



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

ROZŠÍŘENÍ ANALÝZY RIZIK V SYSTÉMU RTC

RISK ANALYSIS EXTENSION IN RTC SYSTEM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

DÁVID FILIČKO

VEDOUCÍ PRÁCE
SUPERVISOR

doc. RNDr. JITKA KRESLÍKOVÁ, CSc.

BRNO 2016

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav informačních systémů

Akademický rok 2015/2016

Zadání diplomové práce

Řešitel: **Filičko David, Bc.**

Obor: Management a informační technologie

Téma: **Rozšíření analýzy rizik v systému RTC**
Risk Analysis Extension in RTC System

Kategorie: Informační systémy

Pokyny:

1. Seznamte se s problematikou managementu rizik v projektech IT. Prostudujte metody používané v managementu rizik. Zaměřte se na metody FTA, ETA, FMEA, HAZOP. Diskutujte jejich vhodnost použití pro různé aplikační oblasti.
2. Seznamte se se systémem RTC pro management projektů v reálné firmě a prostudujte jeho API pro vkládání zásuvných modulů.
3. Specifikujte požadavky reálného prostředí komerční firmy na zásuvný modul analýzy rizik. Modul navrhnete.
4. Diskutujte navržená řešení a po dohodě s vedoucí vyberte vhodné z nich.
5. Zvolené řešení implementujte ve vývojovém prostředí firmy.
6. Ověřte vytvořený zásuvný modul v reálném prostředí.
7. Zhodnoťte kvalitu výsledného produktu na základě praktického ověření a diskutujte možná další rozšíření zásuvného modulu.

Literatura:

- PANDIAN, C., R.: Applied Software Risk Management - A Guide for Software Project Managers, Auerbach Publications, 2007, ISBN 0-8493-0524-1.
- VOSE, D.: Risk Analysis A quantitative guide, John Wiley & Sons, Inc., 2008, ISBN 978-0-470-51284-5.
- RAIS, K, SMEJKAL, V.: Řízení rizik ve firmách a jiných organizacích, Grada Publishing, a.s., 2006, ISBN 80-247-1667-4.

Při obhajobě semestrální části projektu je požadováno:

- Splnění bodů 1 - 3 zadání.

Podrobné závazné pokyny pro vypracování diplomové práce naleznete na adrese

<http://www.fit.vutbr.cz/info/szz/>

Technická zpráva diplomové práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap, které byly vyřešeny v rámci dřívějších projektů (30 až 40% celkového rozsahu technické zprávy).

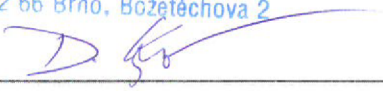
Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Kreslíková Jitka, doc. RNDr., CSc.**, UIFS FIT VUT

Datum zadání: 1. listopadu 2015

Datum odevzdání: 25. května 2016

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav informačních systémů
602 00 Brno, Božetěchova 2


doc. Dr. Ing. Dušan Kolář
vedoucí ústavu

Abstrakt

Táto práca pojednáva o rizikách, čo riziko predstavuje a aké sú metódy analýzy rizík so zameraním na metódy HAZOP, FMEA, ETA, FTA. K záveru práce je popísaný systém RTC s návrhom a implementáciou rozšírenia pre tento systém.

Abstract

This thesis is about the risks, what is the risk and what methods exist for risk analysis with the focus on HAZOP, FMEA, ETA and FTA. At the end of the thesis is described RTC system, design and implementation of extension for the system.

Klíčové slová

Riziko, analýza rizík, metódy analýzy rizík, Rational Team Concert, RTC, FMEA, HAZOP, ETA, FTA

Keywords

Risk, risk analysis, methods of risk analysis, Rational Team Concert, RTC, FMEA, HAZOP, ETA, FTA

Citácia

FILIČKO, Dávid. *Rozšíření analýzy rizik v systému RTC*. Brno, 2016. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Kreslíková Jitka.

Rozšíření analýzy rizik v systému RTC

Prehlásenie

Prehlasujem, že som túto diplomovú prácu vypracoval samostatne pod vedením doc. RNDr. Jitky Kreslíkovej, CSc. Ďalšie informácie mi poskytol Ing. Pavel Fuchs CSc. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal.

.....
Dávid Filičko
25. mája 2016

Podakovanie

Chcel by som poďakovať pani doc. RNDr. Jitke Kreslíkovej, CSc. za vedenie tejto práce a páňovi Pavlovi Fuchsovi, CSc. za poskytnutie materiálov, ktoré mi pomohli pri vypracovaní tejto diplomovej práce.

© Dávid Filičko, 2016.

Táto práca vznikla ako školské dielo na FIT VUT v Brně. Práca je chránená autorským zákonom a jej využitie bez poskytnutia oprávnenia autorom je nezákonné, s výnimkou zákonne definovaných prípadov.

Obsah

1	Úvod	3
2	Manažment rizík a riziko	4
2.1	Riziko	4
2.1.1	Definícia rizika	4
2.1.2	Úžitok z rizika	5
2.1.3	Najčastejšie zdroje rizík v projektoch IT	5
2.2	Manažment rizík	7
2.2.1	Identifikácia rizík	8
2.2.2	Register rizík	12
2.2.3	Hodnotenie rizika	13
2.2.4	Efektívne riadenie rizík s využitím skóre závažnosti	15
2.2.5	Plánovanie reakcie na riziko	15
2.2.6	Sledovanie a kontrola rizík	18
2.3	Manažment rizík v IT	18
2.3.1	Všeobecne o informačných systémoch a technológiách	19
2.3.2	Analýza a meranie problémov rizík	20
2.3.3	Použitie rizikového riadenia v projektoch	22
3	Metódy analýzy rizík	26
3.1	Rozhodovacie modely	26
3.1.1	FTA	31
3.1.2	ETA	36
3.2	FMEA	38
3.3	HAZOP	41
3.3.1	Princípy skúmania	43
3.3.2	Vodiace slová a odchylky	44
4	Rational Team Concert	47
4.1	Všeobecne ku RTC	47
4.2	Vývojové prostredie a API systému RTC	49
5	Návrh a implementácia	54
5.1	Výber metód	54
5.2	Špecifikácia požiadaviek rozšírenia	54
5.3	Implementácia	54

6 Testovanie	59
6.1 Prípadová štúdia - ETA	59
6.2 Prípadová štúdia - FTA	60
7 Záver	63
Literatúra	64
Prílohy	66
Zoznam príloh	67
A Obsah CD	68

Kapitola 1

Úvod

Hlavnou témou tejto diplomovej práce je manažment rizík. Celá práca sa pohybuje v tomto obore a predstavuje metódy používané pri analýze rizík a vysvetľuje, čo riziko vlastne predstavuje.

Cieľom tejto práce je spracovať metódy pre analýzu rizík a návrhnúť rozšírenie pre systém RTC (Rational Team Concert) a následne ho implementovať do tohto systému. Návrh a implementácia sa skladá z dvoch častí. Prvá analyzuje požiadavky na rozšírenie a druhá používanie tohto systému.

V kapitole 2 je všeobecne popísaný manažment rizík. V kapitole 3 sú popísané jednotlivé metódy, konkrétne FTA, ETA, FMEA a HAZOP. Kapitola 4 vysvetľuje na čo sa používa systém RTC a popisuje vývojové prostredie systému. V kapitole 5 sú zanalyzované požiadavky na toto rozšírenie. V kapitole 6 je ukážka dát, ktorá vznikla pri prvotnom používaní tohto rozšírenia a v kapitole 7 je táto práca zhodnotená spolu s diskusiou nad možnými vylepšeniami.

Táto práca je sčasti postavená na semestrálnom projekte. Všetky kapitoly boli doplnené o ďalšie znalosti a informácie. V kapitole 2 boli prevzaté časti o definícii rizika, úžitku z rizika, identifikácii rizík, manažmentu rizík a niektoré plány a reakcie na riziko manažmetu rizík. V kapitole 3 jednotlivé metódy boli čiastočne prevzaté, ale upravené a rozšírené o teóriu rozhodovacích modelov. Z kapitoly 4 bol prevzatý úvod k systému RTC doplnený o chýbajúce informácie. Samotný návrh a implementácia boli úplne pozmenené z dôvodu došpecifikovania rozšírenia.

Zadanie práce

Pri riešení práce je potrebné zoznámiť sa s problematikou analýzy rizík a preštudovať metódy používané v manažmente rizík. Ďalej je pri riešení práce nutné zoznámiť sa so systémom RTC a preštudovať jeho API pre vkladanie zásuvných modulov, špecifikovať požiadavky na tento zásuvný modul, navrhnúť riešenie pre tento modul a následne tento modul implementovať vo vývojovom prostredí firmy.

Kapitola 2

Manažment rizík a riziko

Táto kapitola sa venuje riziku a manažmentu rizík. V úvode je popísané riziko, vysvetlená je aj jeho definícia. Ďalej je vysvetlený dôvod prečo podstupovať riziko a aké su najčastejšie zdroje rizík projektov v odbore IT. V druhej kapitole je vysvetlený manažment rizík, v čom spočíva. V manažmente rizík je popísaná práca pri identifikovaní rizík a ich následná analýza. Na záver kapitoly je rozobraný manažment rizík v IT a ako sa využíva riadenie rizík v IT projektoch.

2.1 Riziko

V originálnom znení je riziko spájané s hazardom alebo s podstupovaním niečoho nebezpečného, čo nám môže ublížiť. Ak berieme riziko na seba je šanca, že vyhráme alebo prehráme. Taktiež neistota v podnikaní sa stala známou pod rizikom. Hoci každé podnikanie je vo svojej podstate riskantné. Ak vyvíjame nový produkt, sú tu neznáme faktory, ktorých dopad na podnikanie je rovnako neznámy. Tieto faktory môžu byť priaznivé, ale rovnako aj nepriaznivé. Tieto faktory sú spojené s pravdepodobnosťou, ktorá zapríčiní generovanie zisku alebo straty, a práve strata môže podnik oslabiť. Preto sa podniky snažia oceňovať pravdepodobnosť straty a porovnávať ju s pravdepodobnosťou zisku. Rozhodnutie, či podstúpiť takéto riziko závisí na šanci ku priaznivému alebo nepriaznivému výsledku. Z toho vyplýva aj, že riziko je pravdepodobnosťou utrpenia straty [14].

2.1.1 Definícia rizika

Ako už bolo zmienené vyššie, za riziko sa považuje pravdepodobnosť utrpenia straty. Túto definíciu by bolo vhodné vylepšiť o ciele, zisky alebo príležitosti. Určite je zrejmé, že riziko môže byť spojené aj so ziskom. Pretože, ak oddelíme riziko od cieľov, tak potom človek vidí len zoznam problémov. Z toho vyplýva, že riziko by nemalo byť len rozdelené do zoznamu problémov. Riziko má totižto širšiu rolu.

Z toho ďalej vyplýva to, že by sa mal zväžiť aj rozsah škôd plynúcich z rizika. Rozsah škôd sa dá finančne ohodnotiť. A ak je rozsah škôd znesiteľný, ale zisky sú mimoriadne atraktívne, objavuje sa nový pohľad na rozhodnutie. Niektorí sú ochotní podstúpiť riziko, aj keď pravdepodobnosť straty je vyššia ako 50%, teda je jasné, že za prah rizika sa nemôže považovať 49%. Riziko je vážený parameter. Jeho váha závisí na rozsahu straty očakávanej rizikom, za predpokladu, že sa riziko niekedy vyskytne. Riziko môžeme definovať ako kombináciu pravdepodobnosti výskytu rizika a rozsahu strát, ktoré pôsobia pri výskyte.

Niekedy procesy nie sú kontrolované a výsledky nie sú predpovedateľné alebo nie je možné povedať, aký výsledok bol zamýšľaný. Toto je neprípustné a práve toto vedie k stratám, ktoré predstavujú riziko. V tomto prípade, pôvod rizika nie je kritérium, ale predvídateľnosť a kontrola sú veľmi dôležité faktory. Na základe toho by kompletná definícia rizika mohla byť nasledujúca: *Riziko je pravdepodobnosť utrpenia straty pri realizovaní cieľov, kvôli faktorom, ktoré nie sú predvídateľné.*

Pri bližšom skúmaní rizík si môžeme všimnúť, že riziká sa dajú rozdeliť do dvoch kategórií. Tieto kategórie popisujú, odkiaľ sa dané riziko môže prejaviť. Tieto kategórie sú:

- **Vonkajšie riziká.**
- **Vnútorne riziká.**

Vnútorne riziko môžeme definovať ako pravdepodobnosť utrpenia straty pri zlepšovaní výkonu a cieľoch rastu z dôvodu nedostatkov v možnostiach procesov a organizačnej štruktúry. Zatiaľ čo **vonkajšie riziko** môžeme definovať ako pravdepodobnosť utrpenia straty pri zlepšovaní výkonu a cieľoch rastu z dôvodu neistoty v externých podmienkach.

2.1.2 Úžitok z rizika

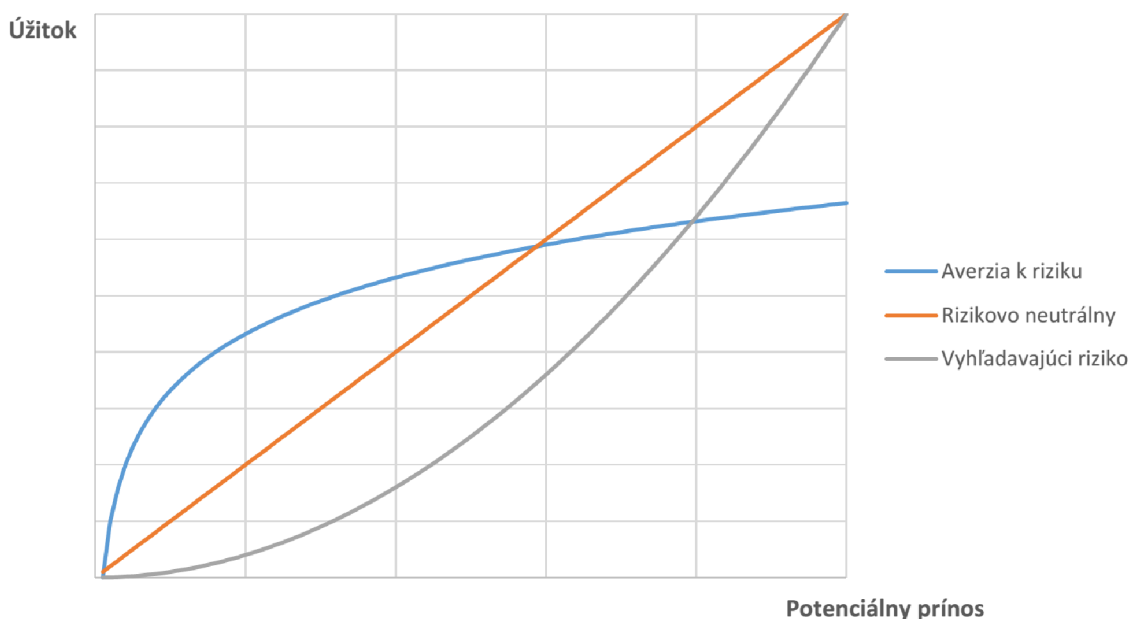
Niektorí odborníci na riziko odporúčajú, aby sa organizácie i jednotlivci vo všetkých stránkach projektov i v osobných životoch pokúsili nájsť vhodnú rovnováhu medzi rizikom a príležitosťami. Myšlienka dosiahnutia rovnováhy medzi rizikom a príležitosťou napovedá, že rôzne organizácie a rôzni ľudia môžu mať k riziku rôznu toleranciu. Sú organizácie aj ľudia, ktorí majú k rizikám neutrálnu toleranciu, iní k nim majú odpor resp. averziu a iní riziko s obľubou vyhľadávajú. Tieto tri typy preferencií rizika sú súčasťou teórie rizík.

Úžitok z rizika resp. **tolerancia k riziku** je množstvo uspokojenia alebo výhod, plynúcich z potenciálnych prínosov rizika. Na obrázku 2.1 vidíme základný rozdiel medzi organizáciami alebo ľuďmi, ktorí majú averziu, ktorí majú neutrálny postoj k riziku a ktorí vyhľadávajú riziko. Na ose y je vynesенý úžitok resp. miera uspokojenia z podstúpenia rizika a na ose x je znázornený objem potenciálnych výhod, príležitostí alebo prínosov, teda peňažná hodnota danej rizikovej príležitosti. **Averzia k riziku** znamená nízku toleranciu k riziku, čiže rast úžitku sa v takomto prípade u rastúcich možných prínosov znižuje. Inými slovami, ak sa takáto organizácia alebo ľudia dostanú k možnosti získania vyšších výhod alebo väčšieho objemu peňazí, získajú menej uspokojenia a menej úžitku. Opakom sú ľudia a organizácie, ktoré **vyhľadávajú riziká**, čiže majú vysokú toleranciu k riziku a ich uspokojenie, či úžitok sa pri rastúcich potencionálnych výnosoch zvyšuje. To znamená, že takíto ľudia a organizácie preferujú takéto príležitosti, aj keď výsledok je zatažený vyššou mierou neistoty, ale zároveň nesie takáto príležitosť aj vyššie výnosy. Často sú tieto organizácie alebo ľudia ochotní niesť finančné straty za podstúpenie rizika. Rizikovo neutrálne organizácie alebo osoby sa snažia dosiahnuť rovnováhu medzi rizikom a prínosom [16].

Aby sme mohli zvyšovať naše príjmy musíme byť ochotní podstupovať určité množstvo rizika, aby sme sa dostali aspoň na úroveň rizikovo neutrálnych. Tým zvýšime potenciálne zisky, preto je potrebné chápať riziko a naučiť sa ho kontrolovať.

2.1.3 Najčastejšie zdroje rizík v projektoch IT

Mnohé z organizácií si vytvárajú svoje vlastné dotazníky rizík. Tieto dotazníky slúžia k tomu aby zistili, na ktoré otázky sa majú najviac zamerať. Ak sa odpovede na tieto otázky pohy-



Obr. 2.1: Funkcia úžitku z rizika pri rôznych preferenciách rizika [16].

byjú v správnych hodnotách, podnik sa rozhodne projekt realizovať. V týchto dotazníkoch nájdeme tieto široko pojaté kategórie rizík spolu s ich prípadnými otázkami:

- **Tržné riziká.** Ak je úlohou daného projektu z informačných technológií vývoj nového produktu alebo služby, bude tento produkt či služba pre organizáciu prínosný, alebo bude mať na trhu šancu uplatniť sa u potenciálnych zákazníkov? Prijímu užívateľa nový produkt (službu) a zvyknú si na jej používanie? Nemôže niekto iný vytvoriť lepší produkt alebo službu, alebo s ním prísť na trh skôr, takže by celý projekt bol len stratou času a peňazí?
- **Finančné riziká.** Môže si organizácia riešenie tohto projektu vôbec finančne dovoliť? Nakoľko kľúčoví účastníci projektu dôverujú finančným odhadom? Splní projekt odhadovanú čistú súčasnú hodnotu (NPV), návratnosť investície (ROI) a dobu návratnosti? Ak nie, môže si organizácia dovoliť v projekte pokračovať? Je projekt skutočne tým najlepším, do čoho môže organizácia investovať svoje finančné prostriedky?
- **Technologické riziká.** Je projekt vôbec technicky zvládnuteľný? Budú sa pri ňom používať stabilné a vyspelé, špičkové alebo zastarané technológie? Kedy budú prijaté rozhodnutia o konkrétnych použitých technológiach? Budú hardwarové, softwarové a sieťové komponenty v projekte správne fungovať? Bude potrebná technológia k dispozícii včas, aby sa dokázali naplniť ciele projektu? Môže sa stať, že príslušná technológia je zastaraná, ešte predtým než sa podarí produkt vytvoriť? Kategóriu technologických rizík môžeme rozdeliť na zmienené hardwarové, softwarové alebo sieťové.
- **Ľudské riziká.** Má organizácia dostatok pracovníkov s odpovedajúcimi schopnosťami, ktoré budú potrebné k úspešnému vyriešeniu projektu, alebo dokáže ich včas prijať? Majú títo ľudia potrebné manažérske a odborné znalosti? Majú dostatok praxe alebo skúseností? Podporuje tento projekt taktiež vyššie firemné vedenie? Má projekt

nejakého kľúčového zástupcu? Pozná organizácia dosatočne dobre svojho zákazníka alebo zadávateľa projektu? Ako dobré vzťahy má s týmto zadávateľom alebo zákazníkom?

- **Štrukturálne a procesné riziká.** Aký stupeň zmeny bude nový projekt zavádzať do užívateľskej oblasti a do vecných či obchodných postupov? Koľko rôznych skupín užívateľov musí tento projekt uspokojiť? S koľkými ďalšími systémami bude musieť nový projekt alebo systém komunikovať? Má organizácia zavedené príslušné procesy, s ktorými bude možné projekt úspešne dokončiť? [16]

2.2 Manažment rizík

Najlepší spôsob ako definovať manažment rizík je preskúmať jeho účel a výhody. Jeho účel môže byť len jeden, a to zredukovať škody spôsobené rizikom. Cieľom nie je eliminovať riziko. Je ním riadenie rizika a orezanie straty ako najviac to len bude možné. Ako iný manažment, manažment rizík využíva stratégie a plány, aby vyhovel cieľom organizácie [14]. V samotnej podstate je manažment rizík systematické používanie politík, postupov a pracovných techník manažmentu úloh, zaoberajúcich sa určovaním súvislostí, zisťovaním, analýzou, vyhodnotením, posudzovaním, ošetrovaním, monitorovaním rizík a komunikáciou o nich takým spôsobom, ktorý umožňuje organizácii minimalizovať straty a maximalizovať vhodné príležitosti nákladovo efektívnym spôsobom.

Čiže skrátene, manažment rizík je systematický prístup k redukcii škôd spôsobených rizikom, čím robí projekt menej zraniteľnejším. Manažment rizík sa skladá z týchto procesov (vývojový diagram týchto procesov je možné vidieť na obrázku 2.2):

1. **Určovanie rizík.** Súvislosti rizika, vrátane technických, podnikových, komerčných, politických, finančných, právnych, zmluvných a tržných cieľov, ktoré môžu obmedzovať alebo presmerovať projekt, majú byť presne vymedzené. Majú byť zistené ciele projektu, ktoré majú byť dosiahnuté, aby sa vyhovel požiadavkám projektu, podniku a zákazníka vo všetkých etapách projektu a tieto ciele sa majú použiť k tomu, aby pomáhali pri zaisťovaní a klasifikácii rizík. Taktiež majú byť zvažované kritériá prijateľnosti a únosnosti rizika. Tieto kritériá sa používajú pre vyhodnotenie rizík v neskorších etapách procesu.
2. **Zisťovanie rizík.** Tomuto procesu je venovaná sekcia 2.2.1.
3. **Posudzovanie rizík.** Tomuto procesu je venovaná sekcia 2.2.3
4. **Ošetrovanie rizika.** Tomuto procesu je venovaná sekcia 2.2.5.
5. **Preskúmanie a monitorovanie rizika.**
 - (a) **Nepretržité.** Prvotnou úlohou preskúmania a monitorovania rizika je zistiť akékoľvek novo vzniknuté riziká a zaistiť, že ošetrovanie rizika zostane efektívne. Efektívnosť procesu manažmentu rizík má byť tiež preskúmaná. Preskúmanie rizika v priebehu životného cyklu projektu zaisťuje to, že príslušné dokumenty, normy, postupy a registre sú aktualizované a udržiavané. Monitorovanie rizika má byť nepretržité po celú dobu života projektu. Má zahŕňať vyšetrovanie rozpočtu projektu a iných údajov projektu. Hlavné činnosti monitorovania môžu byť realizované v kľúčových mílnikoch projektu, alebo keď sa okolité prostredie projektu významne zmenilo.

- (b) **Po realizácii projektu.** Po dokončení projektu sa má zrealizovať preskúmanie manažmentu rizika, aby bolo zaistené to, že je proces manažmentu rizika efektívny a stanovilo sa, ako môže byť tento proces zlepšený pri budúcich projektoch. V mnohých prípadoch je možné získať ponaučenie, ktorého podstata má byť upresnená a začlenená do postupov a procesov.

