

**Univerzita Pardubice
Fakulta ekonomicko-správní**

Analýza rizik metodou SFERA

Bc. Michael Čeliš

**Diplomová práce
2010**

zadávací list 1str

zadávací list 2strana

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 30. dubna 2010

Michael Čeliš

Poděkování

Rád bych touto cestou poděkoval všem, kteří mi pomáhali s napsáním této práce, zvláště pak vedoucímu mé diplomové práce doc. RNDr. Petru Linhartovi, Csc., za cenné rady a připomínky. Dále pak děkuji Ing. Ondřeji Svobodovi za pomoc při práci s programem SFERA.

ANOTACE

Obsahem teoretické části diplomové práce je definování pojmů z oblasti teorie rizika a obecný popis metod, které se používají při analýze rizika. V praktické části se práce zabývá analýzou rizika pomocí programu SFERA v podniku Synthesia, a. s.. Součástí práce jsou i návrhy na příslušná opatření.

KLÍČOVÁ SLOVA

riziko, analýza rizika, metody analýzy rizik, metoda SFERA

TITLE

The risk analysis by SFERA method

ANNOTATION

The theoretical part of the thesis contains definition of elementary notions from the area of theory of risk and description of the method using in risk analysis. My thesis deals with risk analysis by SFERA method in practical. Proposals of relevant precautions are included in my thesis, too.

KEYWORDS

risk, risk analysis, analysis methods, SFERA method

Obsah

Obsah	7
Úvod	13
1 Teorie rizika	15
1.1 Základní pojmy.....	15
1.1.1 Hrozba.....	15
1.1.2 Zranitelnost.....	15
1.1.3 Riziko.....	15
1.1.4 Krize.....	21
1.1.5 Krizové řízení.....	21
1.1.6 Krizový plán.....	21
1.1.7 Mimořádná událost.....	22
2 Analýza rizik obecně	24
2.1 Analýza rizik.....	24
2.2 Metody analýzy rizik.....	24
2.2.1 Metody kvalitativní.....	25
2.2.2 Metody kvantitativní.....	25
2.3 Nejužívanější metody analýzy rizik.....	27
2.3.1 FMEA.....	27
2.3.2 FMECA.....	29
2.3.3 HAZOP.....	29
2.3.4 HACCP.....	31

2.3.5	Bezpečnostní audit	31
2.3.6	Kontrolní seznam	32
2.3.7	ETA	34
2.3.8	FTA	36
2.3.9	PHA	39
2.3.10	RR.....	40
2.3.11	HRA.....	40
2.3.12	CPQRA.....	41
2.3.13	QRA.....	42
2.3.14	What – If Analysis.....	42
2.3.15	CCA.....	43
2.3.16	Matice rizik a kritéria přijatelnosti rizika	44
2.3.17	SFERA.....	45
3	Analýza rizik v Synthesia, a. s. metodou SFERA	46
3.1	Základní údaje o společnosti Synthesia a. s.....	46
3.1.1	Areál společnosti Synthesia, a.s.	47
3.2	Historie společnosti ^[26]	48
3.3	Analýza rizik ve společnosti Synthesia, a. s.	49
3.3.1	Přehled rizik	49
3.4	Zadání dat do programu SFERA	53
3.4.1	SFERA.....	53
3.4.2	Matice.....	54

3.4.3	Vztahy	55
3.4.4	Průvodce zadáním dat	56
3.4.5	Hodnoty prvků.....	57
3.4.6	Výsledky.....	59
3.4.7	Soubory projektu	60
3.5	Vyhodnocení výsledků	60
3.6	Zhodnocení metody SFERA.....	62
3.7	Doporučení	62
Závěr	63

Seznamy

Seznam zkratk

CCA	analýza příčin – následků
CPQRA	kvantitativní analýza rizika chemického procesu
ETA	analýza stromu událostí
FMEA	analýza selhání a jejich dopadů
FMECA	analýza selhání a jejich kritických dopadů
FTA	analýza stromu poruch
HACCP	analýza nebezpečí či ohrožení analýzou kritických bodů
HAZOP	analýza nebezpečí či ohrožení a provozuschopnosti
HRA	analýza spolehlivosti lidského činitele
KLPOD	klimatické podmínky
KNBZL	kontakt s nebezpečnou látkou
MIKPO	mikroklimatické podmínky
MONTZ	montáž
NEOSV	nedostatečné osvětlení
OOCIN	ohrožení opakovanou činností
PADVP	pád z výšky, pád předmětu
PHA	předběžné posouzení nebezpečí
PUPVY	požár, únik plynu, výbuch
SMAUG	Seriousness, Manageability, Acceptability, Urgency, Growth

QRA	analýza kvantitativních rizik procesu
RR	relativní klasifikace
SBU	obchodní jednotka
SFERA	system, fenomen, efekt, riziko, analýza
SNIPR	snížená průchodnost
TRMAN	transport, manipulace
UKCHN	uklouznutí, klopýtnutí, chybné našlápnutí
ZASEN	zasažení energiemi

Seznam obrázků

Obrázek 1: Vztahy v teorii rizik ^[8]	17
Obrázek 2: Činnosti managementu rizik ^[9]	22
Obrázek 3: Organizace HAZOP ^[8]	30
Obrázek 4: Kontrolní seznam	33
Obrázek 5: Strom událostí ^[13]	36
Obrázek 6: Strom poruch	39
Obrázek 7: Matice rizik ^[13]	44
Obrázek 8: Matice rizik ^[13]	45
Obrázek 9: Poloha areálu Synthesia, a. s.	48
Obrázek 10: Dekompozice prvků ^[28]	54
Obrázek 11: Kontingenční tabulka	55
Obrázek 12: Okno vztahy	56
Obrázek 13: Okno Průvodce zadáním dat	57
Obrázek 14: Okno Hodnota prvků	58
Obrázek 15: Výsledný strom	59
Obrázek 16: Procentuální vliv sledovaných rizik na systém	61

