1109/PNPM.1999.796561.

[41] K. Buchacker. "Combining Fault Trees And Petri Nets To Model Safety-Critical Systems". In: *Society for Computer Simulation International*. 1999, pp. 439–444.

[42] L. Bedreaga, B. Guzun, and C. Constantinescu. "Modelling of the human factor using Petri nets". In: *Bulk Power System Dynamics and Control - VII. Revitalizing Operational Reliability, 2007 iREP Symposium*. Aug. 2007, pp. 1–8. DOI: 10.1109/IREP.2007.4410579.

[43] R. V. Melnyk. "Petri Nets: An Alternative to Markov Chains". In: *Journal of the Reliability Analysis Center* 12 (2004), pp. 7–11.

[44] H. Garg. "Reliability analysis of repairable systems using Petri nets and vague Lambda-Tau methodology". In: *ISA Transactions* 52.1 (2013), pp. 6–18. ISSN: 0019-0578. DOI: http://dx.doi.org/10.1016/j.isatra.2012.06.009. URL: http://www.sciencedirect.com/science/article/pii/S0019057812000882.

[45] J. Wu, S. Yan, and L. Xie. "Reliability analysis method of a solar array by using fault tree analysis and fuzzy reasoning Petri net". In: *Acta Astronautica* 69.11–12 (2011), pp. 960–968. ISSN: 0094-5765. DOI: http://dx.doi.org/10.1016/j.actaastro.2011.07.012. URL: http://www.sciencedirect.com/science/article/pii/S0094576511002190.

[46] J.-P. Signoret. "Dependability & safety modeling and calculation: Petri nets". In: *Proceeding of the 2nd IFAC Workshop on Dependable Control of Descrete Systems, DCDS 2009*. 2009.

[47] Y. Dutuit, E. Chatelet, J. Signoret, and P. Thomas. "Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases". In: *Reliability Engineering & System Safety* 55.2 (1997). ESREL '94, pp. 117–124. ISSN: 0951-8320. DOI: 10.1016/S0951-8320(96)00108-1.

[48] G. Zhou, H. Zhao, and W. Guo. "Safety requirements analysis and performance verification of hot standby system using colored Petri net". In: *Industrial Electronics and Applications (ICIEA), 2013 8th IEEE Conference on*. June 2013, pp. 656–661. DOI: 10.1109/ICIEA.2013.6566449.

[49] G. Kumar, V. Jain, and O. P. Gandhi. "Reliability and availability analysis of mechanical systems using Stochastic Petri net modeling based on decomposition approach". In: *International Journal of Reliability, Quality and Safety Engineering* 19.01 (2012), p. 1250005. DOI: 10.1142/S0218539312500052.

[50] N. Brinzei, G. Deleuze, N. Villaume, and J.-F. Pétin. "Common cause failures modelling by means of coloured Petri nets for dependability assessment of a control system of nuclear power plant". In: *European Safety and Reliability Conference ESREL 2014*. Ed. by T. Nowakowski, M. Mlyńczak, A. Jodejko-Pietruczuk, and S. Werbińska-Wojciechowska. Safety and Reliability: Methodology and Applications. Wroclaw, Poland: CRC Press / Balkema, Taylor & Francis Group, Sept. 2014, pp. 2121–2129. URL: https://hal.archives-ouvertes.fr/hal-01083192.

[51] G. Centrone, W. Ukovich, M. Fanti, and G. Iacobellis. "A Colored Petri Net Model of motorways for risk evaluation of HAZMAT transportation". In: *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on*. Oct. 2011, pp. 562–567. DOI: 10.1109/ICSMC.2011.6083770.

[52] B. Omidvar, M. Hojjati Malekshah, and H. Omidvar. "Failure risk assessment of interdependent infrastructures against earthquake, a Petri net approach: case study - power and water distribution networks". In: *Natural Hazards* 71.3 (2014), pp. 1971–1993. ISSN: 0921-030X. DOI: 10.1007/s11069-013-0990-6. URL: http://dx.doi.org/10.1007/s11069-013-0990-6.