Výhody manažmentu rizík môžu byť rozdelené do dvoch kategórií a to na **priame** a **nepriame výhody**. Priame výhody zahŕňajú nasledujúce:

1. **Ciele sú dosiahnuté.**
2. **Projekt je ochránený pred hlavnými rizikami.**
3. **Projekt je viac odolný voči rizikám.**
4. **Ludia sú pripravení riešiť problémy.**
5. **Produkt sa stáva viac spoľahlivejším.**
6. **Náklady na nekvalitné produkty klesajú.**
7. **Praktiky riešenia problémov na mieste krízového manažmentu sú nepotrebné.**

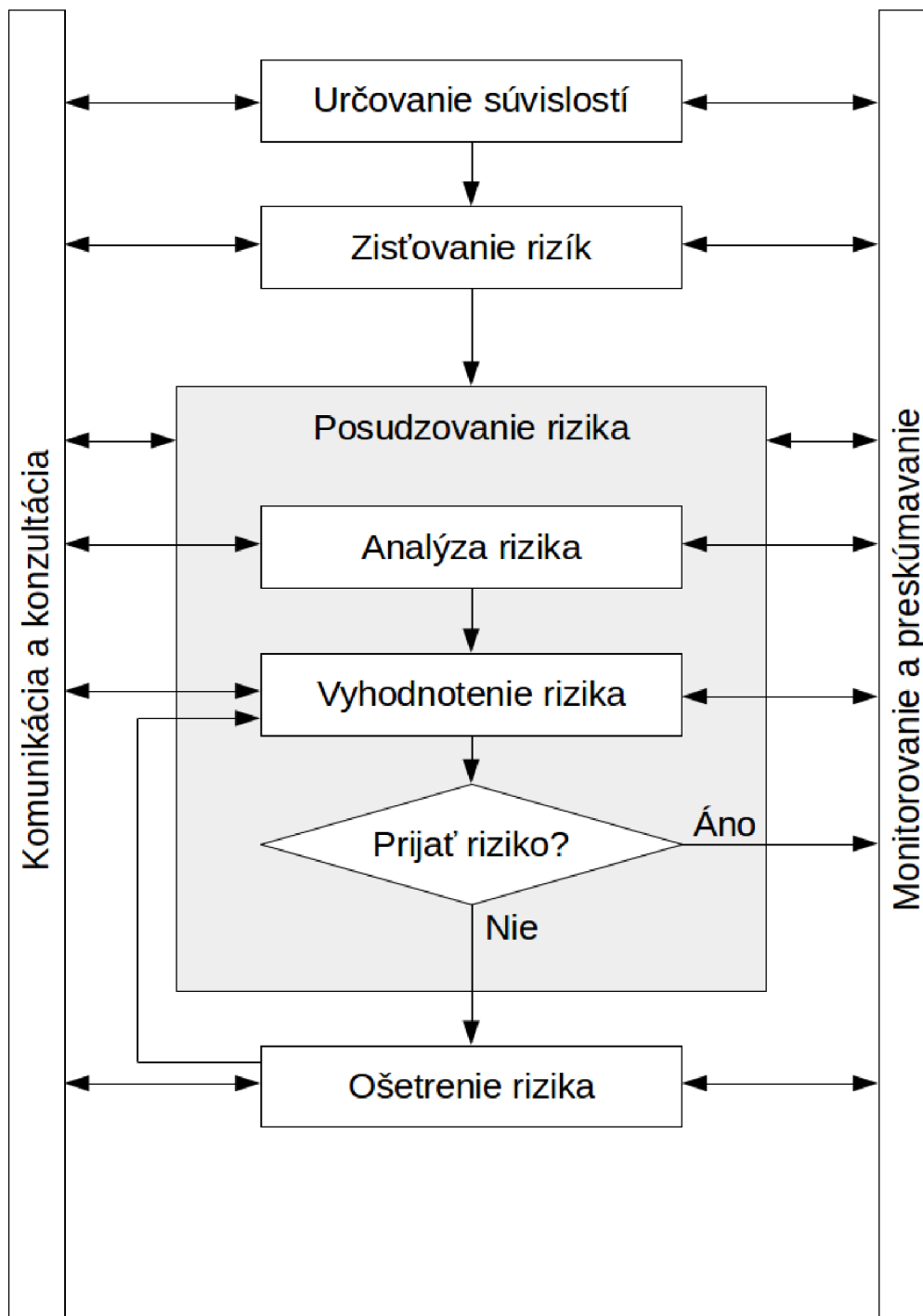
Nepriame výhody vychádzajú z priamych výhod. Zoznam týchto výhod je dlhý, ale je možné ho vidieť vo všetkých oblastiach procesov [2, 14].

2.2.1 Identifikácia rizík

Identifikácia rizík je prvým krokom pri úplnej analýze rizík, vzhľadom na to, ak ten, kto vedie tím dobre definoval ciele. Existuje množstvo techník, ktoré pomáhajú formalizovať identifikáciu rizík. Táto časť analýzy rizík dokazuje, že ide o najviac informatívny a konštruktívny element procesu.

Projektové tímy často zahajujú tento proces revíziami projektovej dokumentácie, aktuálnych a historických informácií súvisiacich s danou organizáciou a zhrnutím predpokladov, ktoré môžu mať vplyv na riešenie projektu. Členovia projektových tímov diskutujú o týchto informáciách na poradách, ktorých sa niekedy účastnia aj externí konzultanti a odborníci a kladú tu dôležité otázky ohľadom vzťahu preberaných faktorov k rizikám. Až keď projektový tím na tejto úvodnej porade indentifikuje základný okruh potencionalných rizík, môže pomocou rôznych techník zhromažďovania informácií indentifikovať ďalšie riziká. Šesť najzákladnejších a najdôležitejších techník zhromžďovania informácií je:

1. **Brainstorming.**
2. **Delfská metóda.**
3. **Rozhovory.**
4. **Analýza prvotných príčin.**
5. **SWOT analýza.**
6. **Promptné zoznamy**[18, 16, 5].



Obr. 2.2: Vývojový diagram procesu manažmentu rizík projektu [2].

Brainstorming

Brainstorming (anglicky doslovne „búrka mozgov“) je technika, pri ktorej sa určitá skupina ľudí pokúša vytvárať nápady alebo nájsť postup pre riešenie určitého problému takým spôsobom, že jednotliví členovia prinášajú nápady najprv spontánne, bez okamžitého kritického posudzovania. Tento postup skupinovej diskusie môže pomôcť vytvoriť vyčerpávajúci zoznam rizík, ktorými sa budú členovia zaoberať neskôr v podrobnej kvantitatívnej a kvalitatívnej analýze rizík. Brainstroming by mal viesť skusený moderátor, ktorý by mal prednášať taktiež nové kategórie potenciálnych rizík a priebežne tak oživovať tok myšlienok. Po zhromaždení nápadov môže moderátor výsledky zjednotiť a rozdeliť do lepšie zvládnuteľných kategórií. Brainstroming je trebné používať opatrne a rozhodne by sme ho nemali používať nadmerne alebo nesprávne. I keď v mnohých firmách sa touto technikou často vymýšľajú nové nápady, odborná psychologická literatúra uvádza, že ak jednotlivci môžu pracovať samostatne, dokážu vyprodukovať nakoniec väčší počet nápadov ako v malej skupinke. Skupinové efekty oslabujú u účastníkov ich kreatívnosť. Najčastejšími dôvodmi sú strach zo spoločenského znemožnenia, vedomie prítomnosti hierarchie autorít a ovládnutie porady jedným alebo dvoma príliš výrečnými a príliš aktívnymi osobami [16, 5, 7].

Delfská metóda

Zaujímavým postupom pre zhromažďovanie informácií, ktorý umožňuje prekonať niektoré z negatívnych skupinových efektov brainstormingu, takzvaná **delfská metóda** (Delfi). Jej základnou myšlienkou je dosiahnutie zhody v skupine odborníkov, ktorí sa pokúšajú predvídať budúci vývoj. Delfská metóda sa realizuje v opakovaných kolách otázok a písomných odpovedí, medzi ktoré môžu patriť aj pripomienky k odpovediam predchádzajúcich kôl. Takto je možné zhromaždiť podklady od celej skupiny, a zároveň sa vyhnúť jednostrannému zaujatiu, ktoré môže pri ústnej diskusii vzniknúť. Pri uplatnení delfskej metódy je nutné predovšetkým zvoliť vhodnú skupinu odborníkov na dotýčnú oblasť. Ak sa odpovede líšia aj po niekoľkých kolách, musí moderátor delfskej metódy zistiť, či nie je v celom procese nejaký skrytý problém [16, 5].

Rozhovory

Rozhovor (interview) je technika hľadania faktov a zhromažďovania informácií, ktorá správne prebieha tvárou v tvár, ale často môže byť realizovaná taktiež formou telefonického rozhovoru alebo videokonferenciou, elektronickou poštou alebo rýchlou výmenou správ. Pýtanie sa a vedenie rozhovoru s ľuďmi, ktorí majú skúsenosti z podobných projektov, sú mimo iných dôležitým nástrojom pre identifikáciu rizík. Ak máme napríklad v rámci nášho projektu pracovať s nejakým konkrétnym typom hardwaru či softwaru, môžeme osloviť niekoho, kto má s touto technológiou čerstvé skúsenosti a opýtať sa, či nemal v projektoch nejaké problémy. Podobne, ak už niekto pracoval s určitým zákazníkom nám môže dodať cenné postrehy ohľadom potencionálnych rizík vznikajúcich pri spolupráci s touto skupinou [16, 5].

SWOT analýza

Ďalšou technikou je SWOT analýza (anglicky to znamená **S**trengths, **W**eaknesses, **O**pportunities, **T**hreats, teda analýza silých stránok, slabých stránok, príležitostí a hrozieb). Táto metóda sa často používa pri strategickom plánovaní. Analýzu SWOT môžeme používať

aj v rámci identifikácie rizík v konkrétnych projektoch. Pred vytvorením určitého návrhu manažér projektu spolu so skupinou vybraných zamestnancov podrobne prediskutuje ich silné a slabé stránky a aké príležitosti a hrozby pre nich existujú (hlavne, ktoré súvisia s navrhovaným projektom). Ak túto analýzu následne aplikujeme na konkrétne projekty, môžeme tým identifikovať viac rizík a príležitostí daného scenára [16, 5].

Promptné zoznamy

Promptné zoznamy poskytujú množinu kategórií rizík, ktoré sú relevantné k typu projektu alebo typu rizika zvažovaného organizáciou. Zoznamy napomáhajú ľuďom rozmýšľať pri identifikácii rizík. Občas sa používajú rôzne typy zoznamov dohrmady, aby sa zlepšila šanca identifikácie všetkých rizík, ktoré sa môžu vyskytnúť. Napríklad, pri analyzovaní projektu jeden z promptných zoznamov môže pozeráť na rôzne aspekty projektu (napr. právne, komerčné, technické), alebo typ úloh zapojených do projektu (napr. návrh, implementácia, testovanie). Plán projektu a štruktúra delenia práce, spolu so všetkými definovanými hlavnými úlohami sú prirodzené promptné zoznamy. Pri analyzovaní spoľahlivosti nejakého výrobného závodu sa môžu použiť zoznamy rôznych druhov porúch (napr. mechanických, elektrických, elektronických, ľudských), alebo zoznam strojov, alebo zahrnutých procesov.

Promptný zoznam nikdy nebude vyčerpávajúci, ale pôsobí ako stredobod pozornosti pri identifikácii rizík. Nezáleží na tom, či riziko spadá do jednej alebo druhej kategórie, podstatné je, že bolo identifikované. Nasledujúci zoznam ukazuje príklad všeobecného promptného zoznamu:

- **Administrácia.**
- **Akceptovanie projektu.**
- **Komerčné.**
- **Enviromentálne.**
- **Finančné.**
- **Znalosti a informácie.**
- **Právne.**
- **Manažment.**
- **Politické.**
- **Kvalita.**
- **Zdroje.**
- **Stratégia.**
- **Technické.**

V každej z kategórií je množstvo podkategórií, ktoré s ňou súvisia [18].

2.2.2 Register rizík

Výstupom procesu indentifikácie rizík je zoznam indentifikovaných rizík a ďalšie informácie nevyhnutné pre zahájenie tvorby takzvaného **registra rizík**. Register rizík je v podstate dokument, ktorý obsahuje výsledky rôznych procesov riadenia rizík a často býva znázornený vo forme tabuľky alebo tabuľkového listu. Je to nástroj pre dokumentovanie potencionálnych rizikových udalostí a s nimi súvisiacich informácií. Rizikové udalosti sú pritom konkrétne neisté udalosti alebo okolnosti, ktoré môžu vzniknúť a poškodiť projekt, alebo pre neho naopak môžu byť prospešné. Medzi negatívne rizikové udalosti patrí napríklad nedosiahnutie výkonových parametrov, omeškanie pri dokončovaní prác oproti časovému plánu, zvýšenie odhadovaných nákladov, nedostatok materiálu pre výrobu, súdne spory s našou spoločnosťou apod. Ako príklad pozitívnych rizík je možné menovať dokončenie prác v kratšej než plánovanej dobe alebo nižšie plánované náklady, lepšia verejná mienka o organizácii, ktorá vzniká pri dokončení projektu apod. Register rizík zväčša obsahuje tieto položky:

- **Identifikačné číslo každej rizikovej udalosti.** Projektový tím potrebuje niekedy rizikové udalosti zoradiť alebo medzi nimi vyhľadávať konkrétne položky, a preto je nutné každé riziko nejakým spôsobom identifikovať pomocou jedinečného identifikátora, napríklad čísla.
- **Hodnotenie danej rizikovej udalosti.** Projektový tím má obvykle číselnú stupnicu, pričom číslo jedna odpovedá najmensej miere rizika.
- **Názov rizikovej udalosti.** Lubovoľný názov, napríklad Závada serveru, Neskoré dokončenie testov, Nižšie náklady na konzultácie, alebo Dobrá verejná mienka.
- **Popis rizikovej udalosti.** Názov rizikovej udalosti zvykne byť často skrátený a nemusí zodpovedať presnému významu, preto je vhodné uviesť do tejto položky jej podrobnejší popis. Udalosť nižších nákladov na konzultácie môžeme napríklad v rámci popisu rozvinúť a uviesť, že organizácia môže za prácu nejakého externého konzultanta vyjednať nižšiu než obvyklú cenu, napríklad preto, že býva v mieste pobočky organizácie a bude rád, ak kvôli zákazke nemusí dochádzať.
- **Kategória, do ktorej táto riziková udalosť spadá.** Závada serveru môže napríklad spadať pod širšiu kategóriu technologických rizík alebo do podkategórie hardwarových technologických rizík.
- **Prvotná príčina rizika.** Prvotná príčina závalu serveru môže byť napríklad závada napájacieho zdroja.
- **Spúšťač danej rizikovej udalosti.** Spúšťače sú symptómy resp. indikátory skutočného vzniku rizikovej udalosti. Prekračovanie nákladov hneď v prvých aktivitách riešeného projektu môže byť napríklad symptómom chybné stanovených dohadov. Chybné výrobky môžu byť symptómom nízkej kvality príslušného dodávateľa. Ak projektový tím zdokumentuje takéto symptómy potenciálnych rizík v projekte, môže tím identifikovať viac potenciálnych rizikových udalostí.
- **Potenciálna reakcia na jednotlivé riziko.** Ako potenciálnu reakciu na rizikovú udalosť chyby serveru môžeme uviesť požiadavku zmluvného ujednanja s dodávateľom serveru, ktorý je povinný opraviť chybný server za vopred dohodnutú cenu a vo vopred stanovený čas.

- **Vlastník rizika**, je osoba, ktorá prevezme zodpovednosť za riziko. Určitý človek bude napríklad zodpovedať za všetky rizikové udalosti spojené s chodom serveru a aj za riadenie reakcie na riziko.
- **Pravdepodobnosť vzniku rizika**. Vznik určitej rizikovej udalosti môže byť zaťažený vysokou, strednou alebo nízkou pravdepodobnosťou. Riziko skutočného vzniku chyby serveru môže byť vyhodnotené ako riziko s nízkou pravdepodobnosťou.
- **Dopady prípadného vzniku rizika pre projekt**. Ak k danej rizikovej udalosti skutočne dôjde, táto udalosť môže mať vysoký, stredný alebo nízky dopad na úspech riešeného projektu. Chyba serveru bude mať napríklad pre úspešné dokončenie projektu vysoký dopad, ak všetky dáta budú uložené práve na tomto servery.
- **Stav rizika**. Došlo skutočne k popísanej rizikovej udalosti? Bola hotová stratégia pre reakciu na riziko? Je riziko pre daný projekt naďalej relevantný? Pri chybe serveru sa môže napríklad uviesť, že už do zmluvy s dodávateľom bola doplnená požadovaná klauzula.

Po skončení identifikácie rizík sa pristupuje k ďalšiemu kroku, pri ktorom sa realizuje kvantitatívna analýza, pri ktorej sa zistí, ktoré riziká sú najzávažnejšie[14, 16, 5].

2.2.3 Hodnotenie rizika

Vo fáze identifikácie rizík sa manažéri pokúšajú identifikovať všetky riziká, ktoré ohrozujú úspech projektu alebo ciele organizácie. Je dôležité, aby bola poroznosť zameraná na tieto riziká, ktoré predstavujú najväčšiu hrozbu. Z toho dôvodu sa realizuje hodnotenie rizík, pri ktorej sú jednotlivé riziká ohodnotené pomocou určitého stupňa (skóre).

Kvantitatívne metódy

Kvantitatívne metódy sú založené na matematickom výpočte rizika z frekvencie výskytu hrozby a jeho dopadu. Tieto metódy používajú číselné ocenenia, ako v prípade pravdepodobnosti vzniku incidentu, tak i pri oceňovaní dopadu udalosti. Vyjadrujú dopad obvykle vo finančnom vyjadrení. Najčastejšie je riziko vyjadrené ako ročná predpokladaná strata. Ich realizácia síce vyžaduje viac času a úsilia, ale potom poskytujú finančné vyjadrenie rizík, ktoré je pre ich zvládnutie výhodnejšie, a to predovšetkým pre finančnú, technicko-bezpečnostnú alebo indromačno-bezpečnostnú oblasť [17, 15].

Kvalitatívne metódy

Kvalitatívne metódy sú postavené na popise závažnosti potenciálneho dopadu a na pravdepodobnosti, že daná udalosť nastane. Riziká sú v týchto metódach vyjadrené v určitom rozsahu, napríklad v intervale 0,0 – 1,0 pre pravdepodobnosť, alebo na škále 1 – 10 alebo dokonca slovným popisom veľké/malé/stredné. Úroveň rizika je určovaná kvalifikovaným odhadom. Tieto metódy sú jednoduchšie, rýchlejšie, ale vďaka tomu i viac subjektívne a chýba im jednoznačné finančné vyjadrenie. Význam týchto metód je predovšetkým v tom, že poskytujú podklady pre plány prevencie [17, 15].

Definovanie kvalitatívneho popisu rizika

Kvalitatívne posúdenie pravdepodobnosti P rizikovej udalosti (možnosť, že nastane udalosť, ktorá negatívne ovplyvní projekt alebo organizáciu) a dopady, ktoré môže vytvárať I , môže byť tvorená priradením popisu k veličinám týchto pravdepodobností a dopadov. Posudzovateľ je opytovaný za účelom popísania pravdepodobnosti a dopadu každého rizika, vyberá ich z prednastavených fráz ako napríklad *žiadne*, *veľmi malé*, *malé*, *stredné*, *veľké* a *veľmi veľké*. Rozsah hodnôt je potom priradený každej fráze v poradí tak, aby bola zaistená konzistencia medzi odhadmi jednotlivých rizík. Príklad takého priradenia môžete vidieť v tabuľke 2.1 [18].

Kategória	Cena (\$)	Zdržanie (dní)	Pravdepodobnosť (%)
Veľmi veľké	>10 000	>60	>70
Veľké	3 000-10 000	40-60	50-70
Stredné	1 000-3 000	20-40	30-50
Malé	300-1 000	10-20	10-30
Veľmi malé	<300	<10	<10

Tabuľka 2.1: Kvalitatívne ohodnotenie rizík [18]

Vizualizácia portfólia rizík

Tabuľka pravdepodobnosti a dopadu ponúka rýchlu cestu, ako vizualizovať relatívny význam všetkých identifikovaných rizík, ktoré sa týkajú projektu alebo organizácie. Tabuľka 2.2 ukazuje príklad vizualizácie rizík. Všetky riziká sú vykreslené v jednej tabuľke, čo umožňuje jednoduchú identifikáciu najviac ohrozujúcich rizík rovnako ako schopnosť ilustrovať celkovú rizikovosť projektu [16, 18].

Pravdepodobnosť	Veľké	Riziko 6	Riziko 9	Riziko 1 Riziko 4
	Stredné	Riziko 3 Riziko 7	Riziko 2 Riziko 5 Riziko 11	
	Malé		Riziko 8 Riziko 10	Riziko 12
		Malý	Stredný	Veľký
		Dopad		

Tabuľka 2.2: Vizualizácia rizík pomocou tabuľky [16]

Klasifikácia rizika pomocou skóre

Hodnotenie pomocou skóre sa používa na klasifikáciu identifikovaných rizík. Váhový vektor je priradený každej fráze použitej k popisu každého typu dopadu. V tejto klasifikácii znamená vyššie skóre vyššie riziko. Najčastejšie sa do váhového vektoru používajú hodnoty pravdepodobnosti a ohodnotený popis dopadu. Tieto hodnoty sú následne vynásobené, a tak získame výsledné číslo hodnotenia rizika.

Môžeme taktiež definovať závažnosť rizika jednoduchými členmi:

$$S = P \cdot I, \quad (2.1)$$

kde P je pravdepodobnosť a I je dopad. Ak má riziko k -možných dopadov (kvalita, cena, reptácia) s rôznymi pravdepodobnosťami pre každý typ, môžeme ho skombinovať do jednej rovnice:

$$S = \log_{10} \left(\sum_{i=1}^k 10^{P_i \cdot I_i} \right). \quad (2.2)$$

Pomocou skóre je teraz možné určiť najdôležitejšie riziká. Manažment sa tým pádom môže zamerať na prostriedky určené k redukcii alebo k eliminácii rizík v projekte. Nevýhodou tohoto prístupu je, že projekt bude značne závislý na jednotlivom škálovaní faktorov, ktoré sú priradené ku každej fráze popisujúcej dopady rizika. Ale ak máme lepšie informácie o pravdepodobnosti alebo dopade, tak hodnotenie nám môže zaistiť presnejšie skóre.

Skóre ponúka konzistentné meranie rizík, ktoré je možné využiť k definovaniu metrík a vytvoreniu analýzy trendov. Napríklad rozdelenie skóre závažnosti v projekte dáva indikáciu celkovej výške podstupovaného rizika [16, 18].

2.2.4 Efektívne riadenie rizík s využitím skóre závažnosti

Efektívne riadenie rizík sa snaží dosiahnuť maximálne redukcie rizík za danej veľkosti inštitúcií (ľudské zdroje, čas, peniaze). Preto potrebujeme posudzovať riziká v určitom pomere (redukcia rizika/investícia k dosiahnutiu redukcie). Pokiaľ použijeme logaritmické merítko pre závažnosť, použijeme nasledujúce vyčíslenie:

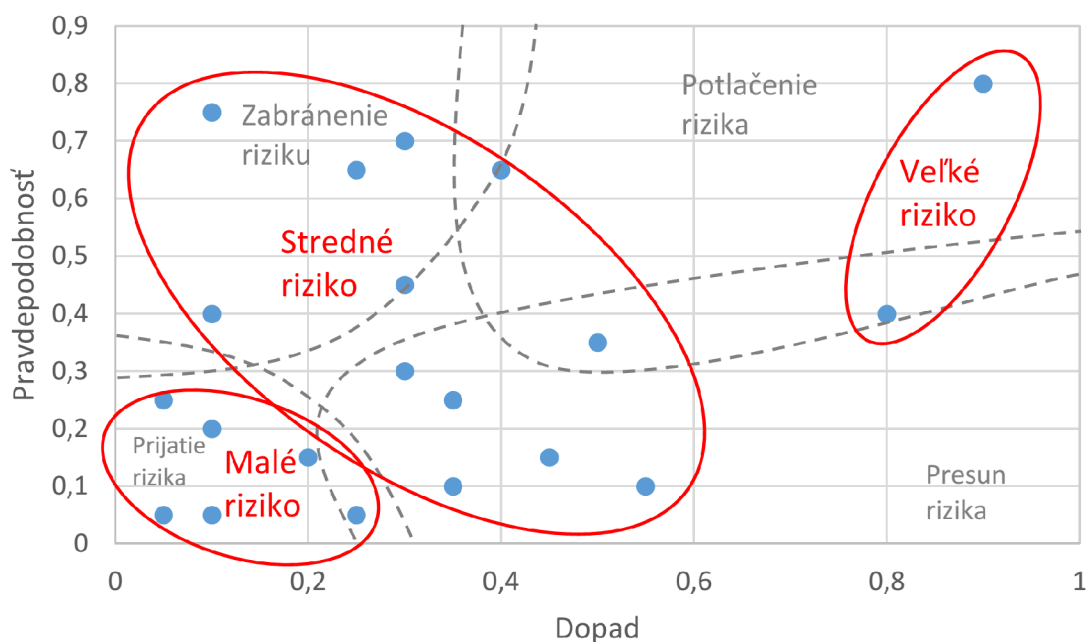
$$Efektivnos = \frac{\sum 10^{S_{nove(i)}} - \sum 10^{S_{stare(i)}}}{investicia} \quad (2.3)$$

Možnosť riadenia rizík, ktoré poskytujú najvyššiu efektívnosť sú logicky preferované. Inherentným rizikom chápeme také riziko, ktoré ešte nebolo zmiernené alebo redukované. Tieto riziká môžu byť vykreslené oproti rámcu rizikových reakcií, v ktorých sú vizualizačné tabuľky rozdelené, pokryté prekrývajúcimi sa oblasťami *zabráneniu rizika*, *prijatie rizika*, *prenos rizika*, *potlačenie rizika*, ako je to možné vidieť na obrázku 2.3.