Seznam tabulek

Tabulka 1: Rizika dle úrovně nejistoty ^[9]	19
Tabulka 2: Vývojové fáze rizika ^[10]	20
Tabulka 3: Tabulka pro metodu FMEA ^[8]	28
Tabulka 4: Tabulka pro metodu HACCP	31
Tabulka 5: Přehled rizik	51
Tabulka 6: Kritéria rizik	52
Tabulka 7: Výsledné hodnoty analýzy	60

Úvod

Vstupujeme do 21. století. 20. století bylo svědkem největšího a nejdynamičtějšího vědeckotechnického pokroku v dějinách lidstva a vše nasvědčuje tomu, že tento trend bude pokračovat. Tento fakt člověku přináší mnoho užitku a ulehčuje mu život, ale na druhé straně sebou přináší i řadu rizik. Z důvodu vědecké evoluce se lidstvo rozhodlo přetvářet přírodu k obrazu svému. Ovšem člověk není na Zemi sám. Je potřeba si uvědomit, že jsme součástí jistého společenství. Jsme pouze jedním dílem z pomyslné skládačky, kde všechny dílky do sebe neomylně zapadají, a pokud se nějaký dílek ztratí nebo je zaměněn, dochází k problémům. V důsledku stále se měnících podmínek (technických, ekonomických, přírodních, politických) lidská činnost vždy neprobíhá podle plánu a vzniká tady prostor k řadě negativním jevům – rizikům. Je třeba si uvědomit, že riziko není jen nějaký údaj uvedený na papíře, ale bohužel se jedná o reálnou hrozbu.

Je tedy nezbytné tato rizika a jejich následky minimalizovat. Prioritou je ochrana lidských životů, ale také majetku a životního prostředí. Základním kamenem se stává prevence. Ideálním stavem by nastala v případě eliminování všech hrozících rizik. Ovšem tato situace se vyskytuje pouze v rovině našich přání a snů. Vznikají proto stále nové postupy a metody jak rizika identifikovat (bez rozpoznání rizika nejsme schopni se proti němu účinně bránit), určit jejich míru a rozsah případných škod, a poté učinit opatření vedoucí k minimalizaci škod. Touto oblastí se podrobně zabývá analýza rizik.

Tato diplomová práce má za cíl seznámit čtenáře právě s touto oblastí a to pomocí tří částí:

První část práce nazvaná Teorie rizika je určena k obeznámení čtenáře s problematikou v teoretické rovině. Jsou zde vysvětleny základní pojmy jako riziko, mimořádná událost nebo krizové řízení, důležité pro pochopení celé problematiky. Druhá část s názvem Analýza rizik obecně se zaměřuje na rozpracování pojmu analýza rizik. Je zde podrobně popsáno, čím se analýza zabývá a jaké může mít podoby. Dále je zde čtenář seznámen s konkrétními metodami, které jsou v praxi nejčastěji používány.

Ve třetí nazvané Analýza rizik v Synthesia a. s. metodou SFERA je práce zaměřena na podrobné zpracování rizik v jednom z největších chemických podniků v Pardubickém kraji. Jako nástroj pro tuto analýzu byl zvolen program SFERA. Čtenářovy je zde představena společnost (její předmět činnosti, historie, struktura) a dále rizika, která ohrožují provoz tohoto podniku. Je zde provedena podrobná analýza již výše zmíněným softwarem a uvedeny výsledky a jejich interpretace.

Cílem této práce je zanalyzovat rizika v jedné z významných společností v Pardubickém kraji, která působí v chemickém průmyslu, kde se vyskytuje relativně vysoký rizikový potenciál, a z výsledků provedené analýzy vyvodit logické závěry.

1 Teorie rizika

1.1 Základní pojmy

1.1.1 Hrozba

Hrozbou je myšleno nebezpečí, které může poškodit chráněné zájmy. Jedná se o sílu, aktivitu nebo osobu, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu [5]. Hrozba se také může vyjádřit, jako součin pravděpodobnosti výskytu počáteční události a pravděpodobnosti selhání ochranných a bezpečnostních systémů [8].

Základní charakteristikou hrozby je její úroveň. Úroveň hrozby se hodnotí podle následujících faktorů:

- Nebezpečnost: schopnost hrozby způsobit škodu.
- Přístup: pravděpodobnost, že se hrozba svým působením dostane k aktivu (získá k němu přístup). Jednou z forem vyjádření může být i frekvence výskytu hrozby.
- Motivace: zájem iniciovat hrozbu vůči aktivu. Odhad motivace spočívá v pochopení skupinových a národních záměrů i záměrů jednotlivců, jejich cílů a politiky - to vše se analyzuje s ohledem na předchozí podmínky a činnost těchto ohrožovatelů (útočníků). Odhad motivace napomáhá při tvorbě expertních stanovisek a odhadů hrozeb [1].

1.1.2 Zranitelnost

Zranitelnost vyjadřuje míru citlivosti vůči působení hazardu a je součtem faktorů vystavení riziku a neschopností toto vystavení zvládat. Dopad můžeme vyjádřit jako součin důsledku události a zranitelnosti a protiopatření jako činnost vedoucí ke snížení zranitelnosti aktiva.

1.1.3 Riziko

Pojem riziko byl poprvé použit údajně v 17. století, kdy tímto pojmem označovali italská mořeplavci objekty na moři, kterým se bylo potřeba vyhnout.