[53] E. Paintsil and L. Fritsch. "Executable Model-Based Risk Analysis Method for Identity Management Systems: Using Hierarchical Colored Petri Nets". In: *Trust, Privacy, and Security in Digital Business*. Ed. by S. Furnell, C. Lambrinoudakis, and J. Lopez. Vol. 8058. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, pp. 48–61. ISBN: 978-3-642-40342-2. DOI: 10.1007/978-3-642-40343-9_5. URL: http://dx.doi.org/10.1007/978-3-642-40343-9_5.

[54] R. Zeng, Y. Jiang, C. Lin, and X. Shen. "A stochastic Petri nets approach to dependability analysis of control center networks in smart grid". In: *Wireless Communications and Signal Processing (WCSP), 2011 International Conference on*. Nov. 2011, pp. 1–5. DOI: 10.1109/WCSP.2011.6096966.

[55] A. Adamyan and D. He. "Analysis of sequential failures for assessment of reliability and safety of manufacturing systems". In: *Reliability Engineering & System Safety* 76.3 (2002), pp. 227–236. ISSN: 0951-8320. DOI: DOI:10.1016/S0951-8320(02)00013-3.

[56] Y. Dutuit, F. Innal, A. Rauzy, and J.-P. Signoret. "Probabilistic assessments in relationship with safety integrity levels by using Fault Trees". In: *Reliability Engineering & System Safety* 93.12 (2008). 17th European Safety and Reliability Conference, pp. 1867–1876. ISSN: 0951-8320. DOI: http://dx.doi.org/10.1016/j.ress.2008.03.024. URL: http://www.sciencedirect.com/science/article/pii/S0951832008001099.

[57] P. Škňouřilová and R. Briš. "Coloured Petri Nets and a dynamic reliability problem". In: *Journal of Risk and Reliability* 222.4 (2008), pp. 635–642. ISSN: 1748-006X.

[58] F. Kadri, P. Lallement, and E. Chatelet. "The Quantitative Risk Assessment of domino effect on Industrial Plants Using Colored Stochastic Petri Nets". June 2012. URL: https://hal.archives-ouvertes.fr/hal-01002863.

[59] Department of Computing, Imperial College London. *PIPE2 - Platform Independent Petri net Editor 2*. Computer software v2.5. Dec. 11th, 2007. URL: http://pipe2.sourceforge.net/.

[60] P. N. Bonet, C. Lladó, R. Puigjaner, and W. J. Knottenbelt. "PIPE v2.5: A Petri Net Tool for Performance Modelling". In: *23rd Latin American Conference on Informatics (CLEI 2007)*. 2007. URL: http://pubs.doc.ic.ac.uk/pipe-clei/.

[61] RWTH Aachen - Institute of Automatic Control. *Netlab 1.80*. Jan. 14th, 2008. URL: http://www.irt.rwth-aachen.de/en/downloads/petri-net-tool-netlab.html.

[62] M. Heiner, M. Herajy, F. Liu, C. Rohr, and M. Schwarick. "Snoopy - A Unifying Petri Net Tool". In: *Application and Theory of Petri Nets*. Ed. by S. Haddad and L. Pomello. Vol. 7347. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012, pp. 398–407. ISBN: 978-3-642-31130-7. DOI: 10.1007/978-3-642-31131-4_22. URL: http://dx.doi.org/10.1007/978-3-642-31131-4_22.

[63] M. Heiner, M. Schwarick, and J.-T. Wegener. “Charlie - An Extensible Petri Net Analysis Tool”. In: *Application and Theory of Petri Nets and Concurrency*. Ed. by R. Devillers and A. Valmari. Vol. 9115. Lecture Notes in Computer Science. Springer International Publishing, 2015, pp. 200–211. ISBN: 978-3-319-19487-5. DOI: 10.1007/978-3-319-19488-2_10. URL: http://dx.doi.org/10.1007/978-3-319-19488-2_10.