2.2.5 Plánovanie reakcie na riziko

Hneď ako organizácia zistí, teda identifikuje riziká a podrobí ich kvantitatívnej analýze, musí pre ne pripraviť vhodnú reakciu. Pri tvorbe reakcií na riziko sa definujú nasledujúce stratégie oslabenia negatívnych rizík a posilnenia pozitívnych rizík. Na negatívne riziká môžeme reagovať pomocou nasledujúcich stratégií:

1. **Akceptácia rizika.** Nerobí sa nič pre kontrolu rizika. Je to vhodné pre riziká, kde náklady na kontrolu rizika sú úplne mimo v pomere k riziku. Akceptovať riziko je



Obr. 2.3: Graf vizualizačnej tabuľky s hranicami jednotlivých stratégií plánovania reakcie na riziko [18]

vhodné pre riziká s nízkou pravdepodobnosťou a nízkym dopadom. Musíme dať ale pozor, aby dané riziko nebolo vysoko rizikové. Ak zvolíme akceptáciu rizika, mali by sme ho zvažovať a zaradiť ho do pohotovostného plánovania. Napríklad projektový tím pripravuje veľkú poradu s revíziou celého projektu. Tento tím môže pristupovať k rizikám aktívne a pre prípad, že by sa im nepodarilo rezervovať si vhodnú zasadaciu miestnosť, si pripraví mimoriadny či záložný plán a mimoriadne rezervy. Na strane druhej môžu postupovať pasívne a prijať takú miestnosť, akú im prideli asistentka v organizácii.

2. **Zabránenie riziku** znamená potlačenie konkrétnej hrozby alebo rizika, dosiahnutie zvyčajne potlačením jeho príčin. Samozrejme nie všetkým rizikám môžeme úplne zabrániť, konkrétnym rizikovým udalostiam ale zabrániť môžeme. Obyčajne je využívané pre riziká s vysokou pravdepodobnosťou a vysokou mierou dopadu. Napríklad používať odskúšanú a otestovanú technológiu namiesto novej, ktorá bola zamýšľaná alebo presunúť výrobu do novej krajiny, kvôli vyhnutiu sa nestabilite vlády v terajšej krajine. Je potrebné uvedomiť si, že so zmenou môžu prísť aj ďalšie nové riziká a pravdepodobne omnoho viac dôležitejšie.
3. **Prenos rizika** zahŕňa manipuláciu s rizikom tak, že riziko je presunuté z jednej skupiny ľudí na druhú. Stratégia prenosu rizika využíva kontrakty, kde je istá forma penalizácie zahrnutá v zmluve kontraktora. Ďalšou možnou formou prenosu rizika je poistenie. Poistenie sa veľmi často používa pri práci s finančnými rizikami. Ak poisťovňa vypočíta riziká správne, tak organizácia zaplatí menšiu čiastku navyše ako boli očakávané náklady kvôli provízii poisťovne. Vo všeobecnosti organizácie prenášajú riziká preto, lebo chcú držať riziká mimo vlastnú organizáciu.

4. **Potlačenie rizika** vyjadruje zníženie dopadu rizikovej udalosti pomocou zníženia pravdepodobnosti jeho výskytu. Príkladom potlačenia rizika môže byť používanie osvedčených technológií, zapojenie preškoleného personálu alebo zdatného odborníka, uplatnenie rôznych analytických a validačných techník.
5. **Rezervy na pokrytie rizík.** Reakcia manažmentu na identifikované riziká je zvyčajne pridať nejaké rezervy na pokrytie rizika, ktoré môže nastať. Je to vhodné pre riziká s malým až stredným dopadom. Príkladom takejto stratégie môže byť alokovanie extra financií na projekt, alokovať extra čas na dokončenie projektu, mať hotovostné rezervy, mať dostatočné zásoby kópii softwaru na predaj (krabicové verzie).

Pri príprave stratégií sa myslí aj na pohotovostné plánovanie. Pohotovostné plánovanie vo svojej podstate reprezentujú plány navrhnuté na optimalizovanie odozvy na riziko, ktoré môže nastať. Môžu byť použité v spolupráci s akceptačnými a redukčnými stratégiami. Pohotovostný plán by mal identifikovať jednotlivcov, ktorí berú zodpovednosť za monitorovanie výskytu rizika a identifikované riziko vedú ku zmene jeho pravdepodobnosti alebo možného dopadu. Takýto plán by mal identifikovať všetko, čo je potrebné urobiť, kto to má urobiť a v akom poradí. Príkladom pohotovostného plánovania môže byť trénovaný požiarný tím, pripravená tlačová správa, viditeľný telefónny zoznam s číslami koho kontaktovať ak riziko nastane, pripravené záložné zdroje elektrickej energie.

Pri plánovaní stratégií na negatívne riziká je potrebné myslieť aj na pozitívne riziká. Na pozitívne riziká môžeme reagovať pomocou nasledujúcich stratégií:

1. **Využitie rizika** znamená urobiť čokoľvek, aby príslušné riziko nastalo. Príkladom takéhoto využitia rizika môže byť, že manažér projektu môže zorganizovať napísanie článku do miestnych novín o tomto projekte, sám napísať tlačovú správu, ale usporiadať inú verejnú udalosť, v rámci ktorej využije projekt pre posilnenie verejnej mienky o firme. Týmto môže firme vzniknúť ďalšia obchodná príležitosť.
2. **Zdieľanie rizík** je pridelenie vlastníctva rizika druhej strane. Príkladom môže byť spojenie organizácie s inou organizáciou, ktorá bude projekt ďalej distribuovať, a tak sa budú spolupodieľať na publicite.
3. **Posilnenie rizika** je zmena veľkosti príležitosti, ktorej dosiahneme pomocou identifikácie a maximalizácie kľúčových faktorov pozitívneho rizika. Dôležitým faktorom pri získavaní dobrej publicity projektu je, ak sa podarí zainteresované strany nadchnúť pre projekt tak, že urobia projektu formálnu a neformálnu reklamu.
4. **Prijatie rizika** platí aj pre pozitívne riziká, a to v prípade, že projektový tím nemôže ku vzniku rizika prispieť žiadnym opatrením alebo sa rozhodne takéto opatrenie nezrealizovať.

Analýza rizík môže popisovať úroveň neistoty ako rozhodovací problém. Neistotu používame ako odlišnosť od prirodzenej náhodnosti. Neistota môže byť často redukovaná alebo posilnená (pri pozitívnych rizikách) získaním nových znalostí. Vtedy môže človek zodpovedný za rozhodnutia stanoviť, že je tam až príliš veľa neistoty pre vytvorenie robustného rozhodnutia a môže požiadať o dodatočné získanie znalostí. Použitím analýzy rizík, analytik môže poradiť nízkonákladovú metódu zbierania ďalších dát, ktoré budú potrebné pre získanie potrebnej úrovne presnosti [18, 16, 2].

2.2.6 Sledovanie a kontrola rizík

Do činností monitorovania resp. sledovania a kontroly rizík radíme vykonávanie takých procesov riadenia rizík, ktoré reagujú na konkrétne rizikové udalosti. Vykonávanie týchto procesov riadenia rizík potom znamená zabezpečiť, že celý tím bude udržiavať povedomie o rizikách a sledovať ich ako priebežnú aktivitu a budú ju vykonávať počas celej doby riešenia projektu. Riadenie rizík v projekte určite nekončí pri počiatkovej analýze rizík. Riziká, ktoré sme takto identifikovali sa nemusia vôbec prejavíť, prípadne môžu celkovo zaniknúť. U skôr identifikovaných rizikách môžeme zistiť, že majú vyššiu pravdepodobnosť vzniku alebo u nich hrozí vyššia odhadovaná strata. Podobne v priebehu riešenia projektu identifikujeme aj nové riziká, ktoré musia prejsť rovnakým procesom ako riziká identifikované pri počiatkovej analýze rizík. Ak dôjde ku zmenám v relatívnom vystavení projektu jednotlivým rizikám, môže byť niekedy potrebné zmeniť taktiež rozdelenie zdrojov vyhradených na riadenie rizík.

Pri vykonávaní jednotlivých plánov riadenia rizík musíme sledovať riziká podľa definovaných milníkov a prijímať rozhodnutia ohľadom rizík a stratégie reakcie na ne. Ak sa určitá stratégia ukáže byť neúčinnou, za predpokladu, že implementujeme plánovanú mimoriadnu aktivitu alebo odstránime zo zoznamu riziko, ktoré už prestalo existovať, musíme stratégiu rizík zmeniť. Projektové tímy taktiež často zasahujú k rôznym náhradným riešeniam. Náhradné riešenia sú neplánované reakcie na rizikovú udalosť, ktorá nie je pokrytá vhodným mimoriadnym plánom.

Ako nástroje a techniky pre sledovanie a kontrolu rizík môžeme používať metódy opakované hodnotenia rizík, audity rizík, analýzu odchýliek a trendov, technické výkonové opatrenia, analýzu rezerv a pravidelné porady s hodnotením a revíziami stavu rizík, na ktorých môžeme vykonávať taktiež sledovanie desiatich najrizikovejších položiek. Výstupom z popísaného procesu sú požadované zmeny, doporučené nápravné opatrenia a preventívne opatrenia, aktualizované verzie registra rizík, plánov projektu a organizačných aktív organizácie, ako sú napríklad poučné informácie, ktoré využijeme pri riešení nových a budúcich projektov.

2.3 Manažment rizík v IT

Rozšírený výskyt rizík a problémov v bežnom živote, v obchodovaní a projektoch, podporujú proaktívne pokusy k riadeniu rizík, ich účinkov a následkov. Moderné koncepty vznikli okolo 17. storočia vplyvom priekopníckej činnosti Pascala a jeho súčasníkov. Viedli k zlepšeniu porozumenia povahy rizika a lepšie štrukturovali snahu riadiť ich.

V súčasnej dobe je rizikový manažment používaný ako súčasť projektového manažmentu. Využívaný je predovšetkým pre veľké, komplexné a inovatívne projekty. Niektoré názory však považujú rizikový manažment iba za dočasnú alebo prechodnú časť v oblasti projektového riadenia, výsledky rizikových analýz sú často zanedbávané a nie je na nich kladený dostatočný dôraz, čo vedie k chybnej činnosti celej tejto časti projektového riadenia.

Aby bolo rizikové riadenie plne efektívne, je potrebné integrovať ho do celkového projektového riadenia s čo najužšími väzbami k jednotlivým procesom riadenia. Nesmie byť nastavené iba ako voliteľná súčasť. Rizikové riadenie musí byť plne integrované v systéme, tak aby pomáhalo organizáciám efektívne dosahovať ich vopred nastavených cieľov [13, 15].

2.3.1 Všeobecne o informačných systémoch a technológiách

Informačné systémy a technológie sú medzi nami cez 50 rokov a ich cieľom je efektívne zmeniť a vylepšovať podnikateľské a informačné procesy. Ľudia sa o tieto kroky snažia viac než tisíc rokov. Zdalo by sa, že s takými bohatými skúsenosťami budú informačné technológie a systémy už na veľmi vysokej úrovni úspešnosti (za predpokladu, že by bol dodržaný časový plán a rozpočet). Bohužiaľ to tak nie je. V osemdesiatych rokoch bola viac ako polovica všetkých IT riešení neúspešná a aj z tých, ktoré boli úspešné veľmi malý počet prispel k zmene alebo vylepšeniu.

Dôvody prečo väčšina IT projektov sklamala, sú tieto:

- Problémy boli rozpoznané príliš neskoro.
- Problémy boli zle riadené - typicky nesystémovým, ad-hoc spôsobom (riešenie určitého problému až v dobe, kedy nastane a jedinečným spôsobom) a manažéri riešili rovnaké problémy rôznymi metódami.
- Problémy neboli sledované a vedené v databáze.
- Skúsenosti z riešenia problémov neboli použité k vylepšeniu budúceho rozhodovacieho modelu manažmentu.
- Ľudia mali tendenciu opakovať rovnaké chyby.

Pri deklarovaní požiadaviek na vývoj nového alebo na úpravy starého systému sa predpokladá, že užívatelia podporujú snahu o zmeny a vylepšenia, to však nebýva pravda. Tento problém sa týka predovšetkým skúsenejších osôb, ktoré už majú svoj spôsob riešenia problémov a neradi ich menia. Ďalším problémom býva prípad, keď užívateľ, ktorý má systém schvaľovať, často nerozumie zmenám a vylepšeniam a systém kvôli tomu neschváli. Veľakrát sa chyba nachádza v oblasti inštrukcie a implementácie nového systému.

Väčšina problémov vzniká pri vzájomnom neporozumení sa užívateľov a jednotlivých podnikateľských oddelení [13].

Typy jednotlivých problémov

Problémy vznikajú vo vnútorných oblastiach, ktoré sa týkajú pracovných tímov, samotnej práce, podnikateľských jednotiek, manažmentu a projektov. Ďalej vznikajú problémy vo vnútorných oblastiach, ktoré sa týkajú predovšetkým predajcov, konzultantov, outsourcingu (zaistovanie časti prevádzky organizácie inou externou organizáciou), centrály organizácie, dcérskych spoločností, využívaných technológií a obchodných partnerov. Dajú sa taktiež identifikovať problémy a riziká špecifických IT aktivít medzi, ktoré patrí: analýza zadania, softwarové balíky, samotný vývoj softwaru a servisná podpora.

Najčastejšie príklady problémov v organizáciách

Najčastejšie problémy môžeme rozdeliť do piatich oblastí. Prvou oblasťou sú problémy na strane **zákazníka** alebo **užívateľa**. Medzi tieto problémy patria: nedostatok dostupných prostriedkov, neochota tímu k zmenám a novým návrhom, neznáma kvalita dát, nekvalifikovaný zákaznícky personál, nepoužívanie určitých položiek korektnou cestou, nedostatočné porozumenie obchodných pravidiel, nedostatok informácií o konkrétnom systéme (systém potom nemusí byť schválený), neodsúhlasenie špecifikácie systému, problémy s jazykovými

prekladmi, užívatelia neprijímajú nové zmeny, veľká zaneprázdnenosť užívateľov vedúca k nespokojnosti pri práci na projekte a nedostatok štandardizovaných postupov.

Druhou oblasťou sú problémy na strane **manažmentu**. Jedná sa o nedostatok času na generovanie testovacích dát, nedostupnosť prostriedkov, nesledovanie interpretácie problémov, nízka priorita, časové pásma, jazykové problémy, vysoké očakávania manažmentu, talentová nezhoda, nedostatočné financovanie, oneskorenie pod vplyvom previazania rôznych projektov, veľká závislosť na externých organizáciách a zmeny v oblasti top manažmentu.

Ďalšou oblasťou sú **projektové a plánovacie problémy**. Patrí k nim: príliš sekvenčné úlohy, príliš detailné plánovanie, situácie, kedy zmysel daného projektu nie je od začiatku jasný, narastajúci rozsah projektov, neochota zmeny štruktúry projektu, asynchrónny plán s aktuálnymi výsledkami, potreba organizovaného prístupu pri riešení mimoriadnych situácií, opakované prepracovanie projektu a príliš veľa úloh nevčlenených do plánu.

Štvrtou oblasťou sú **technické a systémové problémy**. Patria sem: neaktuálnosť dát, potreba veľkého vstupného manuálu, staré systémy bez dokumentácie, zlé alebo chybné znalosti, neplatný zdrojový kód, obmedzené znalosti aplikácií, nedostatočné znalosti overených postupov, prechody na nové technológie, nedostatočný rozsah testovacích dát, chybné pracujúce moduly, testovacie prostredie, ktoré nedostatočne kopíruje reálny priebeh a kvalita práce.

Poslednou oblasťou sú problémy na strane **subdodávateľov**. Do tejto oblasti patrí: nízka kvalita ponúkaného softwaru, skutočnosť, kedy dodávateľ tvrdí, že na zadanú úlohu je málo času alebo si dodávateľ nastavil vysokú prioritu v oblasti konkurencieschopnosti, výber zlého dodávateľa, neporozumenie medzi projektovým vedúcim dodávateľa a jeho zamestnancami, proces vyhľadávania dodávateľa, ktorý dodá riešenie za stanovenú cenu, oneskorenie projektu spôsobené nedostatočným dodávaním, odstúpenie dodávateľa od projektu pred jeho ukončením, častá výmena zamestnancov u dodávateľa, nezdieľanie informácií dodávateľa s jeho zákazníkmi, situácie, v ktorých dodávateľ používa iné metódy a nástroje než zadávateľská organizácia a situácie, kedy dodávateľ nereaguje dostatočne pružne a rýchle [13].

2.3.2 Analýza a meranie problémov rizík

Cieľom analýzy a merania je zavčas varovať pred vznikom nežiadúcich udalostí.

Problémy pri štandardnom meraní

Každý projekt má svoj rozpočet, rozsah a časový plán. Tak môžeme sledovať a porovnávať celkový rozpočet a plán s aktuálnym stavom. Tieto kroky sú veľmi časté pri riadení projektov, napriek tomu však náklady na začiatku projektu nekorešponujú s celkovými nákladmi vynaloženými na dokončenie projektu. Pôvodný plán totiž nepočíta s tým, že môže nastať väčšia potreba hardwaru, softwaru a sieťových infraštruktúr, a tým dochádza k ďalšiemu nárastu práce, ktorá sa premietne v celkovom rozpočte.

Príčinou oneskorenia projektu je väčšinou to, že v určitej fáze vznikol problém, a že po identifikácii tohto problému sa ľudia snažili vysporiadať sa ním, ale nepodarilo sa im to, a tým pádom bolo potrebné plán upraviť. V tejto situácii nastáva zároveň problém s časom, ktorý sa v priebehu riešenia problémov stratí a oneskorenie sa stáva oveľa viac viditeľnejšie, čo vedie k narastajúcemu tlaku.

V IT projektoch nastáva problém najčastejšie v neskoršej fáze projektu. Pri zostavovaní požiadaviek, vytváraní designu alebo získavaní nástrojov a materiálov pre vývoj nepracujeme s príliš veľkým rizikom, to vzniká až v neskoršej fáze, pri implementácii a nasadení.

V IT projektoch väčšinou nevieme, či:

- Softwarový balík pokrýva dostatočne zadanú obchodnú činnosť - je potom potrebná modifikácia balíkov.
- Integrácia medzi novým a starým systémom je uskutočnená včas.
- Testovanie neukáže nepríjemné prekvapenia.
- Sú užívatelia prispôsobiví k zmenám.
- Môže tréning vyvolať prekážky.

Rovnaké problémy platia pre udržiavanie a vylepšovanie IT projektov. Napríklad, ak programátor dostane za úlohu urobiť malú zmenu v systéme, ohodnotí časové požiadavky na dva týždne. Po uplynutí tejto doby však programátor zistí, že zmena nebola triviálna, ako sa a prvý pohľad zdalo a práca mu zaberie ešte viac času. Prípadne môže programátor pracovať na prioritnejších úlohách a k riešeniu zadanej zmeny sa nedostane.

Riziká v IT systémoch sa často objavujú v neskorších fázach projektu predovšetkým kvôli neprispôsobivosti užívateľov a vývojárov k zmenám, konverzií dát, testovaniu a integrácii. Pokiaľ si však projektoví manažéri a vývojári včas uvedomia, v čom spočívajú hlavné problémy, budú mať väčšiu možnosť presunúť tieto riziká a problémy do skoršej fázy práce projektu. Situácia je taká istá pri testovaní - čím skôr chybu objavíme, tým viac času máme na jej opravu.

Sledovanie statusu problémov a rizík

Cieľom je, aby bol projektový manažér schopný sledovať problémy, množstvo odhaleného rizika a množstvo práce zamerané na odstránenie zvyšných rizík. Metódy merania sú nasledujúce:

- **Aký starý je najstarší nevyriešený hlavný problém.** Každý problém má čas svojho vzniku. Najčastejšie ostávajú najstaršie a najdôležitejšie problémy naďalej nevyriešené, čo patrí k tým najhorším situáciám, ktorá môže pri vývoji projektu nastať. Dôsledkom je predovšetkým to, že tímy musia predpokladať určitý výsledok tak, aby sa v práci mohlo aj ďalej pokračovať. Niekedy nie je výsledkom riešenia problému to, čo sa a jeho začiatku predpokladalo, čo môže negatívne ovplyvniť časový plán projektu.
- **Metóda riadenia dosiahnutej hodnoty projektu - EVM** (Earned Value Management) posudzuje časový postup projektu vo väzbe na vynaložené náklady a zároveň manažérovi umožní odhad zvyšných nákladov. V prípade, že je správne používaná, tak zavčas varuje pred problémami vo fáze realizácie projektu.
- **Cenu rizík** získame až porovnáme počet hodín s hotovými úlohami, v ktorých bolo riešenie rizík a problémov už vykalkulované. Získame tak približnú hodnotu toho, koľko nás budú stáť zvyšné riziká.
- **Rozdelenie problémov a rizík v čase.** Každá časová perióda (mesiac, týždeň, ...) má konečný počet hodín práce. V tejto časovej perióde je menší počet hodín spojený s rizikom. Môžeme tak nastaviť riziká na časové periódy [13].

2.3.3 Použitie rizikového riadenia v projektoch

Integrované riadenie rizík má dve kľúčové charakteristiky

1. Rozhodovanie v projektovom riadení je vykonávané s porozumením rizík, ktoré sú súčasťou daných procesov. Toto porozumenie obsahuje plný rozsah aktivít vykonávaných pri projektovom riadení ako sú definícia rozsahu, princípy a financovanie projektu, finančné riadenie, plánovanie, získavanie prostriedkov, riadenie kvality, kontrola zmien, preskúvanie výsledkov a ďalšie. Tieto aktivity musia byť plne ovplyvnené rizikovým riadením, vďaka čomu získame rizikovo založený plán projektu.
2. Proces rizikového riadenia musí byť integrovaný s ostatnými procesmi v oblasti riadenia. To ovplyvňuje okrem projektových postupov zároveň projektové nástroje a celú infraštruktúru.

Riadenie aktívnych hrozieb a príležitostí

Pokiaľ chceme efektívne využívať riadenie rizík, je potrebné správne definovať jednotlivé procesy, zaistiť existenciu správnych nástrojov a techník, a taktiež zaistiť dostatok príležitostí k tréningu. Tieto kroky ako jednotlivé nestačia. Problém je veľakrát v tom, že väčšina manažérov, ktorí riadia veľké projekty nevie správne využívať rizikové riadenie. Cieľom rizikového riadenia v projektoch je vytvorenie jednoduchého, ľahko nastaviteľného a dobre zdokumentovateľného procesu, ktorý odstráni alebo minimalizuje prekážky pri práci na projekte.