Později se tímto výrazem mělo na mysli jakékoli vystavení nepříznivým okolnostem. V dnešní době výraz riziko chápeme jako možnou nežádoucí akci nebo změnu, která může nastat při vykonávání činnosti člověkem nebo skupinou lidí. Riziko je tedy pravděpodobnost, že tyto okolnosti nastanou.

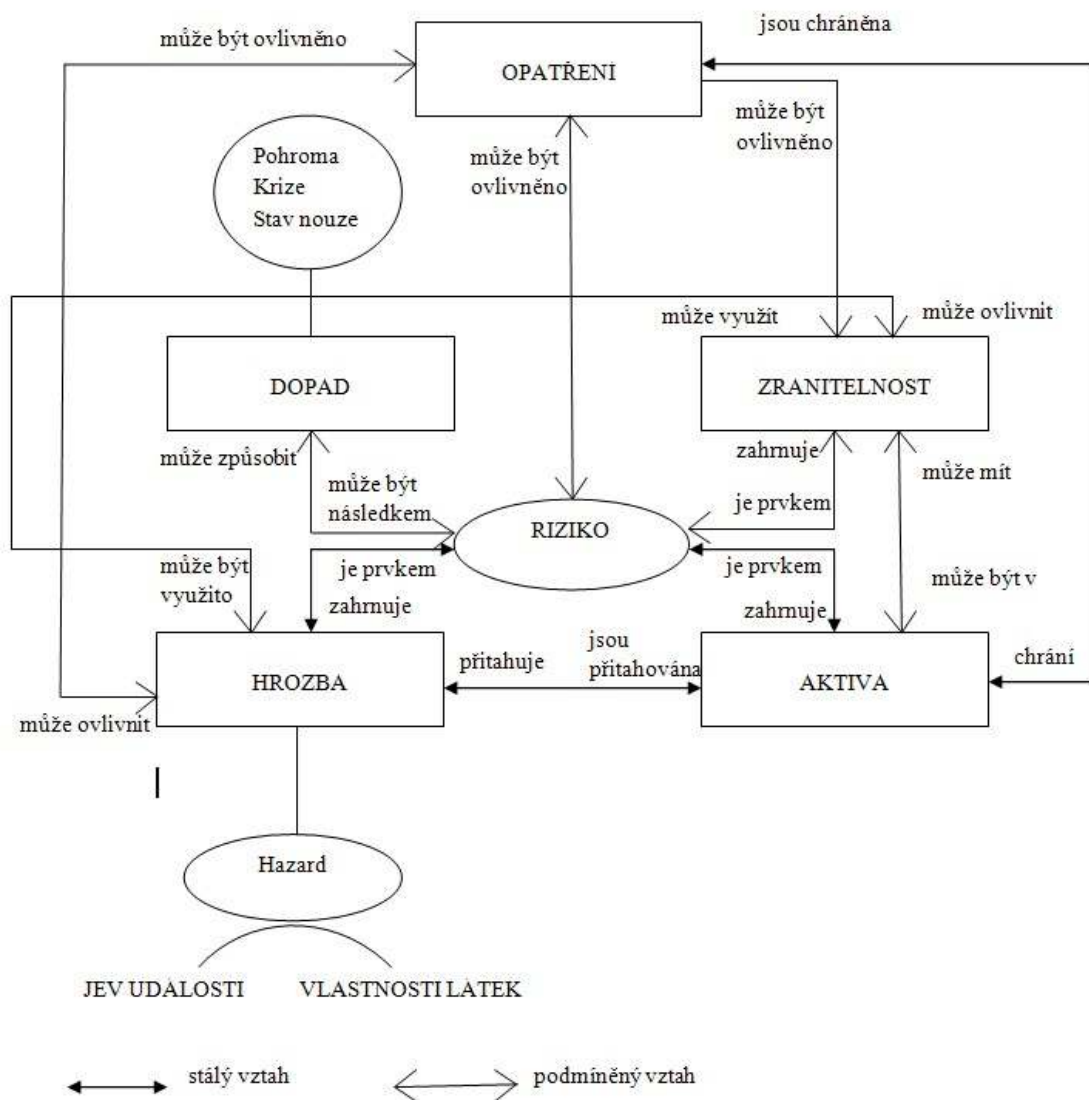
Pro pojem riziko existuje více definic ^[1]:

- Pravděpodobnost či možnost vzniku ztráty, obecně nezdaru.
- Variabilita možných výsledků nebo nejistota jejich dosažení.
- Odchýlení skutečných a očekávaných výsledků.
- Pravděpodobnost jakéhokoliv výsledku, odlišného od výsledku očekávaného.
- Situace, kdy kvantitativní rozsah určitého jevu podléhá jistému rozdělení pravděpodobnosti.
- Nebezpečí negativní odchylky od cíle (tzv. čisté riziko).
- Nebezpečí chybného rozhodnutí.
- Možnost vzniku ztráty nebo zisku (tzv. spekulativní riziko).
- Neurčitost spojená s vývojem hodnoty aktiva (tzv. investiční riziko).
- Střední hodnota ztrátové funkce.
- Možnost, že specifická hrozba využije specifickou zranitelnost systému.

Riziko můžeme obecně popsat následující rovnicí:

$$\mathbf{RIZIKO = HROZBA \times ZRANITELNOST \times DOPAD / OPATŘENÍ}$$

Jednotlivé vztahy a souvislosti jsou zobrazeny na obr. 1.



Obrázek 1: Vztahy v teorii rizik ^[8]

Při vyhodnocení rizik se jako základní, úvodní kritéria používají kritéria se zkratkou SMAUG. Jedná se o zkratku prvních písmen úhlů pohledů na konkrétní riziko.