[64] M. Heiner, C. Rohr, and M. Schwarick. “MARCIE - Model Checking and Reachability Analysis Done Efficiently”. In: *Application and Theory of Petri Nets and Concurrency*. Ed. by J.-M. Colom and J. Desel. Vol. 7927. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, pp. 389–399. ISBN: 978-3-642-38696-1. DOI: 10.1007/978-3-642-38697-8_21. URL: http://dx.doi.org/10.1007/978-3-642-38697-8_21.

[65] Real-Time Systems and Robotics group of Technische Universität Berlin. *TimeNET*. Jan. 15th, 2008. URL: http://www.tu-ilmenau.de/fakia/TimeNET.timenet.0.html.

[66] A. Zimmermann and M. Knoke. *TimeNET - User Manual*. Tech. rep. Real-Time Systems and Robotics group of Technische Universität Berlin, Aug. 10th, 2007. URL: http://www.tu-ilmenau.de/sse/timenet/.

Publications of the Author

Publications Related to the Thesis

Publications in Journals with Impact Factor

[Dis-A1] O. Nývlt, S. Prívara, and L. Ferkl. "Probabilistic risk assessment of highway tunnels". In: *Tunnelling and Underground Space Technology* 26 (2011). (co-authorship: Nývlt: 50%; Prívara: 30%; Ferkl: 20%), pp. 71–82. ISSN: 0886-7798. DOI: http://dx.doi.org/10.1016/j.tust.2010.06.010.

[Dis-A2] O. Nývlt and M. Rausand. "Dependencies in event trees analyzed by Petri nets". In: *Reliability Engineering & System Safety* 104 (2012). (co-authorship: Nývlt: 80%; Rausand: 20%), pp. 45–57. ISSN: 0951-8320. DOI: 10.1016/j.ress.2012.03.013.

[Dis-A3] O. Nývlt, S. Haugen, and L. Ferkl. "Complex accident scenarios modelled and analysed by Stochastic Petri Nets". In: *Reliability Engineering & System Safety* 142 (2015). (co-authorship: Nývlt: 80%; Haugen: 15%; Ferkl: 5%), pp. 539–555. ISSN: 0951-8320. DOI: http://dx.doi.org/10.1016/j.ress.2015.06.015. URL: http://www.sciencedirect.com/science/article/pii/S0951832015001908.

Publications in Reviewed Journals

[Dis-B1] O. Nývlt and J. Necid. "Bezpečnostní analýza rizik modelu Žonglér". In: *Automa* 2 (2011). (co-authorship: Nývlt: 95%; Necid: 5%), pp. 10–13. ISSN: 1210-9592.

[Dis-B2] O. Nývlt, S. Prívara, and L. Ferkl. "Probabilistic risk assessment of highway tunnels". In: *Tunnelling and Underground Space Technology* 26 (2011). (co-authorship: Nývlt: 50%; Prívara: 30%; Ferkl: 20%), pp. 71–82. ISSN: 0886-7798. DOI: http://dx.doi.org/10.1016/j.tust.2010.06.010.

[Dis-B3] O. Nývlt and M. Rausand. "Dependencies in event trees analyzed by Petri nets". In: *Reliability Engineering & System Safety* 104 (2012). (co-authorship: Nývlt: 80%; Rausand: 20%), pp. 45–57. ISSN: 0951-8320. DOI: 10.1016/j.ress.2012.03.013.

[Dis-B4] O. Nývlt, S. Haugen, and L. Ferkl. "Complex accident scenarios modelled and analysed by Stochastic Petri Nets". In: *Reliability Engineering & System Safety* 142 (2015). (co-authorship: Nývlt: 80%; Haugen: 15%; Ferkl: 5%), pp. 539–555. ISSN: 0951-8320. DOI: http://dx.doi.org/10.1016/j.ress.2015.06.015. URL: http://www.sciencedirect.com/science/article/pii/S0951832015001908.

Patents

There are no patents related to the thesis.