Najskôr je potrebné stanoviť, čo bude takýto jednoduchý a ľahko nastaviteľný proces pokrývať:

- Pokiaľ je riziko definované ako akákoľvek neistota, ktorá pokiaľ sa objaví má pozitívny alebo negatívny efekt na dosiahnutie jedného alebo viacerých cieľov, tak prvým krokom rizikového riadenia je zaistenie, aby boli riziká správne definované a pochopiteľné. Ciele efektívneho riadenia môžu byť definované mimo proces rizikového riadenia, ale toto riadenie sa bez nich nemôže začať. Pokiaľ teda v projektovom riadení chýbajú, musí ich proces riadenia rizík vygenerovať.
- Po definovaní cieľov môže dochádzať k ovplyvneniu procesu stanovenia neistôt. Potenciálne škodlivé neistoty (hrozby) musia byť identifikované rovnako ako tie, ktoré by pomohli v projekte v dosiahnutí stanovených cieľov.
- Nie je však nutné identifikovať všetky neistoty. Proces rizikového riadenia musí obsahovať časť, ktorá bude vyberať, triediť a nastavovať priority rizikám tak, aby boli nájdené najväčšie hrozby a najlepšie príležitosti. Ďalej je veľmi užitočné skúmať jednotlivé skupiny rizík, či obsahujú niektoré významné znaky alebo koncentráciu určitých rizík. Užitočné je tiež stanovenie celkového dopadu všetkých nájdených rizík na finálny výsledok projektu.
- Po identifikácii a nastavení priority rizikám prechádzame z analýzy ku konkrétnej akcii. V tejto časti rizikového riadenia sa obracia pozornosť k rozhodovaniu ako vhodne zareagovať na konkrétne hrozby a príležitosti, a zároveň ako sa vysporiadať s celkovým rizikom projektu. Existuje celá rada scenárov ako rizikám čeliť.
- Reakcia na riziká väčšinou nie je dostatočná, aby pokryla všetky aktuálne riziká. V procese často chýba okamžitá reakcia na nájdené riziká. Plánované reakcie musia

byť implementované v správnom poradí tak, aby zmenili odhalenie rizika v projekte. Výsledky týchto odhalení musia byť sledované tak, aby zaistili požadovaný efekt.

- Tieto kroky rizikového riadenia môžu byť vykonávané iba niekoľkými členmi projektového tímu, ale výsledky sú dôležité pre všetkých členov tímu. Preto je nevyhnutné o rozhodnutiach informovať všetkých členov tímu.
- Analýza rizík je v každom projekte premenlivá a jeho výsledok musí kontinuálne a opakovane posudzovať riziká k zaisteniu vhodnej reakcie, ktorá bude prebiehať v priebehu celej fázy práce na projekte.
- Plne efektívny rizikový proces v tomto bode nekončí, pretože organizácia sa musí poučiť a získavať ďalšie skúsenosti pre svoje budúce projekty. Klasické zhrnutie po ukončení projektu musí obsahovať rizikovo zamerané elementy, vďaka čomu budú hrozby v budúcnosti obmedzené na minimum a zistené príležitosti dotiahnuté k vyššej efektívnosti.

Metóda riadenia aktívnych hrozieb a príležitostí

Metóda ATOM (Active Threat and Opportunity Management) definuje, že každý projekt by mal obsahovať 8 nasledujúcich krokov:

1. Definícia cieľov.
2. Identifikácia relevantných neistôt.
3. Nastavenie priorít pre jednotlivé neistoty.
4. Vypracovanie vhodných riešení.
5. Oznámenie výsledkov zainteresovaným stranám.
6. Implementácia dohodnutých akcií.
7. Sledovanie zmien.
8. Získavanie skúseností pre ďalšie projekty.

Metóda pre riadenie aktívnych hrozieb a príležitostí je navrhnutá tak, aby pokryla potreby jednoduchého škálovateľného procesu riadenia rizík tak, aby bola aplikovateľná na všetky typy projektov. Táto metóda prináša spojenie osvedčených postupov, vyskúšaných a otestovaných metód, nástrojov a techník, ktoré sú skombinované tak, aby boli ľahko použiteľné v praxi riadenia rizík projektov.

Metóda ATOM sa skladá z 8 krokov:

1. Zahájenie.
2. Identifikácia.
3. Posúdenie.
4. Plánovanie reakcií.
5. Reportovanie.

6. Implementovanie.
7. Preskúmanie.
8. Poprojektové preskúmanie.

Posúdenie obsahuje kvantitatívnu rizikovú analýzu k zaisteniu dopadu jednotlivých rizík na celkový projekt.

Riziká sa väčšinou neobjavia hneď na začiatku projektu a potom nezmiznú. Metóda ATOM vyžaduje používanie všetkých jej krokov po celú dobu životného cyklu projektu [11].

Riadenie projektov

Pri riadení projektov dávame dôraz na niekoľko atribútov, ktoré priamo či nepriamo ovplyvňujú riziká. Jedným z atribútov je **projektová viditeľnosť**, ktorá odkazuje na prostriedky, prostredníctvom ktorých môže vedenie sledovať v akej fáze sa jednotlivé projekty nachádzajú. Riziká ovplyvňujú všetky typy projektov, najviac však tie, ktoré sú zamerané na vývoj software. Projekty s abstraktnou prácou a nehmotnými výsledkami sú čiastočne voči rizikám bezbranné. Projektová viditeľnosť je v projektoch pre redukciu rizík dôležitá. Vyspelosť všetkých zainteresovaných procesov zlepšuje celkovú viditeľnosť, a tým minimalizuje riziká.

Ďalším atribútom je **nastavenie cieľa**. Každý cieľ je totiž zatienený rizikom. Ak definujeme ciele, musíme tieto riziká rozpoznať. Vnímanie rizík sa potom rozširuje, pokiaľ sú ciele v projekte jasne definované. Naopak hľadanie príležitostí, ktoré ostatní opomínali znamená pokrývanie rizík, ktoré ostatní nepokryli.

Medzi atribúty patrí aj **vývoj produktu**. Spoločnosti, ktoré vyvíjali produkty, majú často k rizikám paranoidný prístup. Investície do vývoja sú veľké a niekoľko rizík ohrozuje produkt ešte pred jeho vstupom na trh. Produkty môžu byť taktiež znehodnotené pred samotným uvoľnením na trh, pretože dopyt môže klesnúť na minimum. Riziká preto musia byť starostlivo preskúmané pri každom kroku vývojového procesu.

Hlavnou úlohou **procesu riadenia rizík** je skúmanie cieľov a benefitov- hlavným cieľom je redukcia dopadov jednotlivých rizík. Cieľom väčšinou nie je riziká eliminovať, ale čo najviac znížiť straty vzniknuté pri ich výskyte. Riadenie rizík používa pre dosiahnutie cieľov stratégie a plánovanie. Jedná sa teda o systematický prístup k redukcii dopadov rizík s cieľom vytvárať projekty menej zraniteľné a viac robustné [11, 15].

Výhody rizikového riadenia môžeme rozdeliť do dvoch kategórií. **Primárne-priame-výhody** sú nasledujúce:

- Dosiahnutie cieľov.
- Projekt je zbavený hlavných rizík.
- Projekt je zbavený zraniteľných oblastí.
- Ľudia sú pripravení riešiť problémy.
- Produkt je spoľahlivejší.
- Odpadajú následky nízkej kvality.
- Nie je využívaný náhodný a nesystematický postup.

Medzi **sekundárne- nepriame-** výhody spadá veľa oblastí, ktoré vychádzajú z výhod priamych. Napríklad:

- Vylepšené definovanie cieľov.
- Alternatívne prístupy pri riešení problémov.
- Pragmatické rozhodovanie.
- Procesná optimalizácia.
- A ďalšie ...

Kapitola 3

Metódy analýzy rizík

Táto kapitola rozoberá teóriu využívanú pre analýzu rizík. Ďalej táto kapitola popisuje metódy, ktoré sa najčastejšie používajú pri analýze rizík a to konkrétne metódy ETA, FTA, HAZOP a FMEA. Metóda ETA je skratka pre Event Tree Analysis, čo v preklade znamená Analýza Stromom Udalostí, v texte je prezentovaná skratkou ETA. Metóda FTA je skratka pre Fault Tree Analysis, čo v preklade znamená analýza stromom porúch, v texte prezentovaná skratkou FTA. FMEA je skratka pre Failure Mode and Effects Analysis, čo v preklade znamená analýza možných výskytov a vplyvov väd, v texte je preprezentovaná skratkou FMEA. Poslednou z vymenovaných metód je HAZOP. Je to skratka pre Hazzard and Operability study, čo v preklade znamená analýza ohrozenia a prevádzkyschopnosti, v texte je reprezentovaná skratkou HAZOP.

3.1 Rozhodovacie modely

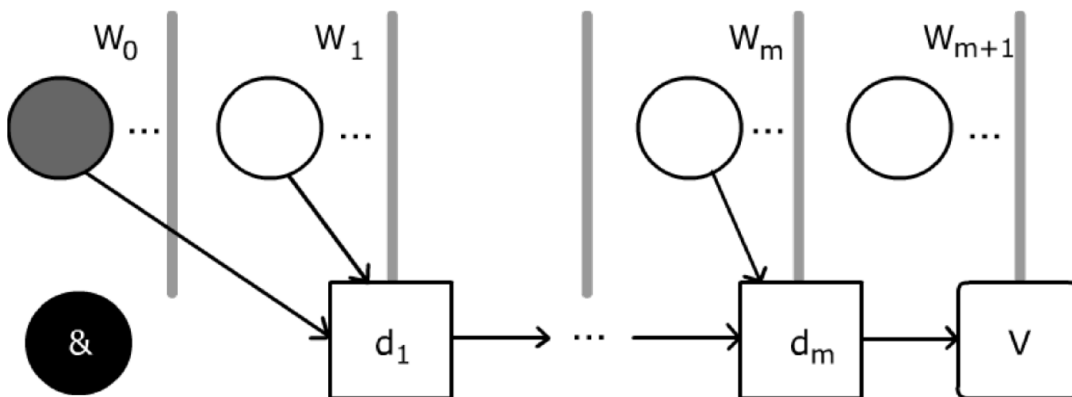
V tejto časti sú popísané príklady rozhodovacích modelov reprezentovaných pomocou diagramu vplyvu. Diagramy vplyvu vyjadrujú možnosti a preferencie rovnako ako informácie. Skladajú sa zo sietí s ďalšími dvoma typmi uzlov reprezentujúcich rozhodnutia a kritériá pre rozhodovanie. Diagram vplyvu reprezentuje perspektívne sledovanie premenných, ktoré sú stále neisté. Z diagramu vplyvu vychádzajú (dajú sa z neho transformovať) rozhodovacie stromy, preto je nutné objasniť najskôr terminológiu tvorby a úpravy diagramu vplyvu.

Štruktúra diagramu vplyvu je zložená z uzlov, oblúkov a logických AND operátorov. Rozhodovacie uzly D korešpondujú s premennými, ktoré sú kompletne pod kontrolou rozhodovacieho modelu a hodnota uzlu V reprezentuje kritériá, ktoré sa používajú pre rozhodnutia.

Diagram vplyvu je kompletne špecifikovaný, pokiaľ sú prípustné hodnoty priradené každému uzlu a podmienené rozloženie pravdepodobnosti priradené pre každý uzol U a V. Hodnoty premennej V sú predpokladané ako deterministické funkcie ich predkov rovnako ako premenné F (neistoty) a predpokladáme, že celková hodnota je súčet všetkých hodnôt funkcií. Rozloženie podmienené pravdepodobnosťou nie je potrebné pre rozhodovacie uzly D- tieto budú určené ako maximalizácia očakávanej celkovej hodnoty.

Očakávame, že všetky rozhodovacie premenné môžu byť zoradené v čase d_1, d_2, \dots, d_m a predchodcovia každej z nich reprezentujú všetky ostatné premenné, ktoré boli stanovené predtým ako bolo rozhodnuté. Predpokladáme, že tu nie je žiadny zabudnutý stav, ktorého predchodcovia každého rozhodnutia obsahujú skoršie rozhodnutie a premenné stanovené predtým. Ako výsledok môžeme rozdeliť neistoty na $m + 2$ stavov, rozhodovacie

okná W_0, W_1, \dots, W_{m+1} , kde premenné neistôt vo W_0 už boli vykonané, tie vo W_1 budú vykonané pred rozhodnutím d_i , ale až po rozhodnutí d_{i-1} a tie vo W_{m+1} nebudú vykonané pred žiadnym rozhodnutím tak ako je naznačené na obrázku 3.1. Okná môžu byť myslené



Obr. 3.1: Rozhodovacie okna [8, 15]

ako jednosmerná cesta, takže budúce rozhodnutia môžu uskutočniť čokoľvek, čo sa nachádzalo v predchádzajúcich oknách, ale nič, čo sa nachádza v budúcich oknách. Formálny zápis je nasledujúci:

$$P_a(d_1) = W_0 \cup aP_a(d_i) = P_a(d_{i-1}) \cup W_i \quad \text{pre } i = 2, \dots, m. \quad (3.1)$$

Sieť sa nazýva *bežnou sieťou*, pokiaľ sú rozhodovacie modely kompletne kontrolovateľné jednou alebo viacerými premennými neistôt, diagram vplyvov získame odrezaním prichádzajúcich oblúkov z predchodcov ich premenou na rozhodovací uzol.

Klasický model rozhodovania v priebehu času je Markovov rozhodovací proces reprezentovaný diagramom vplyvov ukázaný na obrázku 3.2. Je na ňom viacej priebehov, obvykle myslených ako udalosti v čase $t, t+1, \dots$ a každý priebeh je tu stavom procesu - akcií k výberu a postihom/odmenou za túto udalosť. Stav pre ďalšiu udalosť je ovplyvnený súčasným stavom, súčasnou akciou a nasledujúcim stavom. Je dobre známe, že i pokiaľ všetky stavy a rozhodnutia v minulosti sú vykonané v prítomnom čase, súčasný stav obsahuje všetky informácie z minulosti a súčasnosti potrebné k ohodnoteniu a vykonaniu rozhodnutí v prítomnom a budúcim čase [8, 15].

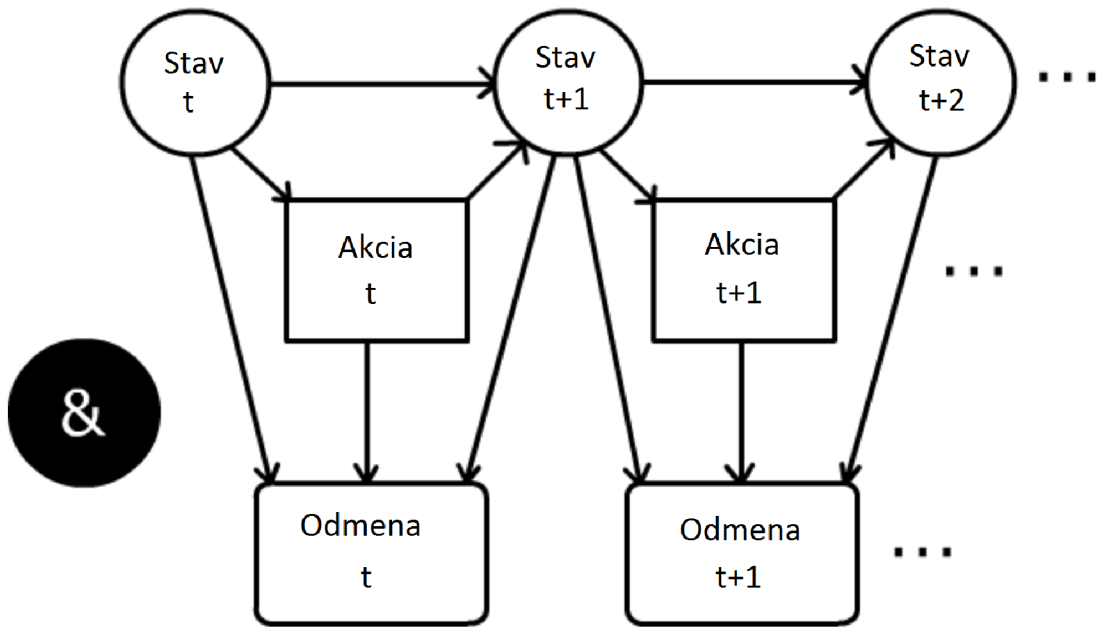
Analýza rozhodovacích modelov

Existuje priame rozšírenie *Bayes-Ball algoritmov* pre rozhodnutia, ktoré skúma štrukturovaný diagram vplyvov k určaniu predpokladaného pozorovania pre každé rozhodnutie. Prechádzaním každého rozhodovacieho uzlu d_i v spätnom chronologickom poradí $i = m, \dots, 1$ a zmenou d_i na deterministické uzly s predchodcami dostaneme:

$$P_a(i) = N^E(V \cap D_e(d_i) \mid d_i \cup P_A(d_i)) \quad (3.2)$$

Na tomto mieste je predpokladané pozorovanie k určaniu celkovej hodnoty dané ako $N^E(V \mid W_0)$.

Ako príklad Bayes-Ball algoritmu pre rozhodovanie si predstavme situácie, kde historické dáta a nové experimentálne dôkazy o nových stavoch neistôt sú dostupné rozhodovacím modelom pri rozhodovaní. Je tu cena dôkazu a benefit založený na voľbe stavu. Diagram



Obr. 3.2: Markovov rozhodovací proces [8, 15]

vplyvu pre túto situáciu je znázornený na obrázku 3.3 Bayes-Ball algoritmus pobeží na rozhodnutí *Úkon*, *Návrh* a situáciách pred rozhodnutím *Návrh* v diagramoch B,C,D. V tejto situácii sú všetky premenné nutné.

Rovnaká rozhodovacia situácia v *Stav* pred *Úkon* je reprezentovaná diagramom vplyvu na obrázku 3.3 a Bayes-Ball diagram je ukázaný na obrázku 3.3 diagramy F,G, H. Teraz tu sú iba potrebné informácie k vytvorenej optimálnej voľby hodnoty funkcií a *Stav* pozorovania. Oveľa viac informácií je potrebných k ohodnoteniu tohto rozhodnutia - v takomto prípade je iba premenná *Experiment* vynechateľná.

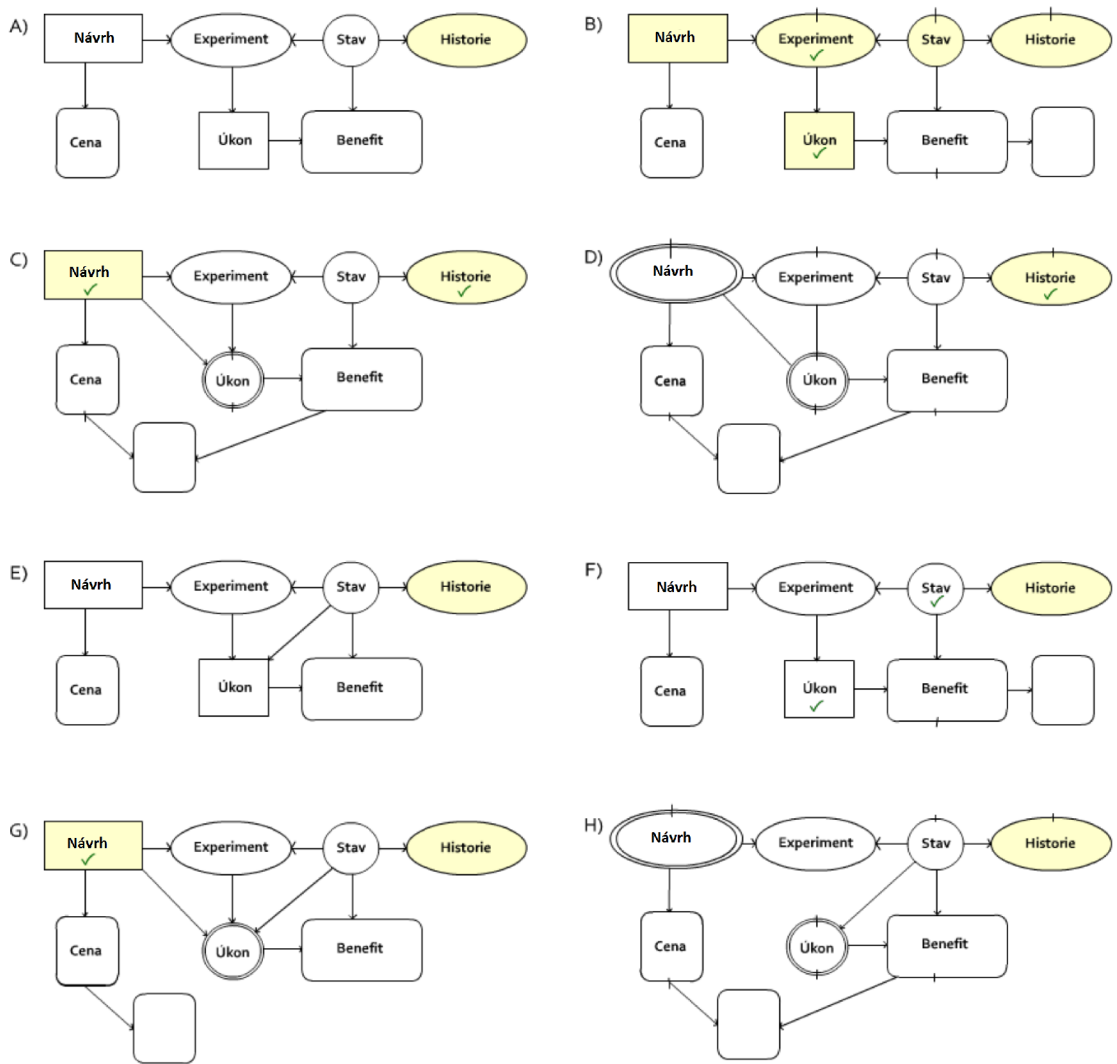
Úlohou analyzovania diagramu vplyvov je určenie optimálnych podmienok a hodnotenie rozhodovacích situácií, ktoré môžeme dosiahnuť grafickými operáciami na diagrame, ktoré zmenia poradie zoznamu a postupne odstránia uzly z diagramu. Diagram je redukovaný, pokiaľ všetky zostávajúce uzly sú samostatné ohodnotené uzly a vďaka tomu môžeme ohodnotiť rozhodovaciu situáciu.

Najjednoduchšie transformácie, odstránenie nerozvíjajúcich sa uzlov. Môže byť použitá kedykoľvek, pokiaľ rozhodnutie alebo nerozvíjaný uzol neistoty nemá ďalších potomkov - v tomto bode môže byť jednoducho zmazaný z diagramu, pokiaľ to nebude mať dopad na celkovú hodnotu. Nutné sady predchodcov pre rozhodovanie vypočítané Bayes-Ballom môžu byť taktiež využité k zjednodušeniu problému elimináciou niektorých predchodcov rozhodnutí.

Pre redukciiu diagramu potrebujeme 3 grafické transformácie - jedna k odstráneniu rozhodovacích uzlov, jedna k odstráneniu uzlov s neistotami a jedna k odstráneniu ohodnotených premenných. Pokým rozhodovací uzol *i* má iba jedného potomka, hodnotový uzol a všetci predchodcovia hodnotového uzlu sú taktiež predchodcovia rozhodovacieho uzlu.

$$P_a(i) \supseteq P_a(j) - i \quad (3.3)$$

Potom optimálne určenie volieb nahradí rozhodovaciu premennú na deterministickú premennú ako je ukázané na obrázku 3.4 bod a). Nová rozhodovacia funkcia pre uzol *i* je



Obr. 3.3: Bayes-Ball algoritmus pre rozhodovanie [8, 15]

daná:

$$F_i(x_K | AA = \arg \max_{x_i \in \Omega_j} f_j(x_i, x_F)) \quad \text{pre všetky } x_k \in \Omega_K, \quad (3.4)$$

kde $K = P_a(i) \cap P_a(j) = P_a(j) - \{i\}$. Voľba x_i môže byť ľubovoľná, pokiaľ tu sú väzby. Táto optimálna voľba môže byť zaznamenávaná pred vlastným zmazaním. Pamätajte si, že akýkoľvek predchodca i , ktorý nie je predchodcom j , je integrovaný výberom optimálnej stratégie a nemusí byť stále rozvíjaný. Ostatní predchodcovia i danej K sú nutní k prechádzaniu pre i .