- *Seriousness* (nebezpečnost, závažnost, kritičnost) - nejvyšší hodnocení mají rizika, která nejvíce ovlivňují
- *Manageability* (ovladatelnost, zvladatelnost) - rizika dobře zvladatelná mají nejvyšší hodnocení
- *Acceptability* (přijatelnost) - nejvyšší hodnocení mají rizika, která jsou málo přijatelná z hlediska sociálního a politického

- Urgency (naléhavost) rizika, o nichž panuje přesvědčení, že vyžadují bezodkladná řešení k jejich stabilizaci, mají nejvyšší hodnocení
- Growth (nárůst, eskalace) - nejvyšší hodnocení mají rizika, která nejrychleji eskalují v nežádoucích dopadech ^[8]

Podle těchto kritérií pak můžeme rizika dělit do různých skupin:

➤ dle ovlivnitelnosti

- Ovlivnitelné – výskyt rizika je ve značné míře možno omezit (podnikatelské, finanční)
- Neovlivnitelné – jedná se rizika z „vyšší moci“, kterým je potřeba se podřídit a akceptovat je (přírodní vlivy) ^[17]

➤ dle závažnosti

- kritické,
- netolerovatelné,
- respektovatelné,

kde je hlavním kritériem velikost dopadu na chráněné zájmy a z toho plynoucí preventivní opatření.

➤ dle úrovně nejistoty jsou rizika rozdělena v následující tabulce na:

Úroveň nejistoty	Charakteristika	Příklady
Nulová úroveň	výsledek může být přesně předpovězen, výsledky jsou identifikovány	fyzikální zákony
První úroveň (objektivní)	výsledky jsou identifikovány a pravděpodobnosti známy	hry karetní, hry s kostkami
Druhá úroveň (subjektivní)	výsledky jsou plně identifikovány, pravděpodobnosti neznámé	požár, dopravní nehoda

Třetí úroveň	výsledky nejsou plně identifikovány, pravděpodobnosti jsou neznámé	kosmický výzkum, genetický výzkum
--------------	--	-----------------------------------

Tabulka 1: Rizika dle úrovně nejistoty^[9]

Největší význam mají 2. a 3. úroveň. Zde je na první pohled zřejmé, že kontaktní omezení mohou posunout 3. úroveň na 2. úroveň nejistot. Obecně vzato, redukce nejistoty závisí na množství a typu informace, která je k dispozici z možných výsledků a odhadů jejich pravděpodobnosti. Dalším zdrojem této redukce je komunikace v rámci managementu organizace a jeho aktivit^[9].

➤ dle oblastí, kterých se riziko týká ^[12]

- politická a teritoriální,
- ekonomická - makroekonomická a mikroekonomická, například tržní, inflační, kurzovní,
- úvěrová, obchodní, platební a pod.,
- bezpečnostní,
- právní a spojená s odpovědností za škodu,
- předvídatelná a nepředvídatelná,
- specifická - například pojišťovací, manažerská, spojená s finančním trhem, odbytová, rizika inovací apod,

Riziko se vyvíjí podle L. Šimáka ve 3 hlavních fázích. Každá z těchto fází se dále člení na několik mezifází, kde na každou z nich krizový management reaguje určitými úkony.

Tyto fáze, společně s chováním krizového managementu, nám popisuje následující tabulka.

Vývojová fáze krize	Opatření uskutečňované krizovým managementem	
	Řídící složky krizového managementu	Výkonné prvky
1. PRERIZIKO		
DIVERGENCE (odchylka)	monitorování	pohotovost dispečerských míst
TURBULENCE (nepravidelnost)	analýza informací	pohotovost základních sil
OSCILACE (kmitání)	předběžná opatření	vyrozumění dalších sil
CHAOS (neuspořádané, náhodné procesy)	aktualizace krizových plánů	přípravenost na zásah
2. RIZIKO		
ELEVÁCE (počátek krize)	organizace zásahu	výjezd a nasazení
KULMINACE (vyvrcholení krize)	řízení záchranných prací	vykonávání záchranných prací
DEPRESE (ukončení krize)	koordinace záchranných a likvidačních prací	záchranné a likvidační práce
3. POSTRIZIKO		
DEPRIVACE (stav nedostatku základních potřeb)	organizace odsunu	zabezpečení evakuovaných osob
REPARACE (uvedení do původního stavu)	příprava obnovy	vyčlenění sil a prostředků na obnovu
RENOVACE (obnova)	řízení prvotní obnovy	vykonávání obnovovacích prací
REFORMACE (restrukturalizace)	řízení obnovy na nové podmínky	zvyšování odolnosti systému

Tabulka 2: Vývojové fáze rizika ^[10]

1.1.4 Krize

Odvozeno od slova „Krizis“, které pochází z řeckého slova „krino“ tedy rozhodnutí neodvolatelného typu, které vyjadřovalo naléhavou potřebu, pocitování nejistoty, hledání záchrany nebo zabránění neštěstí. Jedná se o rozhodný okamžik nebo časový úsek, po němž může následovat zásadní změna ve vývoji daného děje nebo systému. Je to složitý, těžko překonatelný a nebezpečný stav nebo průběh dějů v životě společnosti, v přírodě, v činnosti technických prostředků a v technologických procesech, jehož negativní důsledky mohou vážně ohrozit jejich funkci, případně i existenci. Zároveň se tento pojem používá jako obecné označení všech krizových jevů.