Publications indexed in WoS

[Dis-D1] O. Nývlt and M. Rausand. "Dependencies in event trees analyzed by Petri nets". In: *Reliability Engineering & System Safety* 104 (2012). (co-authorship: Nývlt: 80%; Rausand: 20%), pp. 45–57. ISSN: 0951-8320. DOI: 10.1016/j.ress.2012.03.013.

[Dis-D2] O. Nývlt, S. Haugen, and L. Ferkl. "Complex accident scenarios modelled and analysed by Stochastic Petri Nets". In: *Reliability Engineering & System Safety* 142 (2015). (co-authorship: Nývlt: 80%; Haugen: 15%; Ferkl: 5%), pp. 539–555. ISSN: 0951-8320. DOI: http://dx.doi.org/10.1016/j.ress.2015.06.015. URL: http://www.sciencedirect.com/science/article/pii/S0951832015001908.

[Dis-D3] O. Nývlt, S. Prívara, and L. Ferkl. "Probabilistic risk assessment of highway tunnels". In: *Tunnelling and Underground Space Technology* 26 (2011). (co-authorship: Nývlt: 50%; Prívara: 30%; Ferkl: 20%), pp. 71–82. ISSN: 0886-7798. DOI: http://dx.doi.org/10.1016/j.tust.2010.06.010.

[Dis-D4] O. Nývlt, S. Haugen, and L. Ferkl. "Stochastic Coloured Petri Nets as a modelling language for complex Event Trees". In: *SAFETY, RELIABILITY AND RISK ANALYSIS: BEYOND THE HORIZON*. (co-authorship: Nývlt: 70%; Haugen: 20%; Ferkl: 10%). CRC PRESS-TAYLOR and FRANCIS GROUP, 2014, pp. 201–208. ISBN: 978-1-315-81559-6; 978-1-138-00123-7. DOI: http://dx.doi.org/10.1201/b15938-32.

Other Publications

[Dis-E1] O. Nývlt and L. Ferkl. "A New Holistic Approach for Reliability Analysis Using Petri Nets". In: *Proceedings of the 17th ISSAT International Conference on Reliability and Quality in Design*. (co-authorship: 65%). International Society of Science and Applied Technologies, 2011, pp. 113–117. ISBN: 978-0-9763486-7-2.

[Dis-E2] O. Nývlt and L. Ferkl. "A complex analysis of repairable systems using Petri nets". In: *11th International Probabilistic Safety Assessment and Management Conference and The Annual European Safety and Reliability Conference*. (co-authorship: 90%). Curran Associates Inc., 2012, pp. 4957–4966. ISBN: 978-1-62276-436-5.

[Dis-E3] L. Rákosník, S. Prívara, O. Nývlt, L. Ferkl, and J. Zápařka. "Safety Documentation of the Strahov Road Tunnel in Prague". In: *Underground Engineering Constructions: Transport and city tunnels*. (co-authorship: 30%). Czech Tunnelling Association ITA-AITES, 2010, 903–909. ISBN: 978-80-254-7054-1.

[Dis-E4] O. Nývlt, S. Prívara, and L. Ferkl. "Risk Management in Tunnels: What Can We Learn from Aerospace Industry?" In: *ITA-AITES WTC 2009 Safe Tunnelling*. (co-authorship: 50%). Hungarian Tunnelling Association, 2009, pp. 397–398. ISBN: 978-963-06-7239-9.

[Dis-E5] O. Nývlt and M. Rausand. "Dependencies in event trees analyzed by Petri nets". In: *Reliability, Risk and Safety. Back to the Future*. (co-authorship: 70%). CRC PRESS-TAYLOR and FRANCIS GROUP, 2010, pp. 332–339. ISBN: 978-0-415-60427-7.

[Dis-E6] O. Nývlt, L. Ferkl, and J. Šulc. "Reliability of tunnel ventilation control: A conceptual design". In: *Proceedings 19th ISSAT International Conference on Reliability and Quality in Design 2013*. (co-authorship: 40%). International Society of Science and Applied Technologies, 2013, pp. 24–28. ISBN: 978-0-9763486-9-6.