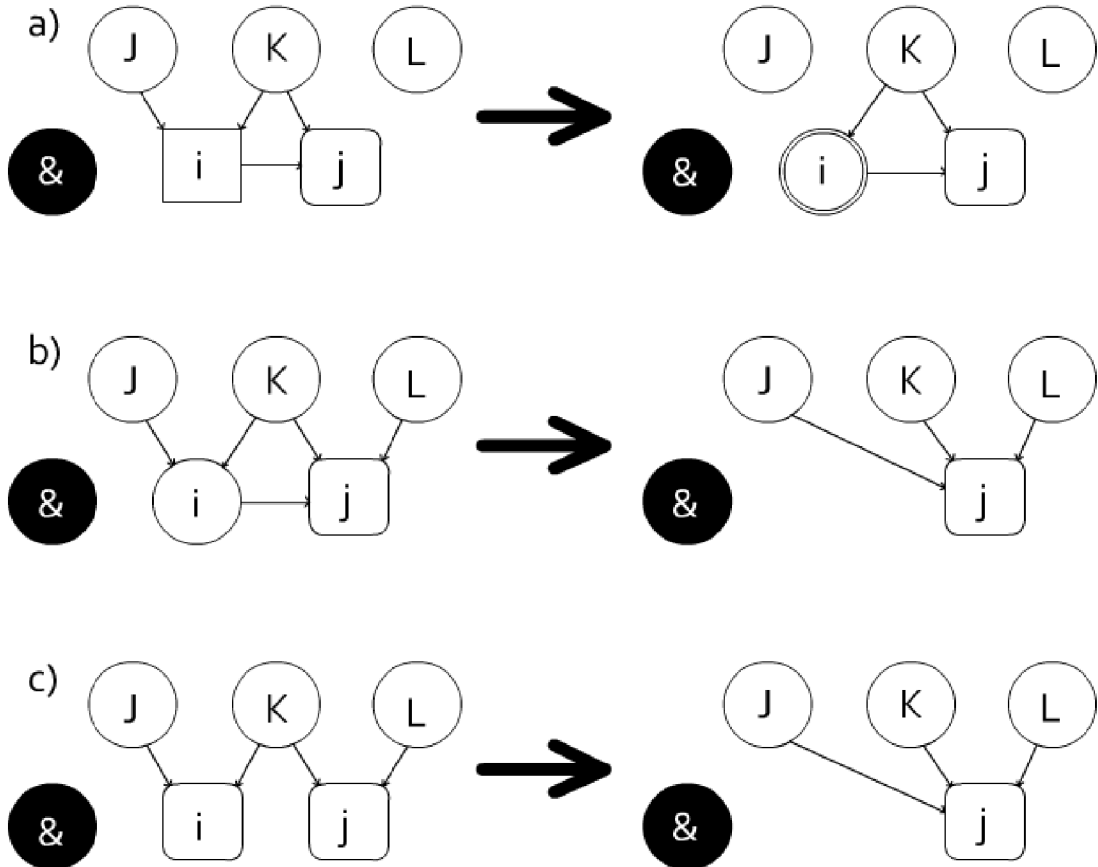
Pokiaľ uzol neistoty i má iba jedného potomka - hodnotový uzol j , potom odstránenie uzlu neistôt odstraňuje uzol i z diagramu, ako je ukázané na obrázku 3.4 bod b). Nová funkcia pre tento uzol j je daná:

$$f_j(X_J, X_K, X_L | AA) = \sum_{x_i \in \Omega_j} P\{x_i | X_J, X_K, AA\} F_j(x_i, X_K, X_L), \quad (3.5)$$

kde $J = P_a(i) - P_a(j)$, $K = P_a(i) \cap P_a(j)$ a $L = P_a(j) - (i \cap P_a(i))$. Podobne, pokiaľ je tu viacero hodnotových uzlov i a j , hodnotový uzol odstránime odstránením uzlu i nahradením

funkcie v uzle j s ich súčtom - ako je naznačené na obrázku 3.4. Nová funkcia uzlu je daná:

$$f_j(X_J, X_K, X_L | AA) = f_i(X_J, X_K) + F_j(X_K, X_L). \quad (3.6)$$



Obr. 3.4: Operácie v diagrame vplyvov slúžiaci k odstraneniu uzlov [8, 15]

Pokým máme k dispozícii tieto operácie, môžeme diagram vplyvov s nepriamymi cyklami (bez zabudnutých stavov a pri zoradenom rozhodovaní) vyriešiť pomocou nasledujúceho algoritmu:

1. Pokým tu je hodnotový uzol bez potomkov, zmeň ich na uzol neistoty a daj mu hodnotový uzol ako potomka s hodnotou rovnakou ako je on samotný.
2. Pokiaľ sa tu nachádzajú ostávajúce uzly okrem tých vo V alebo W_0 , tak:
 - (a) Pokým sa tu nerozvíjal uzol, odstráň ho.
 - (b) Inak, pokým sú podmienky uspokojivé k odstráneniu posledného rozhodnutia, potom určí optimálnu stratégiu.
 - (c) Inak, pokým uzol nebol preskúmaný pred posledným rozhodnutím a má najviac jednu hodnotu potomka, potom ho odstráň po obrátení určitých oblúkov k ich nehodnotným potomkom v poradí.

- (d) Inak, hodnotový uzol potrebuje byť odstránený, najlepšie potomkom posledného rozhodovania.

Veľa ľudí používa diagramy vplyvov ku konštrukcii rozhodovacích modelov, avšak preferujú skôr riešenie pomocou rozhodovacieho stromu. Konverzia na rozhodovacie stromy je priama, pokiaľ sa tu nenachádzajú žiadne nesequenčné oblúky. Oblúk nazývame nesequenčným, pokiaľ ide z uzla neistoty v oneskorenom rozhodovacom okne k prvku v skoršom rozhodovacom okne [8, 15].

Rozhodovacie stromy

Analýza pomocou rozhodovacích stromov je štandardná výpočtová metóda v rozhodovacej analýze. Rozhodovacie stromy sú flexibilné pri vyjadrovaní logiky komplexného rozhodnutia.

Majme databázu $D = \vec{t}_1, \dots, \vec{t}_n$, kde $\vec{t}_i = (t_{i1}, \dots, t_{in})$. Ďalej majme atribúty $\{A_1, \dots, A_n\}$ a množinu tried $C = \{C_1, \dots, C_m\}$. **Rozhodovací strom** pre D je strom, kde:

- Každý vnútorný uzol je ohodnotený atribútom A_i .
- Každá hrana je ohodnotená predikátorom použiteľných na atribút rodiča.
- Každý list je ohodnotený triedou C_j .

Rozhodovací strom je grafická reprezentácia očakávanej hodnoty výpočtu. Strom sa skladá z rozhodnutí, rizík a konečných stavov spojených vetvami. Každé rozhodnutie sa dá analyzovať pomocou analýzy rozhodovacím stromom, ktorý je vhodný pre každodenné problémy, v ktorých chce niekto vedieť najlepšiu alternatívu zo všetkých možností.

V rozhodovacom strome berieme premenné do úvahy v takom poradí, v akom sa vyskytujú na zozname udalostí a stavov. Z rozhodovacích stromov vychádzajú nasledujúce dva spôsoby analýzy rizík, naviac môžu byť využité k odhadu pravdepodobnosti nežiadúcich účinkov. Oba modely môžu byť popísané logickým ekvivalentom diagramu vplyvov a môžu byť riešené štandardnými algoritmami [8, 15].

3.1.1 FTA

Analýza FTA je deduktívna technika, ktorá sa zmeriava na jednu určitú nehodu alebo na veľké zlyhanie systému a ozrejmuje metódu pre stanovanie príčin takejto udalosti. FTA využíva grafický model, ktorý zobrazuje rôzne kombinácie porúch zariadení a ľudských chýb, ktoré môžu vyústiť do vážnej systémovej poruchy. FTA ako kvalitatívny nástroj má schopnosť identifikovať kombinácie základných porúch zariadení a ľudských chýb, ktoré môžu viesť k nehode. To analytikovi umožňuje zamerať sa na preventívne alebo zmierňujúce opatrenia, tak aby znížili pravdepodobnosť vzniku nehody.

Účelom FTA je nájsť kombináciu porúch zariadení a ľudských chýb, ktoré môžu vyústiť v nehodu. FTA je vhodná pre veľmi zložité a komplikované systémy.

FTA vytvára logické modely porúch systému. Tieto modely používajú booleovských logických hradiel pre popis spôsobu, ako môžu byť zlyhania skombinované, aby zapríčinili veľkú systémovú poruchu. Analytik obvykle rieši každý logický model, aby vytvoril zoznam porúch nazývaný minimálne kritické rezy, ktoré môžu vyvrcholiť vo vrcholovú udalosť. Kontrola takýchto zoznamov odhaľuje slabiny projektu alebo prevádzkového systému. Pre tieto systémy môže analytik navrhnúť alternatívy možných bezpečnostných vylepšení.

Použitie techniky FTA vyžaduje detailne porozumieť tomu, ako podnik alebo systém fungujú, detailne porozumieť nákrasom a postupom, detailne poznať spôsoby zlyhania komponent a účinok takýchto zlyhaní. Doba a náklady na prevedenie závisí na zložitosti systémov, ktorých sa analýza týka a na stupni podrobnosti tejto analýzy. Modelovanie jedinej vrcholovej udalosti jednoduchého procesu nie je časovo náročné. Zložité systémy alebo veľké problémy s množstvom potenciálnych nehodových udalostí sa modelujú i skúseným tímom analytikov niekoľko týždňov až mesiacov [10].

Postup analýzy

Základným predpokladom v FTA je binárne správanie sa všetkých porúch. To znamená, že operátor alebo komponent, buď vykoná činnosť úspešne alebo nie. Podobne sa predpokladá, že systém úspešne vykonáva svoju funkciu, ak všetky jeho komponenty pracujú. FTA neumožňuje pracovať s čiastočne degradovanými systémami. Časové predĺženia sa v FTA neuvažujú, aj keď sú časté pri reálnych udalostiach.

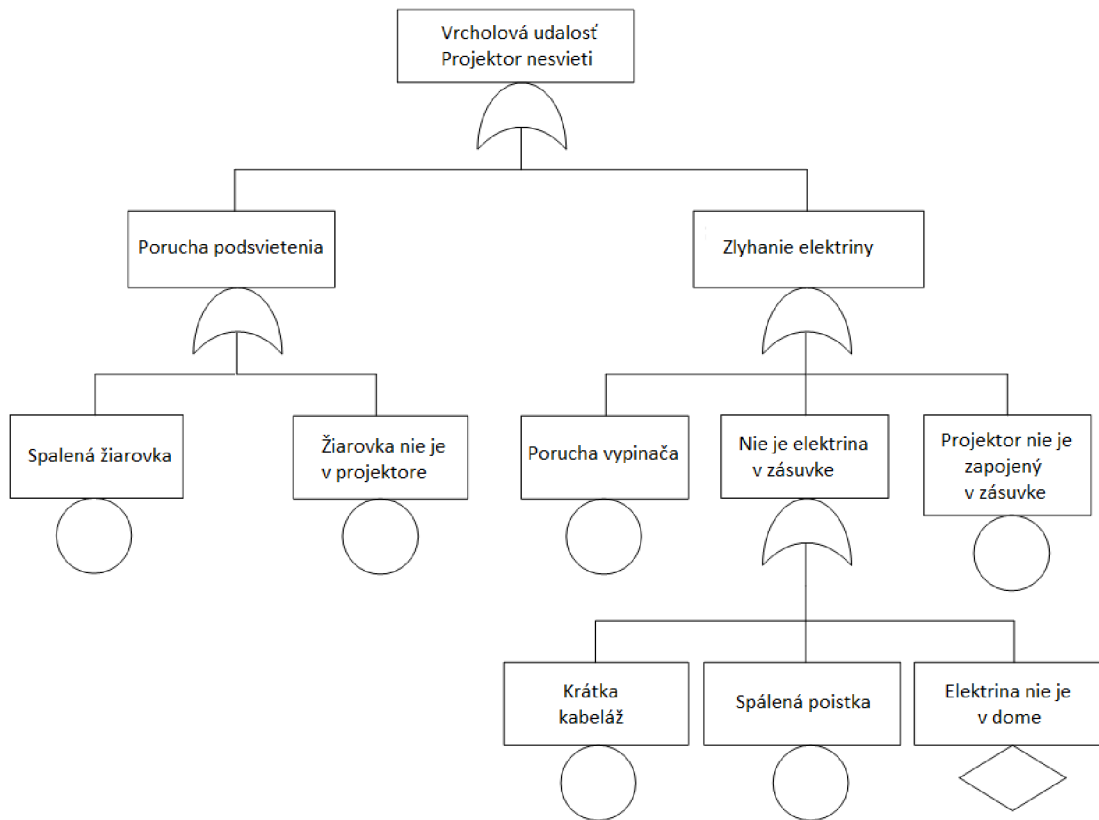
Súčasná technika FTA používa kombináciu relatívne jednoduchých logických hradiel (zvyčajne AND a OR hradla) pre syntézu poruchového modelu určitého zariadenia. Frekvencia alebo pravdepodobnosť vrcholovej udalosti je spočítaná z poruchových dát jednoduchších udalostí.

Všeobecný postup pri aplikácii FTA v úlohách hodnotenia rizika je v jednotlivých krokoch takýto:

1. **Popis systému** - v tomto kroku ide o to pochopiť činnosti systému, do ktorých môžeme zaradiť napríklad umiestnenie prevádzky, popis procesov, prevádzkové podmienky a diagramy, plány zariadení, základne vlastností a iné.
2. **Odhalenie zdrojov rizika** - v tomto kroku sa určujú vrcholové udalosti, ktoré vychádzajú z historických záznamov, skúseností, HAZOP, FMEA.
3. **Konštrukcia stromu porúch** - v tomto kroku sa vyvíja logika porúch, využívajú sa hradlá AND a OR a pokračuje sa dolu k základným udalostiam, príklad je na obrázku 3.5.
4. **Kvalitatívny prieskum štruktúry** - v tomto kroku sa robí analýza minimálnych kritických rezov, pracuje sa na porozumení všetkých poruchových módoch, kvalitatívne sa zaradzuje importancie, skúma sa citlivosť k poruchám so spoločnou príčinou.
5. **Kvantitatívne vyhodnotenie stromu porúch** - v tomto kroku sa skúma frekvencia výskytu vrcholových udalostí s využitím booleovského prístupu alebo prístupu hradloza-hradlom.

Krok 1 a krok 2 patria do všeobecného postupu analýzy rizík, zatiaľ, čo kroky 3 až 5 sú špecifické pre FTA [10].

Krok 3 – Konštrukcia stromu porúch Strom porúch je logický diagram, ktorý ukazuje, ako môže systém zlyhať. Zvyčajne sa postupuje zhora dole. Za vrcholovú udalosť je zvolená nežiadúca udalosť. Pri vrcholovej udalosti sa identifikujú nevyhnutné a dostačujúce príčiny spolu s ich logickými vzťahmi. Aby toho analytik dosiahol, pýta sa otázku ako „Ako sa to mohlo stať?“ alebo „Aké sú príčiny tejto udalosti“. Tento proces deduktívneho uvažovania pokračuje, dokým si analytik myslí, že nenašiel dostatočnú presnosť, aby to stačilo pre neskoršie pridelovanie pravdepodobnosti základným udalostiam.



Obr. 3.5: Príklad FTA, stromu porúch [10].


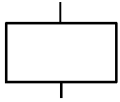
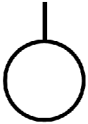
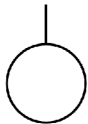
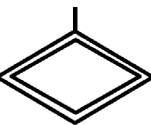
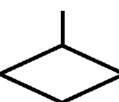
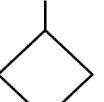
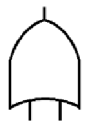
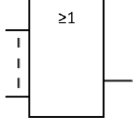
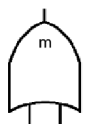
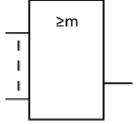
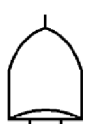
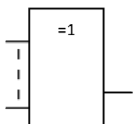
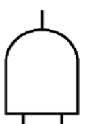
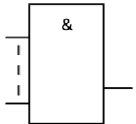
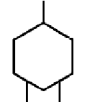
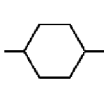
V technickej praxi sa často používajú symboly, ktoré vychádzajú z noriem (viď obrázok 3.6). V rozsiahlych stromoch porúch je bežné označovať každé logické hradlo a základnú udalosť jedinečnými identifikátormi. Toto označenie je potom používané ako logické vstupy počítačových programov pre výpočet frekvencie vrcholovej udalosti.

Je nutné podotknúť, že ručne robené stromy porúch môžu byť neúplné, kvôli vlastnej subjektivite. Avšak umožňujú získať úplnú analytickú predstavu a porozumenie systému a poruchových módov. Ručná konštrukcia stromu porúch je najpoužívanejší prístup [10].

Krok 4 – Kvalitatívny prieskum štruktúry stromu porúch Akonáhle je strom porúch zostrojený, môže byť kvalitatívne vyšetrený pre porozumenie mechanizmov porúch. Táto informácia je cenná preto, že vnáša jasno do možných poruchových modulov, tj. do všetkých kombinácií udalostí, ktoré vedú k vrcholovej udalosti. Tento postup je známy ako analýza minimálnych kritických rezov.

Jednoduché stromy udalostí pozostávajúce len z niekoľkých hradiel môžu byť preskúmané len dôkladnou prehliadkou. U zložitejších stromov musíme použiť metodicky presnejšie prostriedky ako je booleovská analýza. Strom porúch môže byť prevedený na ekvivalentnejší booleovský výraz definujúci vrcholovú udalosť ako kombináciu všetkých nižších udalostí. Tento výraz sa obvykle rozvíja pomocou zákonov Booleovej algebry, pokiaľ nevyjadruje vrcholovú udalosť ako súčet všetkých minimálnych kritických rezov.

Kvalitatívna dôležitosť - hlavne poradie rady základných udalostí vo všetkých poruchových skupinách- môže byť stanovená z minimálnych kritických rezov. Kritické rezy sú

Značky		Názov	Popis
		Komentár	Blok s názvom alebo popisom udalosti, prípadne s uvedením pravdepodobnosti výskytu (ak sa to požaduje).
		BASIC Event (Základná udalosť)	Udalosť na najnižšej úrovni, pre ktorú sú k dispozícii pravdepodobnosti výskytu alebo informácie o bezporuchovost.
		DORMANT Event (Neaktívna udalosť)	Primárna udalosť, ktorá reprezentuje neaktívnu poruchu udalostí, ktorá nie je bezprostredne detekovaná, ale ktorá by možno bola detekovaná pri dodatočnej kontrole alebo analýze.
		UNDEVELOPED Event (Nerozvíjajúca sa udalosť)	Primárna udalosť, ktorá reprezentuje časť systému, ktorá nebola doteraz rozvíjaná.
		Hradlo OR (Alebo, logický súčet)	Výstupná udalosť nastane, ak nastane akákoľvek zo vstupných udalostí.
		Hradlo MAJORITY VOTE (Majoritné hradlo)	Výstupná udalosť nastane, ak nastane m alebo viac vstupných udalostí z celkového počtu n vstupných udalostí.
		Hradlo EXCLUSIVE OR (Nonekvivalencia, vzájomné vylúčenie)	Výstupná udalosť nastane, ak nastane jedna ale nie iná vstupná udalosť.
		Hradlo AND (A, i, logický súčin)	Výstupná udalosť nastane iba vtedy, ak nastanú všetky vstupné udalosti.
		Hradlo INHIBIT (Blokovanie)	Výstupná udalosť nastane iba vtedy, ak nastanú obe udalosti, z nich jedna je podmienková.

Obr. 3.6: Symboly často používané pri konštrukcii stromu porúch [3].

radené v poradí počtu základných udalostí, ktoré musia byť kombinované, aby výsledkom bola vrcholová udalosť. Je dokázané, že jednoduché poruchové kritické rezy (jednoduché ohrozenia) sú vysoko nežiadúce, pretože len jedna porucha (zlyhanie) môže viesť k vrcholovej udalosti, dve poruchové kritické rezy (zdvojené ohrozenie) sú lepšie atd. Avšak kvalitatívny prístup môže byť zavádzajúci. Je dosť možné, že väčšie kritické rezy budú mať väčšiu frekvenciu zlyhania, než menšie kritické rezy. Kvalitatívne zhodnotenie je požadované pre určenie najfrekvencovanejšej príčiny vrcholovej udalosti.

Samostatným problémom sú poruchy so spoločnou príčinou, kedy sa môže jednou poruchou vyjadriť niekoľko komponentov alebo systémov naraz.

Krok 5 – Kvantitatívne vyhodnotenie stromu porúch Akonáhle máme konečnú štruktúru stromu porúch a odhadnuté frekvencie pre každú základnú udalosť alebo nerozvinutú udalosť, je možné spočítať frekvenciu alebo pravdepodobnosť vrcholovej udalosti. Tento výpočet sa za normálnych okolností vykonáva použitím prístupov minimálnych kritických rezov vyjadrených booleovským výrazom diskutovaným v kroku 4.

Alternatívnym je jednoduchší prístup *hradlo-za-hradlom*, ktorý nie je vhodný pre rozsiahlejšie stromy porúch. Je náchylný k numerickej chybe pri výpočte frekvencie vrcholovej udalosti, ak má strom v rôznych vetvách opakujúce sa udalosti, ktoré sú oddelené AND hradlom.

Technika hradlo-za-zhradlom začína pri základných udalostiach stromu a pokračuje hore k vrcholovej udalosti. Pred výpočtom výstupu z hradla musia byť definované všetky vstupy do hradla. Všetky spodné hradlá musia byť spočítané pred pokračovaním do ďalšej vyššej hladiny.

Matematické vzťahy použité v technike *hradlo-za-hradlom* uvádza (viď tabuľka 3.1) Predpokladá sa, že všetky vstupy do hradiel sú štatisticky nezávislé, a že strom je koherentný, tzn. že používa len hradlá typu AND a OR pre vyjadrenie logiky porúch. Tieto matematické vzťahy môžu byť rozšírené na viac než dva vstupy (súčty pre OR hradlá a súčiny pre AND hradlá). Pokiaľ má OR hradlo niekoľko vstupov, ktoré sa sčítajú, všetky súčinnové členy sa zanedbávajú, a tým výstupný súčet bude o niečo málo vyšší (viď tabuľka 3.1). Toto zjednodušenie spôsobí pre malé pravdepodobnosti zanedbateľnú chybu a je vždy konzervatívne. Do hradla AND môže byť vnesených niekoľko pravdepodobnostných členov, ale len jedna frekvencia (viď tabuľka 3.1).

Hradlo	Plánovanie vstupu	Výpočet pre výstup
OR	$P_A \text{ OR } P_B$	$P(A \text{ OR } B) = 1 - (1-P_A) \cdot (1-P_B) = P_A + P_B - P_A \cdot P_B \approx P_A + P_B$
	$F_A \text{ OR } F_B$	$F(A \text{ OR } B) = F_A + F_B$
	$P_A \text{ OR } F_B$	Nie je dovolené
AND	$P_A \text{ AND } P_B$	$P(A \text{ AND } B) = P_A \cdot P_B$
	$F_A \text{ AND } F_B$	Neobvyklé párovanie, nutné previesť na $F_A \text{ AND } P_B$
	$F_A \text{ AND } P_B$	$F(A \text{ AND } B) = F_A \cdot P_B$

Tabuľka 3.1: Vizualizácia rizík pomocou tabuľky [10]

Po spočítaní celkového stromu porúch môže byť uskutočnených niekoľko ďalších voliteľných výpočtov pre lepšie použitie vypovedacej schopnosti metódy FTA. Takýmito výpočtami sú analýzy citlivosti, neurčitosti a dôležitosti. Citlivostná analýza sa používa pre

stanovenie citlivosti frekvencie vrcholovej udalosti k možným chybám v základných poruchových dátach. Analýza neurčitosti určuje chybové medze vrcholovej udalosti (bežne sa k tomu používajú simulácie metódou Monte Carlo). Analýza dôležitosti radí rôzne minimálne kritické rezy v poradí ich príspevkov k celkovej frekvencii zlyhania systému [10, 3].

3.1.2 ETA

ETA (event tree analysis) znamená analýza stromom udalostí. Strom udalostí ukazuje možné koncové stavy nejakej hodnoty, ktorá nasledovala po iniciačnej činnosti. Analýza stromu udalostí uvažuje odozvy bezpečnostných systémov a operátorov na iniciačnú udalosť a určuje možné koncové stavy tejto nehody. Výsledkom tejto analýzy sú scenáre nehody. Stromy udalostí sú používané pre identifikáciu rôznych nehôd, ktoré sa môžu objaviť pri zložitých procesoch. Po identifikácii týchto nehodových sekvencií môžu byť určené typické kombinácie porúch pomocou analýzy stromu porúch, ktoré vedú k týmto nehodám.

Výsledkom analýzy stromu udalostí sú modely stromu udalostí a úspechy alebo neúspechy bezpečnostných systémov, ktoré vedú ku každému definovanému koncovému stavu. Nehodové sekvencie zobrazené v strome udalostí predstavuje operátor logického AND. Teda tieto sekvencie môžu byť prevedené na formu model stromu porúch pre ďalšiu kvalitatívnu analýzu [10].

Postup analýzy

Strom udalostí je grafický logický model, ktorý identifikuje a kvantifikuje možné výsledky iniciačnej udalosti. Strom udalostí systematicky pokrýva časové sekvencie vývoja udalostí, a to buď skrz sériu činností bezpečnostného systému a zásahov operátora alebo pokiaľ sa objaví strata celistvosti, skrz radu možných koncových stavov. Následky môžu byť priame alebo nepriame.