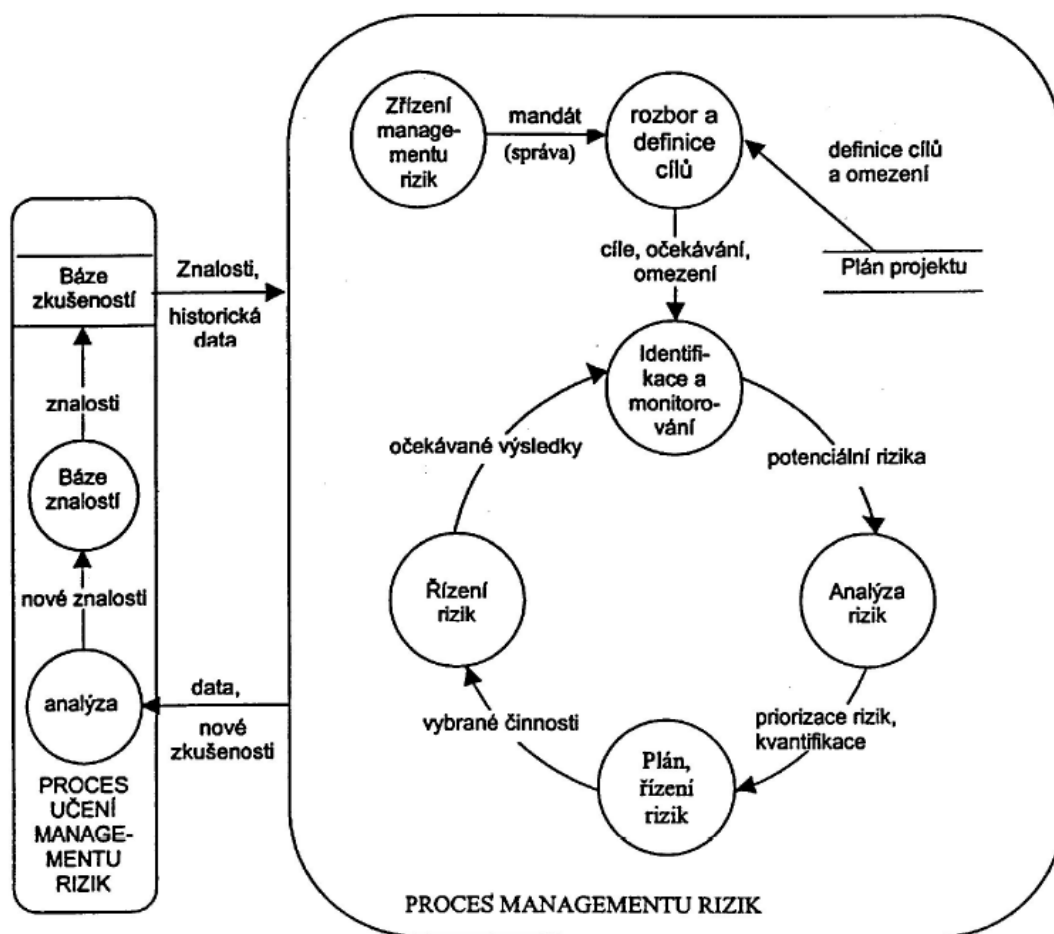
1.1.5 Krizové řízení

Krizovým řízením se podle zákona č. 240/2000 Sb, o krizovém řízení a o změně některých předpisů rozumí souhrn řídicích činností věcně příslušných orgánů zaměřených na analýzu a vyhodnocení bezpečnostních rizik, plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s řešením krizové situace^[24].

Je to souhrn vědeckých poznatků, odborných postupů a aplikačních nástrojů preventivních, rozhodovacích a technologických opatření napomáhajících řešit krizové situace. Zahrnuje přípravu a zajištění krizových a havarijních plánů ochrany a záchrany života a zdraví obyvatelstva, ochrany životního prostředí, duchovních hodnot a ekonomiky, jako základních hodnot státu.

1.1.6 Krizový plán

Krizový plán je souhrnný plánovací dokument, kterým orgány krizového řízení plánují své věcné a územní působnosti, opatření a postupy pro případ řešení krizové situace, která dosáhla takové úrovně, že k jejímu řešení je nezbytné použít mimořádná opatření. Je zpracováván, aktualizován a ověřován mimo období hrozby vzniku KS příslušnými orgány krizového řízení v rozsahu vycházejícím z jejich věcné působnosti. Náležitosti a způsob zpracování upravuje nařízení vlády č. 462/2000 Sb., ve znění nařízení vlády č. 36/2003 Sb. v § 15 a 16.^[17]



Obrázek 2: Činnosti managementu rizik^[9]

1.1.7 Mimořádná událost

Mimořádná událost je závažná, časově obtížné předvídatelná a prostorově ohraničená příhoda, způsobená vlivem živelné pohromy, technické nebo technologické havárie, provozní poruchy, případně úmyslného jednání člověka, která vyvolala narušení stability systému nebo probíhajících dějů a činností, ohrožuje životy a zdraví osob, hmotné a kulturní statky či životní prostředí. Přináší s sebou změny kvality prvků systému, a tím i změny kvality vztahů a vazeb mezi nimi. Uvedené změny mají velmi často rozkladný charakter a jsou tedy nežádoucí, výjimečně se v nich mohou objevovat i rozvojové prvky a tendence. Mimořádné události jsou tedy součástí krizových jevů, případně mohou představovat přímo jejich spouštěcí mechanismus.