Publications Not Related to the Thesis

Publications in Reviewed Journals

[NonDis-B1] O. Nývlt. "Komunikace v chytrých domech". In: *Automa* 4 (2013). (co-authorship: 100%), pp. 16–17. ISSN: 1210-9592.

[NonDis-B2] O. Nývlt. "Přehled protokolů a systémů pro řízení inteligentních budov". In: *Automatizace* 3-4 (2010). (co-authorship: 100%), pp. 121–124. ISSN: 0005-125X.

Patents

There are no patents related to the thesis.

Other Publications

[NonDis-E1] J. Šulc, O. Nývlt, and L. Ferkl. "Design and Implementation of the Control System of the Operational Ventilation in the Blanka Tunnel". In: *Tunnels for a better life - Proceedings of the World Tunnel Congress 2014*. (co-authorship: 20%). CBT/ABMS, 2014, pp. 1–9. ISBN: 978-85-67950-00-6.

[NonDis-E2] M. Rausand and O. Nývlt. "Risk Assessment: Theory, Methods, and Applications". In: (co-authorship: 40%). John Wiley & Sons, 2011. Chap. 10.6 Petri nets. ISBN: 978-0-470-63764-7.

Curriculum Vitae

Ondřej Nývlt was born in Trutnov, Czech Republic, in 1983. He finished his bachelor degree in 2006 at the Faculty of Electrical Engineering (FEE) of the Czech Technical University in Prague (CTU) in the study program *Cybernetics and measurement*. In 2008 he received his master degree at FEE CTU in the same study program with the specialisation *Control engineering*. His master thesis was supported by the *CEPOT* project. He started his Ph.D. studies in the year 2008 at the Department of control engineering (DCE) FEE CTU in the study program *Control engineering and robotics*.

Ondřej Nývlt has been involved in several research and development projects:

- *DAMIC* building control system – Department of control engineering FEE CTU
- Research grant of the Czech Ministry of Trade and Industry "Control system for optimisation of energy consumption in low-energy and passive buildings",
- Research grant of the Czech Ministry of Industry "Integration of building systems, research and application of smart algorithms affecting energy consumption in buildings",
- Research grant of the Czech Ministry of Education "EuSophos",
- Preseed project "MPC for buildings commercialization" of the University Centre for Energy Efficient Buildings of Czech Technical University in Prague.

During his bachelor and master terms, he passed two short-term abroad study stays: in 2005 at the Kristianstad University in Sweden (*ALICE* trainee-ship) and in 2008 at the TU Wien in Austria (*ATHENS TUW7* project). During his Ph.D. studies, he attended several study stays: in 2009 he spent three month at the Department of Production and Quality Engineering of NTNU Trondheim in the group of professor Marvin Rausand as a visiting researcher (supported by *EEA Research Grants*). He also attended two short-term summer schools within the *CEEPUS* project – TU Plovdiv in Bulgaria (2012) and TU Kielce in Poland (2013).

Ondřej Nývlt taught two courses at his department during his Ph.D. studies: Combinatorial Optimization and Distributed control systems. He also supervised several bachelor thesis and student projects.

He presented his scientific work at several important international conferences e.g. at *The annual European Safety and Reliability Conference* (ESREL) 2010, 2012 and 2013 or at *World Tunnel Congress* (WTC) 2009 and 2014. He published three papers in international reviewed journals, which have been cited by 16 publications indexed in the database of Web of Science. He also published three papers in Czech reviewed journals. From his other work, study materials *Buses, Protocols and Systems for Home and Building Automation* (for the study program *Intelligent buildings*) can be mentioned. He represented his department at the *IQRF Wireless Challenge* (2nd place) in 2012 and at the trade-show *INVENTO 2013*. He also acted as tutor at the *Conference and Workshop on Advanced HVAC Control*, which took place at the DCE FEE CTU in 2010.