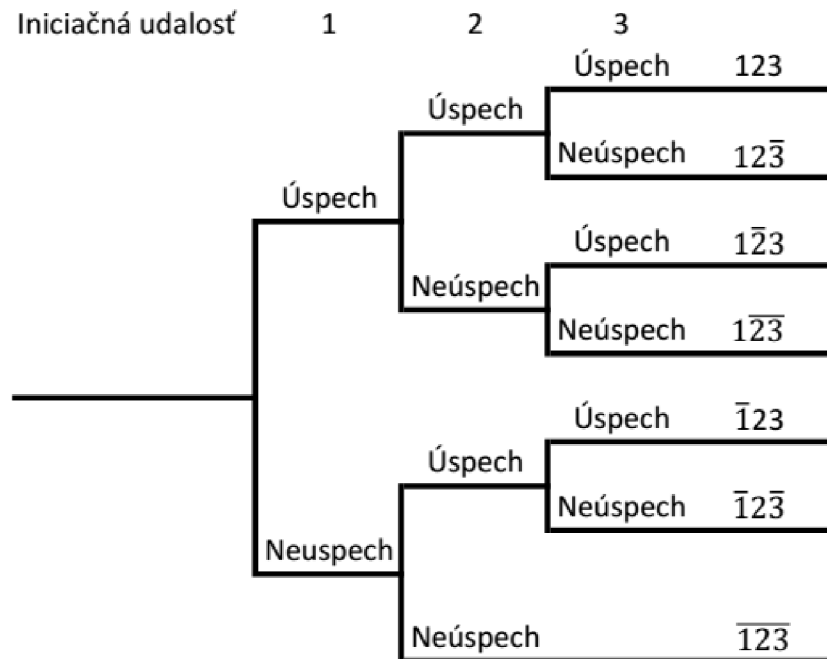
Každá udalosť nasledujúca po iniciačnej udalosti je podmienená výskytom svojej predchádzajúcej udalosti. Výsledky každej predchádzajúcej udalosti sú najčastejšie binárneho charakteru, ale môže sa jednať aj o viacej výsledkov. Rozlišujú sa 2 použitia stromov udalostí:

1. **Pred-nehodová aplikácia** sa zaoberá systémami, ktoré môžu zabrániť vzniku nehodových udalostí z predchodcov týchto udalostí.
2. **Po-nehodová aplikácia** sa používa ku zisteniu stavov nehodovej udalosti.

Stromy porúch sú často používané, aby modelovali rozvetvenie z nejakého uzla stromu udalostí, preto taktiež môže byť vrcholová udalosť stromu porúch iniciačnou udalosťou stromu udalostí. Konštrukcia stromu udalostí sa realizuje zľava doprava smerom od iniciačnej udalosti k jednotlivým prejavom postupným pridávaním všetkých dôležitých bezpečnostných funkcií alebo udalostí (viď Obrázok 3.7). Každá vetva stromu udalostí predstavuje samostatnú sekvenciu udalostí a koncový stav. Postup konštrukcie stromu udalostí je nasledujúci:

1. Rozpoznanie iniciačnej udalosti.
2. Identifikácia bezpečnostných funkcií alebo nezabezpečia podporujúceho faktory a určenia výsledku sekvencií.
3. Konštrukcia stromu udalosti do všetkých významných výsledkov sekvencií.
4. Triedenie výsledkov sekvencií do kategórií podľa podobných následkov.

5. Odhad pravdepodobnosti každej vetvy stromu udalosti.
6. Kvantifikácia výsledku sekvencií.
7. Testovanie výsledkov sekvencií.



Obr. 3.7: Ukážka stromu udalostí [10].

Bezpečnostné funkcie sú zariadenia, bariéry alebo činnosti, ktoré môžu prerušiť sekvenciu od iniciačnej udalosti po nebezpečné koncové stavy iniciačných udalostí. Nebezpečie produkujúce faktory môžu zmeniť koncový stav sekvencie. Záhlavie stromu udalosti sa používa k označeniu bezpečnostných funkcií a faktorov podporujúcich nebezpečie. Väčšina vetví je binárneho charakteru. Analytik musí v záhlaví presne vymenovať všetky možnosti, ktoré môžu ovplyvniť koncové stavy sekvencií iniciačnej udalosti. Záhlavia musia byť zoradené v časovom slede výskytu bezpečnostných funkcií a faktorov podporujúcich nebezpečie. Tak sa v záhlaví môže niekoľkokrát objaviť aj rovnaká funkcia alebo faktor v závislosti na tom, čo sa deje v čase.

Strom udalostí sa konštruuje zľava doprava od iniciačnej udalosti. U každého záhlavia či uzlu sú analyzované dve alebo viac alternatív, pokiaľ nie je získaný koncový stav sekvencie pre každý uzol. Niektoré vetvy môžu byť modelované podrobnejšie než iné. Dôležitým výstupom analýzy je zoznam bezpečných a naopak nehodových koncových stavov sekvencií, ktoré sa ďalej použijú v analýze rizika. Pokiaľ sú následky niektorej vetvy malé alebo zanedbateľné, môže zostať táto vetva nerozvinutá. V krajnom prípade sa takto môže jednať o všetky výstupy, a preto sa príslušná iniciačná udalosť ďalej neanalyzuje. Mnoho koncových stavov sekvencií rozvinutých z rôznych vetví môže byť rovnakých.

Každé záhlavie v strome udalostí (okrem iniciačnej udalosti) odpovedá podmienene pravdepodobnosti určitého výstupu za podmienky výskytu predchádzajúcich udalostí. Tak

pravdepodobnosti spojené s každým ramenom musia dávať súčet 1,0 (100%) pre každé záhlavie a musí platiť ako pre binárne tak pre viacnásobné výstupy z uzlu. Zdrojom dát podmienených pravdepodobnosťou môžu byť historické záznamy, prevádzkové dáta, chemické dáta, dáta životného prostredia, spoľahlivostné dáta zariadení, dáta o ľudskej spoľahlivosti, expertný úsudok a ďalšie.

Frekvencia každého koncového stavu sekvencie môže byť stanovená vynásobením frekvencie iniciačnej udalosti a podmienených pravdepodobností pozdĺž každej cesty vedúcej ku koncovému stavu sekvencie. Ako kontrola správnosti výpočtov slúži súčet frekvencií všetkých koncových stavov sekvencií, ktorý sa musí rovnať frekvencii iniciačnej udalosti. Predpokladom je nezávislosť medzi udalosťami a taktiež to, že sa nevyskytuje len čiastočný úspech alebo porucha [10, 6].

3.2 FMEA

Analýza FMEA je štruktúrovaná kvalitatívna analýza slúžiaca k identifikácii spôsobov porúch systému, ich príčin a dôsledkov. Jedná sa o metódu indukčnú, ktorá realizuje kvalitatívnu analýzu bezporuchovosti a bezpečnosti systému od nižších k vyšším úrovňam členenia systému a skúma, akým spôsobom môžu objekty na nižšej úrovni zlyhať a aký dôsledok môžu mať tieto zlyhania pre vyššie úrovne systému. Hlavné ciele metódy FMEA sú:

- Posúdenie dôsledkov a postupnosti javov pre každý zistený spôsob poruchy prvku, nech už má akúkoľvek príčinu a to na rôznych funkčných úrovniach systému.
- Určenie významnosti každého spôsobu poruchy vzhľadom k požadovanej funkcii alebo prevádzkyschopnosti systému s uvažovaním dôsledkov na bezporuchovosť alebo bezpečnosť daného procesu.
- Klasifikácia zistených spôsobov porúch podľa toho, ako ľahko je ich možné zistiť, diagnostikovať, testovať, nahradiť danú súčasť alebo robiť kompenzačné opatrenia, i podľa ľubovoľných iných odpovedajúcich charakteristík.
- Odhady ukazovateľov významnosti a pravdepodobnosti poruchy, ak sú k dispozícii potrebné dáta.

Najvýznamnejšie využite nachádza metóda predovšetkým v etape návrhu a vývoja, kde slúži ako súčasť preskúmania návrhu a zohráva tu rolu tzv. metódy predbežného varovania, ktorá má zabrániť neskorším problémom vyplývajúcim z nespoľahlivosti systému. Svoje uplatnenie však nachádza i v etape tvorby koncepcie a špecifikácie požiadavkou, ako nástroj predbežnej analýzy rizík a pri modifikácii a modernizácii systému alebo pri zmenách prevádzkových podmienok ako prostriedok identifikácie a posúdenia dôsledkov konštrukčných zmien a prevádzkových podmienok na bezporuchovosť. S úspechom taktiež býva táto metóda používaná pri dokazovaní, že navrhovaný systém spĺňa v oblasti bezporuchovosti a bezpečnosti požiadavky noriem, predpisov alebo užívateľov. Výsledky analýzy taktiež poskytujú nevyhnutné informácie pre racionálny návrh diagnostických postupov a systému údržby.

Široké možnosti využitia metódy sú dobre zrejmé z nasledujúceho prehľadu najvýznamnejších aplikácií a prínosu metódy:

- Systematický, presný a jednotný postup pre pochopenie funkcií systému a jeho častí.

- Identifikácia všetkých potenciálne možných porúch a určenie tých, ktoré i keď sa vyskytnú, majú diferencované dôsledky a stanovenie týchto spôsobov porúch, ktoré môžu významne ovplyvniť očakávaný alebo požadovaný prevádzku.
- Stanovenie požiadavkou na zvýšenie spoľahlivosti kritických prvkov, na zálohovaní, na vlastnosti návrhu, na zjednodušení návrhu, znížení hladín námahy.
- Stanovenie požiadaviek na alternatívne riešenie, výber prvkov, materiálu, technológií.
- Identifikácia porúch so závažnými až katastrofickými dôsledkami.
- Vyvarovanie sa neskorších nákladných modifikácií včasnou identifikáciou nedostatkov návrhu.
- Stanovenie požiadaviek na zber údajov pre vývojové, výrobné a prevádzkové skúšky.
- Ulahčenie spôsobu riešenia problémov medzi všetkými partnermi, účastníkmi kontraktu.

K tomu aby mohla byť urobená analýza systému metódou FMEA je nevyhnutné, aby boli podrobne vymedzené podmienky prevedenia a analytik mal k dispozícii všetky potrebné vstupné údaje. Ide hlavne o nasledujúce podmienky a informácie:

1. **Účel a cieľ analýzy** - musí byť presne vymedzené, k akému účelu je analýza robená. Účelom prevedenia analýzy môžu byť napríklad nasledujúce dôvody:
 - (a) Dôkaz, že výrobok spĺňa požiadavky na bezpečnosť.
 - (b) Špecifikovanie kritických prvkov systému, z hľadiska nepriaznivých dôsledkov ich poruchy pre plnenie základných funkcií systému.
 - (c) Preukázanie splnenia požiadaviek na spoľahlivosť pre tím, než budú urobené komplexné skúšky spoľahlivosti.
 - (d) Poskytnutie vstupnej informácie pre návrh optimálneho systému technickej údržby systému.
 - (e) Poskytnutie vstupnej informácie pre návrh optimálneho systému technickej diagnostiky.
 - (f) Kombinácia vyššie uvedených účelov a cieľov, prípadne iné účely.
2. **Technický popis systému** - slovné popisy konštrukčného usporiadania a použitia technologického riešenia systému, doplnené o podrobnú výkresovú dokumentáciu, schémy, grafy apod.
3. **Definície funkcií systému a jeho prvkov** - táto vstupná informácia obsahuje podrobné vymenovanie všetkých dôležitých funkcií a prvkov, ktoré musia plniť a ktoré musia byť podrobené analýze. Funkcie musia byť definované tak, aby bolo možné študovať ich vzájomné súvislosti, podmienenosť, postupnosť, väzby na prevádzkové podmienky systému. Z definície musí byť možné odvodiť závažnosť dôsledkov ich nenaplnení, možnosti vzájomnej oddeliteľnosti jednotlivých funkcií a pod. Funkcia môže niekedy byť pre daný systém alebo prvok iba jedna, avšak väčšinou je funkcií niekoľko a pre každú definovanú funkciu sa realizuje účelovo zameraná analýza.

4. **Funkčné členenie systému** - musí korešpondovať s predchádzajúcim bodom. Špecifikuje sa, do akých funkčných subsystémov sa systém člení a to až do požadovanej hĺbky analýzy. Funkčné členenie môže byť zhodné alebo podobné konštrukčnému členeniu, ale nie je to pravidlom. Funkčné a konštrukčné členenie systému je nutné odlišovať, pretože výrobok jedného konštrukčného typu môže plniť celú radu odlišných funkcií a tomu musí byť prispôsobené i odpovedajúce funkčné členenie. Funkčnému členeniu sa potom prispôsobujú i modely spoľahlivosti, ktoré umožňujú analýzy spoľahlivosti.
5. **Definície rozhrania systému** - ide o presné vymedzenie hraničných bodov a prvkov, kde dochádza ku vzájomnej interakcii so susednými systémami alebo vonkajším okolím systému. V nich potom musia byť vymedzené okrajové podmienky pre analýzu systému. Definícia rozhrania má za cieľ vylúčiť prienik javov systémov tak, aby sa rovnaké analyzované javy neopakovali viackrát v rôznych systémoch.
6. **Údaje o prvkoch systému** - o všetkých prvkoch systému, až do zvolenej úrovne, ktorá je určená požadovanou hĺbkovou analýzou, musia byť k dispozícii aspoň tieto informácie:
 - (a) Jednoznačná identifikácia prvkov na schémach a výkresoch a pod.
 - (b) Popis funkcií prvkov.
 - (c) Popis možných spôsobov porúch prvkov.
 - (d) Popis dôsledkov porúch prvkov.
 - (e) Pravdepodobnosti jednotlivých spôsobov porúch prvkov, ak je požadované realizovanie kvantitatívnej.
 - (f) Zdroj informácií o pravdepodobnostiach.

FMEA sa skladá z nasledujúcich krokov:

1. **Stanovenie systémových prvkov a systémovej štruktúry** - systém sa skladá zo systémových prvkov, ktoré slúžia k popisu a členeniu hardwarovej koncepcie a sú usporiadané do systémovej štruktúry. Systémová štruktúra usporadúva odhora jednotlivé systémové prvky na rôznych hierarchických úrovniach. Okrem toho je nutné popísať existujúce prepojenie jednotlivých systémových prvkov ako rozhranie k ostatným systémovým prvkom.
2. **Znázornenie funkcií a funkčnej štruktúry** - Systémové prvky majú v systéme rôzne funkcie alebo úlohy. Spoločné pôsobenie funkcií viacerých systémových prvkov je možné znázorniť ako funkčnú štruktúru (strom funkcií/funkčnú sieť). Pre stanovenie funkčných štruktúr musíme sledovať vstupujúce a vnútorné funkcie.
3. **Vykonanie analýzy vad** - pre každý sledovaný prvok popísaný v systéme musíme vykonať analýzu chýb. Možné chyby tohoto systémového prvku sú odvodené od známej funkcie vymedzenej v kroku 2 a popisujú chybné funkcie.
 - (a) Ku každej chybe sa stanoví jej **možný dôsledok** a pomocou desaťbodovej stupnice sa ohodnotí jeho význam.
 - (b) **Možné príčiny chýb** sú vďaka chybnej funkcii podriadených systémových prvkov, prostredníctvom rozhrania, priradené systémovému prvku. Pri každej príčine sa odhadne **pravdepodobnosť výskytu chyby**, ktorá sa kvantifikuje pomocou desaťbodovej stupnice.

(c) Analýza je ukončená výčtom **existujúcich preventívnych opatrení** a zavedených **kontrolných opatrení**. Pri týchto opatreniach je hodnotená **pravdepodobnosť odhalenia príčiny vzniku chyby**, ktorá sa kvantifikuje pomocou desaťbodovej stupnice.

4. **Vykonanie hodnotenia miery rizika** - Miera rizika RPN je súčinom hodnôt bodového ohodnotenia:

$$RPN = B * A * E, \quad (3.7)$$

kde A je pravdepodobnosť výskytu chyby, B je význam chyby pre zákazníka a E je pravdepodobnosť odhalenia chyby.

5. **Vykonanie optimalizácie** - pri najvyšších hodnotách RPN sa vykonáva optimalizácia definovaním nápravných alebo preventívnych opatrení. Tieto opatrenia sú termínované a sú prenesené k vybaveniu na zodpovedných miestach/osobami. Pre vysoké hodnoty rizikového čísla RPN sú potrebné optimalizácie, tie sa vykonávajú v nasledujúcom poradí priorit:

- (a) Zmena koncepcie - pre vylúčenie príčiny chyby alebo pre redukcii chyby.
- (b) Zvýšenie spoľahlivosti koncepcie - pre minimalizáciu pravdepodobnosti výskytu príčiny chyby.
- (c) Účinné odhalenie príčiny chyby.

Pre minimalizáciu rizika sa musia dodatočné opatrenia popísať a pre ich zavedenie menovať zodpovednosti za vyriadenie.

6. **Sledovanie opatrení** - vybavenie opatrenia sleduje vedúci projektu/vedúci tímu. Akonáhle je opatrenie plne realizované, vykonáva sa znovu hodnotenie miery rizika.

Táto časť čerpá z [4, 9, 15].

3.3 HAZOP

Štúdia HAZOP bola pôvodne technika vyvinutá pre systémy zaoberajúce sa zachádzaním s tekutými látkami alebo iným tokom materiálu vo spracovateľskom priemysle. Obor použitia tejto metódy sa však v posledných rokoch neustále rozširoval a teraz sa používa napríklad u:

- Softwarových aplikáciách, vrátane programovateľných elektronických systémov.
- Systémov zahrňujúcich pohyb osôb rôznymi spôsobmi dopravy, ako je cestná alebo železničná doprava.
- Skúmaním rôznych postupností operácií a prevádzkových postupov.
- Hodnotenie administratívnych postupov v rôznych priemyslových odvetviach.
- Hodnotenie špecifických systémov, napríklad zdravotníckych zariadení.

Štúdia HAZOP je obzvlášť užitočná pri rozpoznávaní úzkych profilov (anglicky bottlenecks) v systémoch, vrátane toku materiálu, ľudí alebo dát, alebo u rady udalostí alebo činností v plánovanej postupnosti či pri rozpoznávaní postupov riadiacich takúto postupnosť. Okrem toho, že je štúdia HAZOP cenným nástrojom pri projektovaní a vývoju nových systémov, je možné ju taktiež užitočne použiť ku skúmaniu nebezpečia a potenciálnych problémov spojených s rôznymi prevádzkovými stavmi daného systému. Štúdiu HAZOP je možné použiť aj u šaržovitých a štatisticky nevládnutelných procesov a postupností, rovnako ako u kontinuálnych procesov. Na štúdiu HAZOP sa dá pozeráť ako na neoddeliteľnú súčasť všeobecnejšieho procesu hodnotového inžinierstva a managementu rizika.

Štúdia HAZOP je tímový proces podrobného rozpoznávania problémov týkajúcich sa nebezpečia a prevádzkyschopnosti. Štúdia HAZOP sa zoberá rozpoznávaním potenciálnych odchýlok od cieľa projektu, skúmaním ich možných príčin a hodnotením ich následkov. Klúčové vlastnosti skúmania HAZOP:

- Skúmanie sa realizuje pomocou systematického používania sady vodiacich slov, aby sa rozpoznali potenciálne odchýlky od cieľa projektu, a tieto odchýlky sa používajú ako „spúšťač mechanizmu“ pre stimuláciu predstav členov tímu o tom, ako by mohlo k odchýlkam dôjsť a aké by mohla mať následky.
- Skúmanie sa realizuje pod vedením vyškoleného a skúseného vedúceho štúdie, ktorý musí zaistiť podrobné pokrytie študovaného systému pomocou logického analytického myslenia. Vedúcemu štúdie pomáha v prvom rade zapisovateľ, ktorý zaznamenáva rozpoznané nebezpečia alebo narušenia prevádzky pre ďalšie vyhodnotenie a riešenie.
- Skúmanie vychádza zo znalostí špecialistov z rôznych vedných a technických oborov s vhodnými znalosťami a skúsenosťami, ktorí prejavujú intuíciu a dobrý úsudok.
- Skúmanie sa má realizovať v prostredí pozitívneho myslenia a otvorenej diskusie. Keď je rozpoznán problém, zaznamená sa pre následné hodnotenie.
- Riešenie rozpoznávaných problémov nie sú prvotným cieľom skúmania HAZOP, ale kým sa k nim dospeje, zaznamenajú sa, aby ich pracovníci zodpovední za projekt vzali v úvahu.

Štúdie HAZOP sa realizujú v štyroch základných postupných krokoch:

1. Stanovenie rozsahu, cieľov a zodpovedností.

- (a) Stanoví sa rozsah platnosti a ciele.
- (b) Stanovia sa zodpovednosti.
- (c) Vyberie sa tím.

2. Príprava.

- (a) Vypracuje sa plán štúdie.
- (b) Zhromaždia sa dáta.
- (c) Dohodne sa spôsob zápisu.
- (d) Odhadne sa doba.
- (e) Zostaví sa časový plán.

3. Skúmanie.

- (a) Systém sa rozdelí na časti.
- (b) Zvolí sa nejaká časť a stanoví sa cieľ projektu.
- (c) Pomocou vodiacich slov sa u každého prvku zistia odchýlky.
- (d) Rozpoznajú sa následky a príčiny.
- (e) Rozpozná sa, či existuje významný problém.
- (f) Rozpoznajú sa mechanizmy ochrany, detekcie a indikácie.
- (g) Rozpoznajú sa možné opatrenia k náprave/zmierneniu.
- (h) Odsúhlasia sa činnosti.
- (i) To isté sa opakuje u každého prvku a potom u každej časti systému.

4. Dokumentácia a ďalší postup.

- (a) Skúmanie sa zaznamená.
- (b) Schváli sa dokumentácia.
- (c) Vypracuje sa správa o štúdiu.
- (d) Sleduje sa, ako sú tieto činnosti uplatňované.
- (e) Štúdia sa opakuje u akýchkoľvek častí systému, pokiaľ je to nutné.
- (f) Vypracuje sa záverečná výstupná správa.

Tieto kroky nasledujú jeden po druhom, zatiaľ čo medzi kroky nemajú stanovené poradie, aj keď sú celkom logicky usporiadané [10].

3.3.1 Princípy skúmania

Základom štúdie HAZOP je skúmanie „pomocou vodiacich slov“, čo je zámerné vyhľadávanie odchýlok od cieľa projektu. Pre uľahčenie skúmania sa systém rozdelí na časti tak, aby mohol byť pre každú časť primerane stanovený cieľ projektu. Veľkosť zvolenej časti z pravidiel závisí na zložitosti systému a na závažnosti nebezpečia. V zložitých systémoch alebo v systémoch, ktoré predstavujú veľké nebezpečenstvo, bývajú tieto časti z pravidiel malé. V jednoduchých systémoch alebo v systémoch, ktoré predstavujú malé nebezpečie, použitie väčších častí urýchľuje štúdiu. Cieľ projektu pre danú časť systému sa vyjadří pomocou prvkov, ktoré sú nositeľmi význačných vlastností danej časti, a ktoré predstavujú prirodzené rozdelenie systému na časti. Voľba prvkov, ktoré sa majú skúmať je do určitého rozsahu subjektívnym rozhodnutím, keďže môže existovať niekoľko kombinácií, ktorými býva možné dosiahnuť požadovaného účelu a voľba môže taktiež závisieť na konkrétnej aplikácii. Prvky môžu byť samostatné kroky alebo etapy postupu, jednotlivé signály a objekty zariadenia v riadiacom systéme, môžu to byť zariadenia alebo súčiastky v procese alebo v elektronickom systéme.

Tím HAZOP skúma každý prvok z hľadiska odchýlky od cieľa projektu, ktorá môže viesť k nežiadúcim následkom. Rozpoznanie odchýlok od cieľa projektu sa dosahuje procesom pokladania otázok s použitím predom stanovených „vodiacich slov“. Role vodiaceho slova spočíva v stimulácii myslenia, jeho sústredenia na štúdiu a vyvolania nápadov a diskusií, čím sa maximalizujú vyhliadky na úplnosť štúdie. Základné kľúčové slová a ich význam sú uvedené v tabuľke 3.2. Dodatočné vodiace slová vzťahujúce sa k stanovenému času a k poradiu alebo postupnosti sú uvedené v tabuľke 3.3 [10].

Vodiace slovo	Význam
Žiadny, nie je žiadny alebo Nie	Úplná negácia cieľa projektu
Vyšší	Kvantitatívny nárast, kvantitatívne plus
Nižší	Kvantitatívny pokles, kvantitatívne mínus
A taktiež, Ako i, a rovnako	Kvalitatívny nárast, kvalitatívne plus
Čiastočne	Kvalitatívny pokles, kvalitatívne mínus
Obrátený, Spiatočný	Logický opak cieľa projektu
Iný ako	Úplná náhrada alebo zámena

Tabuľka 3.2: Základné vodiace slová a ich všeobecný význam [10].