Mimořádné události lze rozdělit dle jejich vlivu na systém:

- kladná mimořádná událost - podílí se na zvýšení kvalitativní úrovně systému (Hmotnostně, energeticky, informačně,...), její rozsah a dopad na systém nebyl dopředu předpokládán, případně plánovaný a vyvolává problémy při provádění rutinních činností,
- záporná mimořádná událost - způsobuje zastavení činnosti, případně zánik původního systému tím, že přeruší vazby mezi jeho prvky, v krajním případě způsobí jejich plnou fragmentaci (rozpad) nebo zničení.^[10]

2 Analýza rizik obecně

2.1 Analýza rizik

Analýza rizika je prvním a velice důležitým krokem v komplexním zabezpečení prevence rizik. První analýzy rizika vznikali ve druhé polovině minulého století především v USA a ve vyspělých západoevropských zemích. Analýzy rizika jsou zaměřeny na identifikaci a kvantifikaci zdrojů ohrožujících životy a zdraví osob, životní prostředí a majetek, které souhrnně můžeme chráněnými aktivy. Jsou východiskem pro management organizace a vytvářejí podklady pro rozhodovací proces.

Základem je výběr vhodné metody (nebo kombinaci více metod), protože již výběr špatné metody, může výrazně ovlivnit výsledek analýzy. Proto už tento krok vyžaduje tým zkušených specialistů. Provedení analýzy rizika je pak vysoce náročná specializovaná činnost, obvykle časově náročná, vyžadující prohlídky hodnocené technologie, technologických a jiných podmínek, a hlavně kvalifikovanou spolupráci s technologií a dalšími odborníky hodnocené technologie. Jedním z nejdůležitějších faktorů, které mohou ovlivnit správnost a kvalitu analýzy, je konkrétnost, pravdivost, komplexnost a objektivnost ověřených datových souborů o systému, který je předmětem zkoumání.

2.2 Metody analýzy rizik

Na výběr konkrétní metody resp. metod, má vliv mnoho faktorů:

- charakter objektu nebo zařízení,
- provozované technologie,
- druhy nebezpečných chemických látek nebo přípravků,
- množství nebezpečných chemických látek nebo přípravků,
- okolní infrastruktura mimo areál provozovatele,
- zranitelnost okolí (například školy, dětská hřiště, apod.)
- požadovaný cíl analýzy rizika,
- časový prostor na zpracování analýzy rizika,

- finanční prostředky na krytí analýzy rizika (pokud se objednává u odborné firmy).^[16]

V zásadě lze metody analýzy rizik rozdělit na dvě základní - metody kvalitativní a metody kvantitativní.

2.2.1 Metody kvalitativní

Používá nečíselných údajů k popisu rozsahu možných následků a pravděpodobností, že se tyto následky přihodí. Mohou se používat různé bodové škály, hrozby mohou být vyjádřeny pravděpodobností, nebo mohou být popsány slovy (nízké, střední, vysoké riziko). Z těchto důvodů jsou tyto metody více subjektivní a záleží zde na zkušenostech a znalostech hodnotitele. Kvalitativní analýza se používá při prvotní identifikaci rizik, která jsou dále podrobněji zkoumána, nebo v případech, kde máme nedostatek relevantních číselných údajů. Často se vychází z vypracovaných dotazníků či anket a z hodnocení expertů a specialistů z daného oboru.

2.2.2 Metody kvantitativní

U těchto metod se používají číselné hodnoty pro následky i jejich pravděpodobnosti, které stanoví pomocí údajů získaných z různých zdrojů (statistické ročenky, účetnictví, ...). Základem je používání matematických a statistických metod. Výsledná kvalita analýzy závisí především na přesných a úplných datech.

Skládá se obvykle z těchto kroků:

1. identifikace a definice možných nebezpečných událostí (scénářů havárií) a jejich možných konečných stavů;
2. odhad pravděpodobnosti výskytu možných konečných stavů nebezpečných událostí;
3. výpočet následků všech možných konečných stavů všech nebezpečných událostí;
4. kombinace pravděpodobností a následků pro odhad individuálního a společenského rizika.^[5]

Analýzy můžeme dále rozdělit dle dalších kritérií na ^[2]:

- apriorní analýza
Pracuje s jevem, který je zdrojem nebezpečí, již v minulosti (třeba zcela nedávně) nejméně jednou nastal. Známe tedy jeho povahu, je to jev skutečný, není vykonstruovaný, a víme, že k němu příslušná událost nastat může. Jev je tedy předem, tj. a priori, znám, i když nejsou přesně a podrobně známy jeho vlastnosti.
- aposteriorní analýza
Zabývá se jevy a událostmi, o nichž se na základě rozumové (nikoliv citové) úvahy pouze domnívá, že mohou nastat, ani by zatím v minulosti někdy nastaly. Odhaduje tedy riziko na základě odhadu chování jevů, jež nastanou po analýze, tj. a posteriori.
- absolutní analýza
Cílem je získat přesné hodnoty rizika u zkoumaného systému jako základ pro rozhodování
- relativní analýza.
Někdy se také označuje jako preferenční nebo komparativní analýza. Již podle těchto názvů lze usoudit, že se tento druh analýzy používá při výběru z více variant (např. projektů).

Analýza rizik si můžeme rozdělit na řadu dílčích kroků, které bychom mohli jmenovat v následujícím pořadí:

- identifikaci aktiv - vymezení posuzovaného subjektu a popis aktiv, které vlastní,
- stanovení hodnoty aktiv - určení hodnoty aktiv a jejich význam pro subjekt, ohodnocení možného dopadu jejich ztráty, změny či poškození na existenci či chování subjektu,
- identifikaci hrozeb a slabin - určení druhů událostí a akcí, které mohou ovlivnit negativně hodnotit *aktiv*, *určení* slabých míst subjektu, které mohou umožnit působení hrozeb,
- stanovení závažnosti hrozeb a míry zranitelnosti - určení pravděpodobnosti výskytu hrozby a míry zranitelnosti subjektu vůči dané hrozbě^[1].

2.3 Nejužívanější metody analýzy rizik

V dnešní době jsou používány desítky různých analytických metod. V mé práci uvádím ty metody, které jsou nejčastěji používány.

2.3.1 FMEA

Failure Mode and Effect Analysis

(analýza selhání a jejich dopadů)

Tato metoda se užívá ke kvalitativnímu zkoumání potencionálních režimů poruch a k určení vlivů, které mohou narušit sledovaný systém. Jde o dopřednou metodu zabývající se poruchou jednoho prvku. Analytická metoda FMEA se často kombinuje s dotazníky typu kontrolních seznamů (Check List).

Metodu FMEA obecně rozdělujeme do dvou kategorií ^[19]:

- a) FMEA výrobku (angl. design FMEA)
- b) FMEA procesu (angl. process FMEA).

Jedná se o induktivní metodu tvrdého, určitého typu, založenou na principu modelování souvislostí popisujících vztah „příčina - důsledek" nebo „selhání - důsledek".

Jaroslav Mozga a Miloš Vítek uvádějí ve své knize Udržitelný rozvoj a řízení rizik, pohrom a krizí (2002), že při metodě FMEA se postupuje v 9 následujících krocích^[8]:

- Stanovení, vymezení systému
- Formulace problémů, které se mají analyzovat
- Volba přístupu FMEA – u této metody existují dva přístupy, které se mohou kombinovat. Prvním z nich je tzv. „hardwarový“ (zdola nahoru), který je znázorněn stromem, jenž je složen z úrovně prvků, součástí, subsystému a kořenem stromu, který tvoří celý systém. Zde se analýza zaměřuje na poruchy prvků na nejnižší úrovni. V případě složitých nebo obtížně strukturovatelných systémů je však spíše neúčinný. Druhý, tzv. funkční přístup (shora dolů) je také znázorňován stromem, jehož kořenem je systém, který se poté dělí

na sub funkce, sub-sub funkce atd. Tento přístup je více cílený a je vhodný pro nejednoznačně definované systémy.

- Systém se dělí podle předchozího kroku
- Určení potencionálních forem poruch pro prvky systému
- Vyhodnocení způsobů a forem poruch – každá porucha se vyhodnocuje pomocí otázek:
 - Jaký je projev poruchy ?
 - Jaké jsou možné příčiny poruchy ?
 - Jak může být porucha objevena / detekována ?
 - Jak porucha ovlivní systém ? (jaké jsou následky poruchy)
 - Je tento stav přijatelný, co je potřeba udělat ?

Nakonec se pro každý způsob poruchy sestaví tabulka.

Způsob/forma poruchy:									
Provozní režim	Zjišťování poruch	Vlivy			Závažnost	Příčiny	Předvídatelnost poruch	Opatření	Doporučení
		M	V	K					

Tabulka 3: Tabulka pro metodu FMEA^[8]

kde M je místní vliv, V je vliv na vyšší úrovni a K je koncový vliv.

- Použití kvantifikace, je-li to nezbytné – určují se pravdě podobnosti a míra rizika.
- Změna přístupu analýzy, je-li to nezbytné
- Využití výsledků pro rozhodování

Tato metoda není pro analýzu území příliš vhodná a s jejím praktickým využitím se lze setkat u technologických celků (mechanické systémy, chemické rozvody, elektrické sítě apod.). Charakter hledaných příčin je všeobecného charakteru (poruchy, lidský faktor, živelní události apod.). Mezi další nevýhody patří to, že se často mohou přehlédnout chyby hodnotitele. Tato metoda je zaměřena pouze na jednu iniciační událost, takže je obtížné získat rozložení pravděpodobností poruch.

2.3.2 FMECA

Failure Mode and Effect Criticality Analysis

(analýza selhání a jejich kritických dopadů)

Metoda FMECA je zařazována mezi kvantitativní metody. Je odvozenou analytickou metodou, která řeší postupy, jejichž cílem je klasifikace poruch do škály jejich kritičnosti. FMECA je týmově orientovaná metoda k minimalizaci rizik vývojových a plánovacích procesů a vyžaduje interdisciplinární spolupráci všech zúčastněných útvarů již od samého počátku prací. Hledá se relativní míra důsledků projevené poruchy a její opakovatelnost. Podobně jako u metody FMEA jsou u každého prvku analyzovaného systému odhadnuty potenciálně možné druhy všech poruchových stavů. Je určena škála selhání každého poruchového stavu. Je využíván induktivní postup řešení odzodla nahoru. Součástí analýzy je ověřování výsledků metodou FMECA zpětnou vazbou o kontrolující chování analyzovaného systému v různých technologických stavech. Zpětnou vazbou se hlídá bezporuchovost a opatření během života analyzovaného systému^[5].

2.3.3 HAZOP

HAZard and Operability study

(analýza nebezpečí či ohrožení a provozuschopnosti)

Metoda HAZOP je v současnosti uznávaným evropským standardem. Umožňuje při správném použití identifikovat nebezpečné stavy, které se mohou vyskytnout a následně je vyhodnotit. Autor metody HAZOP ve své původní práci charakterizuje tuto metodu jako spojení dvou základních postupů. Jako první lze uvést "studii provozuschopnosti" (Operability Study), což je v podstatě identifikace nebezpečných situací. Na ni navazuje Hazard Analysis, což je vyhodnocení rizika. Metoda vychází z pravděpodobnostního hodnocení hazardů jako zdrojů rizik. Jejím principem je expertní týmová práce často využívající brainstormingové a brainwritingové přístupy. Při této metodě se rozsáhlý a složitý systém rozděluje na menší části, v nich se hledají případné odchylky od normálu a navrhuje se způsoby jejich řešení.