Vodiace slovo	Význam
Predčasný	Vzhľadom k stanovenému času
Oneskorený	Vhľadom k stanovenému času
Pred	Vzhľadom k poradiu alebo postupnosti
Po	Vzhľadom k poradiu alebo postupnosti

Tabuľka 3.3: Dodatočné vodiace slová vzťahujúce sa k stanovenému času a k poradiu alebo postupnosti [10].

3.3.2 Vodiace slová a odchyľky

V etape plánovania štúdie HAZOP má vedúci štúdie navrhnúť počiatočný zoznam vodiacich slov, ktoré sa majú používať. Vedúci štúdie nevrhnuté vodiace slová vyskúša u daného systému a potvrdí ich primeranosť. Voľba vodiacich slov sa má dôkladne zvážiť, pretože vodiace slovo, ktoré je príliš špecifické, môže obmedziť nápady a diskusiu. Vodiace slovo, ktoré je príliš všeobecné, nemusí efektívne zamerať pozornosť štúdie HAZOP.

Kombinácie *vodiace slovo* — *prvok/charakteristika* môžu byť v štúdiách iných systémov, v iných etapách životného cyklu a pri použití iných prezentácií projektu interpretované odlišne. Niektoré kombinácie nemusia mať pre danú štúdiu zmysluplnú interpretáciu a nemá sa na ne brať ohľad. Interpretácia všetkých kombinácií *vodiace slovo* — *prvok/charakteristika* má byť presne vymedzené a zdokumentované.

Sústavu kombinácií *vodiace slovo* — *prvok/charakteristika* je možné považovať za maticu, v ktorej vodiace slová určujú riadky a prvky určujú stĺpce. V každej takto vytvorenej bunke matice potom bude špecifická kombinácia vodiaceho slova a prvku. K úplnému rozpoznaní všetkých nebezpečí je nutné, aby prvky a s nimi združené charakteristiky pokrývali všetky príslušné aspekty cieľa projektu a vodiace slová pokrývali všetky odchyľky. Nie všetky kombinácie budú dávať vierohodné odchyľky, takže i keď sa úvážia všetky kombinácie vodiacich slov a prvkov, môže mať matica niekoľko prázdnych miest.

Existujú dve možné postupnosti, v nich sa môžu bunky matice skúmať, a síce, „*stĺpec po stĺpci*“ tj. *najprv prvok*, alebo „*riadok po riadku*“, tj. *najprv vodiace slovo*. Výsledky týchto skúmaní majú byť v princípe rovnaké.

Analýza sa má riadiť podľa toku alebo postupnosti týkajúcej sa predmetu analýzy, pričom má postupovať od vstupov k výstupom v logickej postupnosti. Sila techník rozpoznávania nebezpečia, ako je HAZOP, spočíva v systematickom procese skúmania krok

za krokom. Existujú dve možné postupnosti skúmania „najprv prvok“ a „najprv vodiace slovo“, ako je znázornené v nasledujúcich algoritmoch [10].

Algoritmus postupnosti „najprv prvok“

1. Vysvetlí sa celkový projekt.
2. Zvolí sa časť.
3. Prezkúma sa a dohodne sa cieľ projektu.
4. Rozpoznajú sa príslušné prvky.
5. Rozpozná sa, či môže byť niektorý z týchto prvkov užitočne rozdelený na charakteristiky.
6. Zvolí sa prvok (a charakteristika, pokiaľ sa používa).
7. Zvolí sa vodiace slovo.
8. Vodiace slovo sa použije pri zvolených prvkov (a pri každej jeho charakteristike, pokiaľ sa používa), aby sa získala špecifická interpretácia.
9. Je odchylka vierohodná? Ak áno tak pokračovať, ak nie tak preskočiť na krok 11.
10. Prezkúmajú a zdokumentujú sa príčiny, následky a ochrana či indikácia.
11. Boli použité všetky interpretácie kombinácií vodiacich slov a prvkov/charakteristík? Ak áno tak pokračovať, ak nie tak preskočiť na krok 8.
12. Boli pri zvolenom prvku použité všetky vodiace slová? Ak áno pokračovať, ak nie tak preskočiť na krok 7.
13. Boli prezkúmané všetky prvky? Ak áno tak pokračovať, ak nie tak preskočiť na krok 6.
14. Boli prezkúmané všetky časti? Ak áno pokračovať, ak nie tak preskočiť na krok 2
15. Koniec algoritmu [10].

Algoritmus postupnosti „najprv vodiace slovo“

1. Vysvetlí sa celkový projekt.
2. Zvolí sa časť.
3. Prezkúma sa a dohodne sa cieľ projektu.
4. Rozpoznajú sa príslušné prvky.
5. Rozpozná sa, či môže byť niektorý z týchto prvkov užitočne rozdelený na charakteristiky.
6. Zvolí sa vodiace slovo.
7. Zvolí sa prvok (a charakteristika, pokiaľ sa používa).

8. Pri zvolenom prvku (a u každej jeho charakteristiky, pokiaľ sa používa) sa použije vodiace slovo, aby sa získala špecifická interpretácia.
9. Je odchylka vierohodná? Ak áno tak pokračovať, ak nie tak preskočiť na krok 11.
10. Prezkúmajú a zdokumentujú sa príčiny, následky a ochrana či indikácia.
11. Boli použité všetky interpretácie kombinácií vodiacich slov a prvkov/charakteristík? Ak áno tak pokračovať, ak nie tak preskočiť na krok 8.
12. Bolo zvolené vodiace slovo použité pri všetkých prvkoch? Ak áno tak pokračovať, ak nie tak preskočiť na krok 7.
13. Boli použité všetky vodiace slová? Ak áno tak pokračovať, ak nie tak preskočiť na krok 6.
14. Boli prezkúmané všetky časti? Ak áno tak pokračovať, ak nie tak preskočiť na krok 2.
15. Koniec algoritmu [10].

Kapitola 4

Rational Team Concert

Táto kapitola vysvetľuje čo systém Rational Team Concert (zkrátene RTC) je a aké je jeho využitie. Táto kapitola zároveň ukazuje možné integrácie s rôznymi aplikáciami tretích strán a prechádza z akých položiek sa plánovanie v systéme RTC realizuje. Ďalej táto kapitola popisuje API systému RTC a ako sa pre tento systém vytvárajú potenciálne rozšírenia.

4.1 Všeobecne ku RTC

Systém Rational System COncert (skrátene RTC) je systém na správu projektu. tento systém je zastrešovaný spoločnosťou IBM a je podobný open-sourceprojektu Redmine. RTC je postavené na technológii IBM Jazz, čo je rozšíriteľná platforma, ktorá pomáha tímom integrovať úlohy naprieč životnému cyklu softwaru. RTC využíva klient-server architektúru, kde klient je v podobe webovej aplikácie alebo desktopová aplikácia, ktorej rozhranie je postavené na vývojom prostredí Eclipse. Vývojové tímy používajú RTC na monitorovanie aspektov ich práce ako je kontrola zdrojových kódov, reportovanie a vstavaný manažment v jednom produkte. RTC je možné spojiť s inými produktmi, ako aj s produktami IBM vrátane:

- SVN
- GIT
- JIRA
- HP Quality Center
- Jenkins
- Hudson
- CruiseControl
- Maven
- Raional ClearCase
- Rational ClearQuest
- Rational Quality Manager

- Rational Focal Point
- Rational System Architekt
- Rational Build Forge

Tento systém veľmi dobre kooperuje s agilnou metodikou SCRUM, kde sa dajú jednoducho nastaviť šprinty a sledovať backlog [1].

Pri plánovaní projektu sa používajú pracovné prvky (anglicky Work Items). Každý pracovný prvok má svoj vlastný workflow (pracovný postup) a asociované atribúty, ktoré sú použité pre riadenie, sledovanie pokroku, reportovanie a spoluprácu. Medzi základné pracovné prvky patria:

- **Epic** - reprezentuje vysokoúrovňovú potrebu, ktorá musí byť rozdelená do menších častí, ktoré sa majú vyvinúť.
- **Story** - sú užívateľské scenáre, ktoré poskytujú pridanú hodnotu produktu a ktoré môžu byť vyvíjané v jednotlivých šprintoch alebo iteráciách.
- **Task** - je úloha s drobnými detailami, ktorá musí byť hotová počas šprintu alebo počas iterácie.
- **Risk** - ide o pracovnú úlohu, ktorá reprezentuje riziko, ktoré môže nastať. Tieto riziká môžu obsahovať podúlohy typu Task, aby bolo jednoznačné, čo sa má urobiť aby sa prišlo na príčinu rizika, alebo čo sa robí pre jeho zabráneniu.
- **Defect** - jedná sa o chyby, ktoré pri vývoji vznikli. Tieto chyby sa môžu skladať rovnako z podúloh typu Task ako je to pri Risk.

Názvy týchto pracovných prvkov sú zámerne nepreložené, aby ich bolo možné odlíšiť na obrázkoch. Odporúčaná hierarchia tých prvkov je:

- Epic
 - Story
 - * Task
 - * Risk
 - Task - voliteľné
 - * Defect
 - Task - voliteľné

Pred samotným pridávaním pracovných prvkov, je nutné pripraviť si iteráciu alebo šprint a backlog. Pre ne je potrebné určiť tímy, ktoré sa budú podieľať na jednotlivých podprojektoch daného projektu [12].

Spoločnosť FEI, pre ktorú toto rozšírenie bolo navrhnuté má vytvorený vlastný pracovný prvok pre analýzu rizík pomocou metódy FMEA. Tento rozširujúci pracovný prvok sa nazýva FMEA Issue. Okrem bežných atribútov pre nastavenie rizika, umožňuje toto rozšírenie zadať aj FMEA vlastnosti ako:

- **Severity** - význam chyby.
- **Probability** - pravdepodobnosť chyby.

- **Detectability** - pravdepodobnosť odhalenia chyby.
- **FMEA RPN** - miera zadaného rizika.

Tieto atribúty sa zadávajú pomocou výberu zo 4 možných hodnôt a to:

- **Unassigned** (slovensky nepriradené).
- **Low** (slovensky malé).
- **Medium** (slovensky stredné).
- **High** (slovensky veľké).

Pre FMEA RPN nie je možné zadávať ani jednu z týchto hodnôt. FMEA RPN sa vypočíta zo zadaných hodnôt, ktorým sú priradené celočíselné hodnoty. Príklad FMEA je možné vidieť na obrázku 4.1.

Obr. 4.1: Príklad zadávania pracovného prvku FMEA Issue.

4.2 Vývojové prostredie a API systému RTC

System RTC poskytuje klientské rozhranie podobné vývojovému prostrediu Eclipse, spolu s webovým rozhraním pre monitorovanie činností na projektoch uvedených v systéme. Prostredie Eclipse (použitý názov Eclipse je aj často využívaný komunitou systému RTC) okrem prehliadania pracovných prvkov umožňuje aj prispôsobovanie systému potrebám užívateľa. System RTC je veľmi univerzálny a poskytuje veľa možností pri vytváraní nových pracovných prvkov a ich vlastností.

Vytváranie projektu

Po úspešnom prihlásení do prostredia Eclipse sa vytvorí spojenie so serverom aplikácie. Ak máte administrátorské práva, systém Vám zobrazí všetky dostupné projekty, ktoré sú uložené v databáze systému. V tomto zozname môžete pravým kliknutím vytvoriť nový projekt, kde nasleduje prvotná konfigurácia projektu. V prvom rade si pridáte ľudí do kolonky administrátorov. Tým umožníte týmto ľuďom spravovať a ovládať váš projekt. Po pridaní administrátorov pridáte členov tímu, ktorí budú môcť pracovať so systémom ako bežní užívatelia.

Ak máme vytvorené tímy pridáme prvú časovú líniu projektu, ku ktorej si následne pridáme ďalšie iterácie alebo šprinty. Ak máme vytvorené prvé línie je dobré si pridať aspoň jednu časovú líniu pre pracovné prvky, ktorá bude slúžiť ako kôš a jednu pracovnú líniu, ktorá bude slúžiť ako backlog (zoznam úloh nepridelených do žiadneho šprintu, z agilnej metodiky SCRUM). Príklad tejto obrazovky je možné vidieť na obrázku 4.2.

Details

Summary
Description

Members

Roles grant users permissions and determine the preconditions and follow-up actions that run. Roles assigned here are inherited in all team areas within this project area. All users in the repository have the Everyone (default) role whether they are a member or not.

Name	Process Roles
Filicko, David	Project Area Administrator

Administrators

If you require permissions, contact an administrator. Project administrators can modify and save this project area and its team areas.

Name	e-mail
Caha, Jaroslav	Jaroslav.Caha@fei.com
Filicko, David	David.Filicko@fei.com

Process Sharing

Specify how to share the process configuration between project areas:

- Do not share the process configuration of this project area
- Allow other project areas to use the process configuration from this project area
- Use the process configuration from another project area for this project area

Process: customized

Timelines

The project timeline defines a start and end date along with a start and end date for each iteration.

- Test1 Timeline [Project Timeline]
 - iteration [3/24/16 - unknown]
 - trash [5/16/16 - unknown]

Overview | Links | Process Configuration | Process Configuration Source | Access Control | Work Item Categories | Releases

Obr. 4.2: Príklad vyvoreného nového projektu.

Vytvorenie tímov

Potom ako sme úspešne vytvorili projekt je potreba prideliť členov do projektových tímov. To urobíme na záložke *kategorie pracovních skupín* (anglicky Work Item Categories). Na ľavej strane okna si môžeme vyvoriť podprojekty tohto veľkého projektu, zatiaľ čo na pravej strane vytvárame tímy, do ktorých po rozkliknutí pridáme členov projektu (podľa potrieb). Ak máme vytvorené tímy a podprojekty pridelíme tímy ku podprojektom. Podmienkou je, že na podprojekte môže pracovať výhradne jeden tím, ale jeden tím môže pracovať na viacerých podprojektoch. Príklad takto rozdelených tímov je možné vidieť na obrázku 4.3. Po pridelení tímov ku podprojektom sme úspešne dokončili prípravu projektu a môžeme ho používať ako bežný užívateľia.

The screenshot displays a project configuration window with several sections:

- Details:** Includes fields for 'Summary' and 'Description'.
- Members:** A table for assigning roles to users. It shows one member: David Filicko with the role 'Project Area Administrator'. Buttons for 'Add...', 'Create...', 'Remove', and 'Process Roles...' are present.
- Administrators:** A table for listing project administrators. It shows two administrators: Jaroslav Caha (Jaroslav.Caha@fei.com) and David Filicko (David.Filicko@fei.com). Buttons for 'Add...', 'Create...', and 'Remove' are present.
- Process Sharing:** Radio buttons to select how process configuration is shared: 'Do not share the process configuration of this project area' (selected), 'Allow other project areas to use the process configuration from this project area', and 'Use the process configuration from another project area for this project area'.
- Process: customized** and **Timelines:** The 'Timelines' section shows a tree view with 'Test1 Timeline [Project Timeline]' containing an 'iteration [3/24/16 - unknown]' and a 'trash [5/16/16 - unknown]'.

At the bottom, a navigation bar includes tabs for Overview, Links, Process Configuration, Process Configuration Source, Access Control, Work Item Categories, and Releases.

Obr. 4.3: Príklad priraďovania tímov ku podprojektom.

Vytváranie nových pracovných prvkov

Ak nám predvytvorené pracovné prvky nevyhovujú a potrebujeme si vytvoriť vlastné, RTC nám ponúka túto možnosť v záložke *konfigurácia procesu* (anglicky process configuration). Táto záložka má najviac možností, ktoré systém RTC umožňuje. Dokážeme si tu prispôbiť akékoľvek nastavenie od plánu cez práva užívateľom, po samotné pracovné prvky. Ak chceme konfigurovať samotné pracovné prvky musíme rozkliknúť záložku v ľavom okne s názvom *konfigurácia projektu* (anglicky project configuration) potom *konfigurácia dát* (anglicky configuration data) a posledné, čo rozklikneme sú pracovné prvky (anglicky work items). Príklad tohto môžeme vidieť na obrázku 4.4. Táto kategória umožňuje programovať vlastnosti jednotlivých pracovných prvkov a to pomocou Javascript.

The screenshot displays the configuration interface for work items in RTC. It is divided into several sections:

- Details:** Includes fields for 'Summary' and 'Description'.
- Members:** A table listing users and their roles, with buttons for 'Add...', 'Create...', 'Remove', and 'Process Roles...'.

Name	Process Roles
Filicko, David	Project Area Administrator
- Administrators:** A table listing administrators and their email addresses, with buttons for 'Add...', 'Create...', and 'Remove'.

Name	e-mail
Caha, Jaroslav	Jaroslav.Caha@fei.com
Filicko, David	David.Filicko@fei.com
- Process Sharing:** Radio buttons to specify how to share the process configuration between project areas:
 - Do not share the process configuration of this project area
 - Allow other project areas to use the process configuration from this project area
 - Use the process configuration from another project area for this project area

At the bottom, a navigation bar shows tabs for 'Overview', 'Links', 'Process Configuration', 'Process Configuration Source', 'Access Control', 'Work Item Categories', and 'Releases'.

Obr. 4.4: Príklad konfigurácie pracovných prvkov.

V tejto položke sa vyskytujú všetky konfiguračné vlastnosti pracovného prvku. Medzi základné patria tieto položky:

- **Typy a atribúty** - tu je možné definovať nové pracovné prvky, ich atribúty a naprogramované zobrazenia pracovných prvkov. Zároveň sa tu vyberá aj pracovný postup.
- **Výčtové typy** - niektoré atribúty nemusia byť typu float alebo string, ale môžu byť výčtové typy, a tu sa definujú jednotlivé položky výčtov. Tie sa potom previažu s pracovnými prvkami.
- **Prispôsobovanie atribútov** - ak má nejaký atribút určitú vlastnosť napríklad pravdepodobnosť je v intervale od 0 do 1, tu je to možné nastaviť. Nastavujú sa tu aj predvolené hodnoty alebo podmienky ich určenia. Prípadne sa tu programujú výpočty hodnôt jednotlivých atribútov.
- **Pracovné postupy** - umožňujú monitorovať a sprehľadňovať priebeh vývoja. Napríklad ak vývojár dokončí nejakú úlohu presunie ju do stavu dokončené a ak prejde testovaním tak sa daná úloha uzavrie.
- **Editor prezentácie** - tu sa nastaví, ktoré položky sa majú ukázať v jednotlivých druhoch editoroch. Potrebné to je z dôvodu, že v prípade rizík nás zaujíma, aká je pravdepodobnosť tohto rizika, ale nezaujíma nás táto hodnota pri bežnej úlohe.
- **Prezentácia rýchlych informácií** - táto kategória je podobná s editorom prezentácií. Nastavujú sa tu aké rýchle informácie sa majú zobrazit užívateľovi.

Kapitola 5

Návrh a implementácia

5.1 Výber metód

Keďže spoločnosť FEI má implementovaný vlastný pracovný prvok pre metódu FMEA, pre účely tohto rozšírenia boli vybrané metódy:

- ETA
- FTA

Síce tieto metódy majú spoločné rysy, ktoré by mohli uľahčiť samotný vývoj, žiaľ preto, že toto rozšírenie má slúžiť výhradne pre dokumentačné účely, je tento prínos zanedbateľný. Pri implementovaní tohto rozšírenia bude potrebné správať sa k týmto metódam rozdielne.

5.2 Špecifikácia požiadaviek rozšírenia

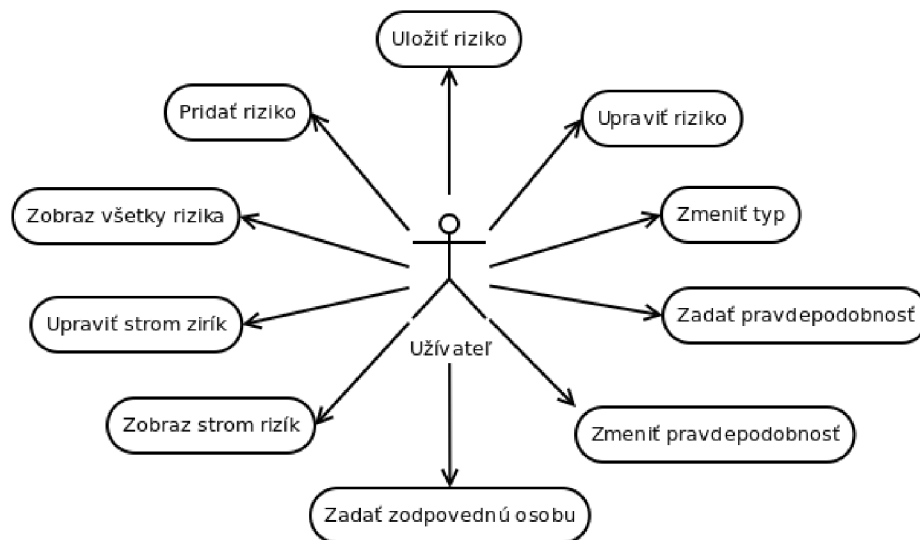
- **Funkčné požiadavky** - rozšírenie umožní zobrazovať riziká rozhodovacích stromov (ETA a FTA). Rozšírenie umožní interaktívne meniť, vytvárať a meniť nové prvky stromu. Ďalej bude možné zobraziť si celý register rizík.
- **Požiadavky na zrozumiteľnosť** - rozšírenie musí byť jednoznačné a ľudia ho musia vedieť bez problémov zadať. Aplikácia by nemala zmeniť pravidlá zadávania údajov ako je zvyknuté používať v systéme RTC.
- **Požiadavky na výkonnosť** - aplikácia nesmie spomaľovať systém RTC a užívateľ nesmie cítiť dlhé spracovanie požiadaviek.

Rozšírenie musí zvládať prípady použitia ako sú znázornené na diagrame, na obrázku [5.1](#).

5.3 Implementácia

Podľa špecifikácie a znalostí z manažmentu rizík a metód ETA a FTA boli vytvorené nasledujúce pracovné prvky:

- FTA
- FTA And



Obr. 5.1: Diagram prípadov užitia [vlastné spracovanie].

- **FTA Or**
- **FTA Term**
- **ETA**
- **ETA Term**

Pracovný prvok *FTA* reprezentuje najvyšší prvok. V samotnej podstate ide o vrcholovú udalosť, ktorá je výsledkom jednotlivých problémov. Z tohto pracovného prvku vychádzajú všetky podprvky.

Pracovné prvky *FTA And* a *FTA Or* reprezentujú hradlá And a Or, ktoré su definované pre metódu FTA. Tieto pracovné prvky môžu bezprostredne nasledovať vrcholovú udalosť. Môžu pozostávať buď to z ďalších pracovných prvkov FTA And alebo FTA Or alebo môžu obsahovať FTA Term pracovné prvky.

Posledným pracovným prvkom pre metódu FTA je *FTA Term*. FTA Term reprezentuje konečné udalosti alebo zdroje porúch. Tieto samotné pracovné prvky môžu smerovať k inému FTA stromu.

Keďže stromy ETA sa neskladajú zo spájacích prvkov, ako stromy FTA, nie sú pre ne potrebné a stačí to pokryť jedným pracovným prvkom. Tento pracovný prvok sa volá *ETA* a pokrýva, všetky rozhodnutia, udalosti alebo riziká, ktoré nastávajú. ETA je zároveň aj vrcholovým pracovným prvkom.

Potom ako sú zadané vetvenia stromu ETA je potrebné vložiť koncové pracovné prvky. Tie sú pomenované ako *ETA Term* a ukazujú pravdepodobnosť danej vetvy stromu.

Keďže tieto rovnako spadajú do kategórie pracovných prvkov, ich editory musia vyzerať podobne ako ostatné. Pre ich účely je možné nastaviť:

- **Názov pracovného prvku** - slúži pre stručný popis rizika, a tým rýchlejšie pochopenie problému.
- **Typ pracovného prvku** (buď FTA, ETA alebo jeden z vyššie vymenovaných).
- **Pravdepodobnosť** - je desatinné číslo, ktoré určuje pravdepodobnosť výskytu rizika.

- **Značky** - značky umožňujú rýchlejšie vyhľadávanie rizík.
- **Vlastník** - tým, že sa určí vlastník rizika je možné sa konkrétne pýtať vlastníka o ďalší postup ak riziko nastane.
- **Vyplnené proti** - toto políčko umožňuje spravovať riziká a priradzovať ich ku kategóriám. Tie môžu byť aj jednotlivé podprojekty, ktorých sa použitia metóda týka, alebo pre sledovanie ako prebieha vývoj a zmeny v jednotlivých iteráciách projektu.
- **Plánované pre** - v tomto políčku má možnosť užívateľ nastaviť ktorej iterácii alebo šprintu sa dané riziko týka, alebo v ktorom sa vyskytlo.
- **Rýchle informácie** - robia rýchly prehľad pre užívateľa aké sú podproblémy, z ktorých sa skladá daný pracovný prvok, prípadne aké sú podobné pracovné prvky.
- **Popis** - keďže názov prvku môžeme byť niekedy veľmi obsírny, je dobre to špecifikovať v popise.
- **Diskusia** - umožňuje užívateľom komunikovať o probléme a informovať majiteľa o tom, že dané riziko sa už nemusí nachádzať v systéme.

Náhľad na tieto prvky môžete vidieť na obrázku 5.2.

The screenshot shows a web form for creating a risk in the RTC system. At the top, there's a title bar with 'FTA <13:18:56>' and a 'Save' button. Below the title bar is a 'Summary' field and a dropdown menu set to 'Uninitialized'. The main form is divided into sections: 'Details', 'Description', and 'Discussion'. The 'Details' section contains several fields: 'Type' (FTA), 'Probability' (0), 'Tags' (empty), 'Owned By' (Unassigned), 'Filed Against' (Unassigned), and 'Planned For' (iteration). The 'Description' section has a large text area. The 'Discussion' section has a 'Add a comment...' input field. On the right side, there's a 'Quick Information' sidebar showing 'No Links'.

Obr. 5.2: Zadávanie rizík cez webové rozhranie systému RTC [screenshot obrazovky].

Pre potreby vizualizácie registra rizík bol naimplementovaný dotaz, ktorý ukáže všetky riziká, ktoré boli zadane pre celý projekt. Užívateľ má možnosť triediť, radiť si vyhladané pracovné prvky, čo mu umožňuje efektívnejšie pracovať s rizikami. Príklad zobrazeného zoznamu všetkých rizík je na obrázku 5.3.

Type	Id	Summary	Probability	Owned By	Modified Date	Actions
	58543	operator restart cooling	0.0075	Filicko, David	May 13, 2016, 10:48:04 AM	
	58542	Operator restarts cooling	0.99	Filicko, David	May 13, 2016, 10:46:39 AM	
	58541	Operator should runaway	0.0025	Filicko, David	May 13, 2016, 10:44:22 AM	
	58540	operator does NOT notice High Temperature	0.0025	Filicko, David	May 13, 2016, 10:41:47 AM	
	58539	Operator notices high temperature	0.0075	Filicko, David	May 13, 2016, 10:40:37 AM	
	58538	Operator NOT alarmed with High Temperature	0.01	Filicko, David	May 13, 2016, 10:38:53 AM	
	58537	Operator alarmed with High Temperature	0.99	Filicko, David	May 13, 2016, 10:38:07 AM	
	58536	Loss of cooling	1	Filicko, David	May 13, 2016, 10:36:22 AM	
	58535	Bad password	0.2	Filicko, David	May 13, 2016, 1:17:28 AM	
	58534	Bad username	0.1	Filicko, David	May 13, 2016, 1:16:49 AM	

Obr. 5.3: Zobrazenie registru rizík v možnosťami triedenia [screenshot obrazovky].

Avšak samotný register nevytvára o ničom. Preto je potrebné tieto riziká nejako vizualizovať a umožniť užívateľovi pochopiť danú problematiku. Ale systém RTC pracuje len s plánmi prípadne iteráciami. Preto ak chce užívateľ vidieť hierarchiu FTA alebo ETA stromov musí si dať ukázať plán, ktorý mu hierarchie ukáže. Po zobrazení plánu užívateľ vidí vrcholové udalosti resp. problémy ako prvé. Po rozkliknutí šípky, čo je pri vrcholovej udalosti zobrazí sa mu najbližšie delenie tohto problému. Toto zobrazenie môžete vidieť na obrázku 5.4. V pláne je možné vidieť aj podprojekty vytvorené v tomto projekte. Tieto projekty nemajú priradené žiadne riziká, pretože boli vytvorené pre testovacie účely.

Po zobrazení registra rizík alebo zobrazení si ich v pláne má užívateľ možnosti upravovať si tieto riziká buď kliknutím na názov, kde ho presmeruje na okno rovnaké ako pri zadávaní rizika. Pri ponechaní myši nad rizikom sa zobrazia dodatočné informácie o riziku.

Risk analysis plan Auto-Save Save

15 items total, 8 loaded items: 8 open, 0 closed | Ends in: --

Plan Details Edit

Planned Items Links Snapshots Dashboard Notes

View As: Default plan view Exclude | Type to Filter Add Work Item

Unassigned									
Closed Items: 0 Open Items: 8									
Summary	Id	Work Item T	Prob:	Owned B	Filed Against	Modif	Childr	Tags	
acquisition pc Closed Items: 0 Open Items: 0									
electricity sources Closed Items: 0 Open Items: 0									
microscope Closed Items: 0 Open Items: 8									
Summary	Id	Work Item T	Prob:	Owned B	Filed Against	Modif	Childr	Tags	
Building Failure	58527	FTA	0.6	Filickc	microsco	May	Lir	--	
Hardware	58528	FTA And	0.01	Filickc	microsco	May	Lir	--	
Software	58529	FTA Or	0.5	Filickc	microsco	May	Lir	--	
Wrong authentication	58532	FTA And	0.2	Filickc	microsco	May	Lir	--	
Failed to start	58533	FTA Terr	0.3	Unass	microsco	May	--	--	
Loss of cooling	58536	ETA	1	Filickc	microsco	May	Lir	--	
Operator alarmed with High Temperature	58537	ETA	0.99	Filickc	microsco	May	58	--	
Operator restarts cooling	58542	ETA Terr	0.99	Filickc	microsco	May	--	--	
Operator NOT alarmed with High Temperature	58538	ETA	0.01	Filickc	microsco	May	Lir	--	

Obr. 5.4: Zobrazenie stromu FTA a ETA v projektovom pláne [screenshot obrazovky].

Kapitola 6

Testovanie

6.1 Prípadová štúdia - ETA

Popis problému

Otestovanie metódy ETA spočíva v znázornení vybraného stromu v systéme RTC. Pre metódu ETA bol vybraný prípad, keď dôjde k strate chladenia. Postupnosťou udalostí dochádza k nasledujúcim koncovým stavom s uvedenými pravdepodobnosťami:

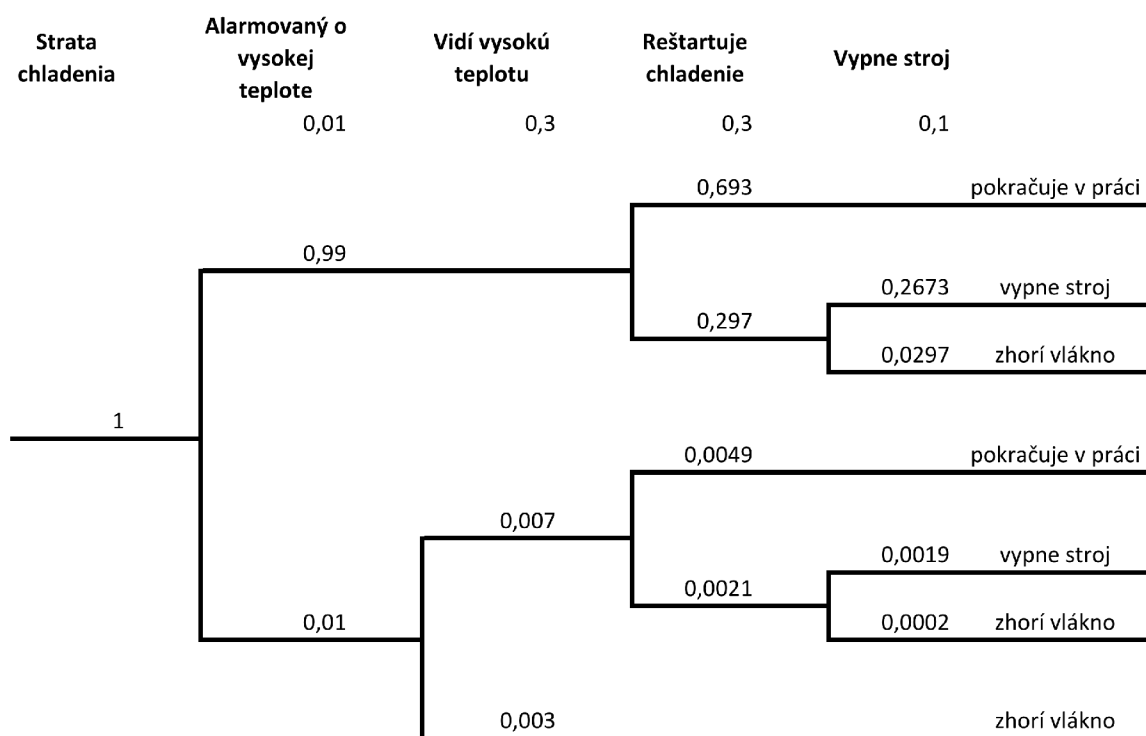
- *Operátor pokračuje v práci* s pravdepodobnosťou 0,6979.
- *Operátor vypne stroj* s pravdepodobnosťou 0,2692.
- *Operátorovi zhorí vlákno* s pravdepodobnosťou 0,0329.

Analýza stromu udalostí

Zo získaných údajov priložených v tabuľke 6.1 bol vytvorený strom, ktorý je na obrázku 6.1. Stromová hierarchia bola konštruovaná podľa logiky jednotlivých udalostí a podľa toho ako plynú v čase. Následne bol tento strom zdokumentovaný do systému RTC ako je možné vidieť na obrázku 6.2.

Udalosť	Pravedpodobnosť
Operátor bol alarmovaný o vysokej teplote	0,99
Operátor nebol alarmovaný o vysokej teplote	0,01
Operátor si všimol vysokú teplotu	0,7
Operátor si nevšimol vysokú teplotu	0,3
Operátor reštartuje chladenie	0,7
Operátor nereštartuje chladenie	0,3
Operátor vypne stroj	0,9
Operátor nechá stroj pracovať	0,1

Tabuľka 6.1: Tabuľka pravdepodobnosti udalostí [vlastné spracovanie].



Obr. 6.1: Strom udalostí prípadovej štúdie [vlastné spracovanie].

6.2 Prípadová štúdia - FTA

Popis problému

Test metódy FTA bude prezentovaný na príklade získavania obrazu skenovania predmetu pomocou CT technológie, kde výsledkom bude čierny obraz pixelov. Tento obraz je samozrejme nevalidný, a k tomuto obrázku došlo poruchou na zariadení alebo pri nastavovaní snímania. Dáta boli získane pri práci na priemyselnom CT. Avšak tieto dáta neukazujú všetky možné scenáre problému, pretože by komplexnosť tohto stromu bola obrovská, čo pre prípadovú štúdiu nie je potrebné.

Analýza stromom porúch

Chyby, ktoré môžu nastať ak získame obraz čiernych pixelov sú dvojakého typu. A to hardwarové a softwarové. Softwarové chyby, môžu byť aj chyby ľudské, pretože zle nastavené parametre skenovania sú z väčšej časti ľudské. Softwarové chyby majú také pomenovanie, pretože sú nastavené v samotnom softwary. Všetky tieto chyby môžeme vidieť v tabuľke 6.2.

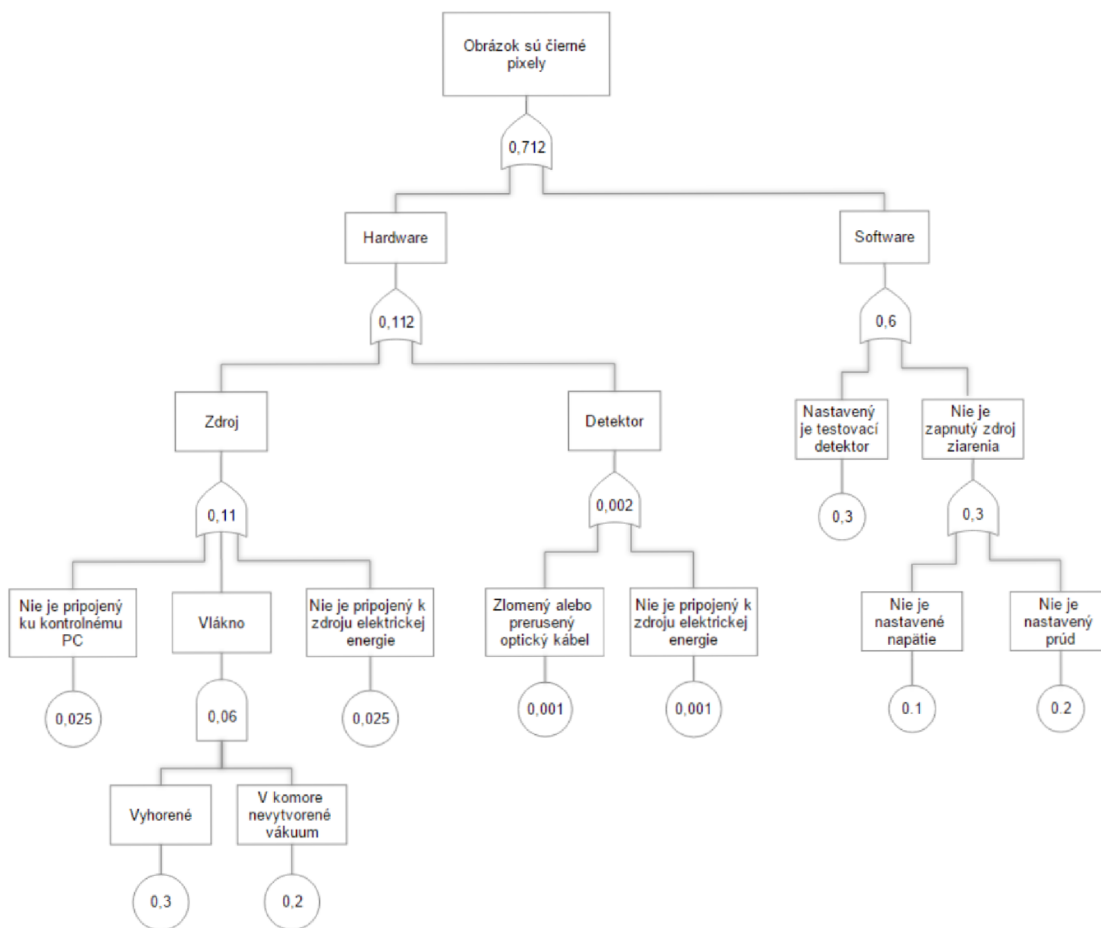
Pre tieto chyby bol vytvorený FTA strom, ktorý môžete vidieť na obrázku 6.3. Tento graf spĺňa všetky požiadavky na strom FTA, definovaných v sekcii o FTA strome (sekcii 3.1.1). Následne tento strom bol prevedený do systému RTC, kde jeho podoba je ukázaná na obrázku 6.4.

Summary	Id	Work Item Typ	Probability	Owned B:	Filed Agai	Modifi	Childr	Tags
▼ Strata chladenia	58536	ETA	1	Filickc	micros	May 20	Li	--
▼ Operator NEBOL alarmovany o vysokej teplote	58538	ETA	0.01	Filickc	micros	May 20	Li	--
▼ Operator si vsimol vysoku teplotu	58539	ETA	0.007	Filickc	micros	May 20	Li	--
▼ Operator restartuje chladenie	58542	ETA	0.0049	Filickc	micros	May 20	5€	--
Operator pokracuje v praci	58565	ETA Term	0.0049	Filickc	micros	May 20	--	--
▼ operator NERESTARTUJE chladenie	58543	ETA	0.0021	Filickc	micros	May 20	Li	--
Operatorovi zhori vlakno	58567	ETA Term	0.0002	Filickc	micros	May 20	--	--
Operator vypne stroj	58566	ETA Term	0.0019	Filickc	micros	May 20	--	--
▼ Operator si NEVSIMOL vysoku teplotu	58540	ETA	0.003	Filickc	micros	May 20	5€	--
Operatorovi zhorelo vlakno	58541	ETA Term	0.003	Filickc	micros	May 20	--	--
▼ Operator bol alarmovany o vysokej teplote	58537	ETA	0.99	Filickc	micros	May 20	Li	--
▼ Operator restartuje chladenie	58563	ETA	0.693	Filickc	micros	May 20	5€	--
Operator pokracuje v praci	58568	ETA Term	0.693	Filickc	micros	May 20	--	--
▼ Operator NERESTARTUJE chladenie	58564	ETA	0.297	Filickc	micros	May 20	Li	--
Operatorovi zhori vlakno	58570	ETA Term	0.0297	Filickc	micros	May 20	--	--
Operator vypne stroj	58569	ETA Term	0.2673	Filickc	micros	May 20	--	--

Obr. 6.2: Zobrazenie stromu udalostí v systéme RTC [screenshot obrazovky].

Typ chyby	Chyba	Pravdepodobnosť
HW	Detektor ma zlomený alebo prerušený optický kábel	0,001
	Detektor nie je pripojený ku zdroju elektrickej energie	0,001
	Zdroj nie je pripojený ku kontrolnému PC	0,025
	Nie je zapojený k zdroju elektrickej energie	0,025
	V komore pre vlákno je potrebné vytvoriť vakuum	0,2
	Vlákno je vyhorené	0,3
SW	Nastavený je SW detektor	0,3
	Nie je nastavené napätie zdroja	0,1
	Nie je nastavený prúd zdroja	0,2

Tabuľka 6.2: Tabuľka pravdepodobnosti chýb [vlastné spracovanie].



Obr. 6.3: Strom porúch prípadovej štúdie[vlastné spracovanie].

Summary	Id	Work Item Type	Probab	Owned By	Filed Against	Modifie	Children	Tags
▼ Obrázok su iba čierne pixely	58527	FTA	0.712	Filicko, D	microscope	May 23	Links	--
▼ Hardware	58528	FTA Or	0.112	Filicko, D	microscope	May 23	Links	--
▼ Detector	58531	FTA Or	0.002	Filicko, D	microscope	May 23	Links	--
detector ma zlomeny alebo prerušený optický kábel veduci ku kontrolnému PC	58559	FTA Term	0.001	Filicko, D	microscope	May 23	Links	--
Detector nie je pripojený ku zdroju elektrickej energie	58558	FTA Term	0.001	Filicko, D	microscope	May 23	Links	--
▼ Zdroj	58530	FTA Or	0.11	Filicko, D	microscope	May 23	Links	--
Nie je zapojený k zdroju elektrickej energie	58557	FTA Term	0.025	Filicko, D	microscope	May 23	Links	--
▼ Vlákno	58560	FTA And	0.06	Filicko, D	microscope	May 23	Links	--
Vlákno je vyhorené	58561	FTA Term	0.3	Filicko, D	microscope	May 23	Links	--
V komore pre vlákno je potreba vytvoriť vákuum	58562	FTA Term	0.2	Filicko, D	microscope	May 23	Links	--
Nie je pripojený ku kontrolnému PC	58556	FTA Term	0.025	Filicko, D	microscope	May 23	Links	--
▼ Software	58529	FTA Or	0.6	Filicko, D	microscope	May 23	Links	--
Nie je zapnutý zdroj zariadenia	58532	FTA Or	0.3	Filicko, D	microscope	May 23	Links	--
Nie je nastavené napätie	58534	FTA Term	0.1	Filicko, D	microscope	May 23	Links	--
Nie je nastavený prúd	58535	FTA Term	0.2	Filicko, D	microscope	May 23	Links	--
Nastavený je testovací detektor	58533	FTA Term	0.3	Filicko, D	microscope	May 23	Links	--

Obr. 6.4: Zobrazenie stromu porúch v systéme RTC [screenshot obrazovky].

Kapitola 7

Záver

Výsledkom tejto práce je fungujúce rozšírenie analýzy rizík pre systém RTC. Implementované metódy sú FTA a ETA. Po zadaní sú stromy týchto metód uložené v systéme a umožňujú servisným technikom a systémovým inžinierom zisťovať príčiny porúch, keďže tento systém používa celá spoločnosť. Vytvorené rozšírenie prešlo schvalovacím riadením a bude nasadené do reálnej prevádzky.

Toto rozšírenie je vyhovujúce pre dokumentačné účely a užívatelia majú možnosť vytvárať si stromy jednotlivých metód celkom intuitívne. Možnými vylepšeniami by mohli byť aj zlepšené vlastnosti a to, že užívatelia budú môcť nahráť strom v určitom formáte do systému, a ten by vytvoril samotný strom. Žiaľ realizovateľnosť takéhoto vylepšenia je otázná.

Práca sa zo začiatku venuje teórii managementu rizík a riziku konkrétne a snaží sa ukázať ako sa identifikujú riziká. Na túto časť nadväzujú metódy analýzy rizík. Po prejdení teórie ku rozhodovacím modelom sa presúva obsah k jednotlivým metódam analýzy rizík. Prvými metódami sú ETA a FTA. Metóda ETA sa používa pre identifikáciu nehôd, ktoré vznikajú. Spätnú analýzu zlyhania, je možné následne dohľadať spätne, podľa toho v akom stave nakoniec skončila. Metóda FTA je vhodná k nájdeniu kombinácii porúch zariadenia a ľudských chýb, ktoré môžu vyústiť v nehodu. Medzi poslednými popísanými metódami je metóda FMEA, ktorej účelom je identifikácia spôsobov porúch jednotlivých zariadení a systémov a potenciálnych účinkov na systém. Po nej je popísaná metóda HAZOP, ktorá identifikuje zdroje rizika a prevádzkové problémy. K záveru práce je popísaný systém RTC a jeho vyvojové prostredie, po ktorom nasleduje špecifikácia a návrh rozšírenia, ktoré bolo predmetom tejto diplomovej práce. Ako testovanie boli urobené dve prípadové štúdie, každá z nich bola zameraná na jednu implementovanú metódu.

Literatúra

- [1] Rational Team Concert. 2001-.
URL https://en.wikipedia.org/wiki/Rational_Team_Concert
- [2] *Management rizika projektu - Směrnice pro použití*. Český normalizační institut, 2002.
- [3] *Analýza stromu poruchových stavů (FTA)*. Český normalizační institut, 2007.
- [4] *Analýza možných způsobů a důsledků poruch (FMEA)*. Praha: Česká společnost pro jakost, Čtvrté vydání, 2008, ISBN 978-80-02-02101-8.
- [5] *Komentované vydání ONR 49002-1 Management rizik pro organizace a systémy*. Praha: Český normalizační institut, 2008, ISBN 978-80-7283-256-9.
- [6] *Techniky analýzy spolehlivosti - Analýza stromu událostí (ETA)*. Úrad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011.
- [7] Couger, J. D.: *Creative problem solving and opportunity finding*. Hinsdale, Ill.: Boyd, 1995, ISBN 08-770-9752-6.
- [8] Edwards, W.; Miles, R. F.; Winterfeldt, D. V.: *Advances in decision analysis*. New York: Cambridge University Press, 2007, ISBN 978-052-1682-305.
- [9] Fuchs, P.: *Využití spolehlivosti v provozní praxi*. Technická Univerzita v Liberci, 2002.
- [10] Fuchs, P.; Vališ, D.: *Metody Analýzy a řízení rizika*. Technická Univerzita v Liberci, 2004.
- [11] Hillson, D.; Simon, P.: *Practical project risk management*. Vienna, VA: Management Concepts, c2007, ISBN 978-1-56726-202-5.
- [12] Jr., R. F.: How are Epics, Stories and Tasks related to each other? 2011.
URL <https://theagileblueprint.wordpress.com/2011/02/21/how-are-epics-stories-and-tasks-related-to-each-other/>
- [13] Lientz, B. P.; Larssen, L.: *Risk management for IT projects*. Boston: Elsevier/Butterworth-Heinemann, c2006, ISBN 978-075-0682-312.
- [14] Pandian, C. R.: *Applied software risk management*. Boca Raton: Auerbach/Taylor&Francis, c2007, ISBN 9780849305245.
- [15] Psota, M.: *Softwarová podpora analýzy rizik*. Diplomová práce, Vysoké učení technické v Brně, Brno, 2013.

- [16] Schwalbe, K.: *Řízení projektů v IT*. Brno: Computer Press, 2007, ISBN 9788025115268.
- [17] Smejkal, V.; Rais, K.: *Řízení rizik ve firmách a jiných organizacích*. Praha: Grada, třetí vydání, c2010, ISBN 978-80-247-3051-6.
- [18] Vose, D.: *Risk analysis*. Hoboken, NJ: Wiley, třetí vydání, c2008, ISBN 0470512849.

Prílohy

Zoznam príloh

A Obsah CD

68

Príloha A

Obsah CD

- `src` - adresár obsahuje zdrojový súbor, exportovaný z prostredia eclipse.
- `text` - adresár obsahuje text práce.
- `text_src` - adresár obsahuje zdrojové kódy práce v prostredí \LaTeX .