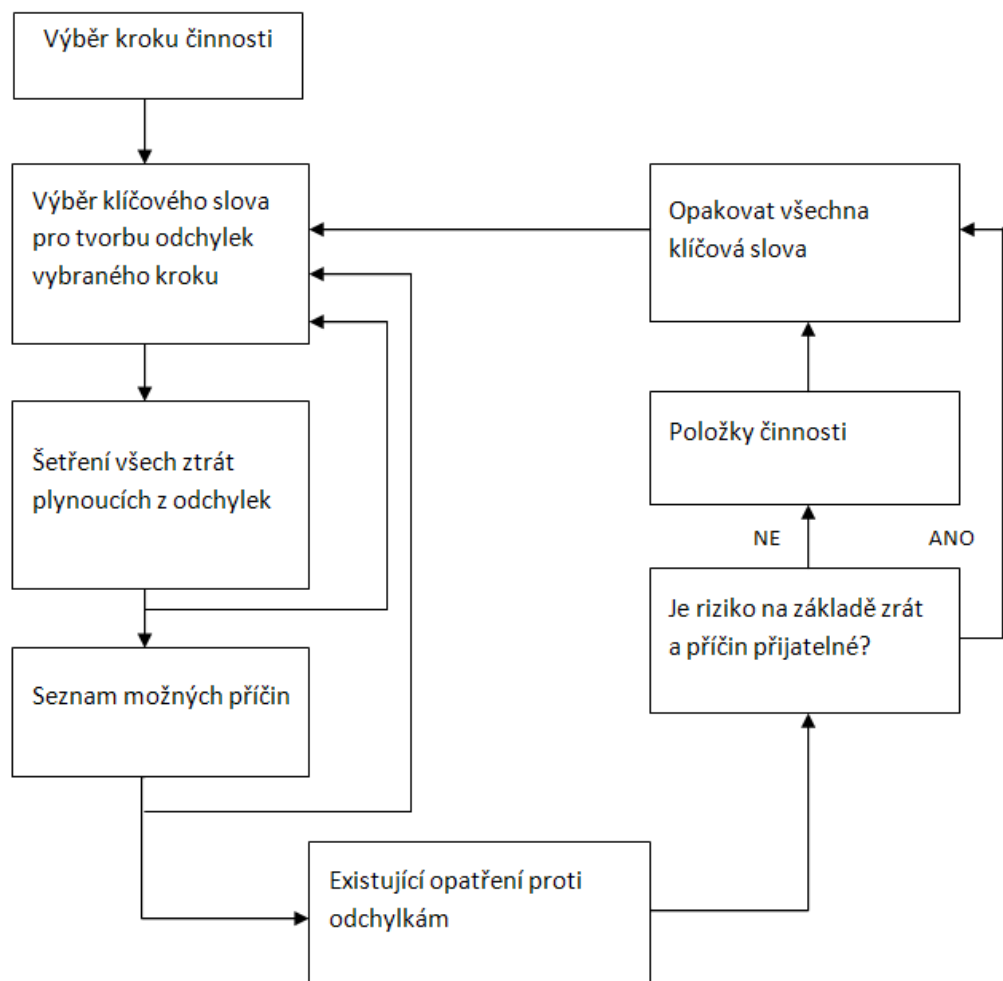
Pro provedení kvalitní analýzy je potřeba splnit 3 základní podmínky:

- jasné vymezení rozsahu a stanovení cílů studie,

- znalosti a schopnosti vedoucího studie, kvalita členů odborného týmu,
- dostatek času.

Metoda se provádí v těchto krocích^[8]:

- Definice systému a jeho hranic
- Specifikace oblastí zájmu zkoumání (bezpečnost provozu a práce, ekonomické dopady, vliv na životní prostředí)
- Rozložení systému a určení možných odchylek
- Organizace HAZOP



Obrázek 3: Organizace HAZOP^[8]

- Využití výsledků a rozhodování

Za nedostatek této metody je označován fakt, že se poruchy obtížně řadí podle závažnosti jejich vlivů, a také se nestuduje efektivnost, s jakou jsou prováděna opravná opatření.

2.3.4 HACCP

Hazard Analysis and Critical Points

(analýza nebezpečí či ohrožení analýzou kritických bodů)

Jedná se o odvozenou metodu od metody HAZOP. Metoda je vyvinuta především pro účely potravinářského průmyslu se zaměřením na fyzikální, chemické a biologické hazardy nejčastěji ve směru k zdravotní nezávadnosti potravin. Tato potřeba vyplývá ze zákona 274/2003 Sb. o ochraně veřejného zdraví, který ukládá od 1. 5. 2004 všem provozovatelům služeb společného stravování zavedení systému kritických bodů HACCP. Opatření navazují na ISO 22000 a na systém běžně používaných postupů a norem, které ošetřují systém managementu kvality (ISO 9001). Metoda určuje kritické kontrolní body pro snížení hazardů. Kritické limity klasifikují přijatelné a nepřijatelné podmínky vyžadující opakované monitorování. V tabulce x je znázorněna pracovní forma tabulky metody HACCP^[8].

Detailní popis hazardu:					
Postup monitorování	Kritické limity	Četnost	Nápravné akce	Odpovědnost	Dokumentace monitorování

Tabulka 4: Tabulka pro metodu HACCP^[8]

2.3.5 Bezpečnostní audit

Safety Audit

Tato metoda se řadí mezi kvalitativní. Jedná se o jednu z historicky nejstarších technik. Základem je kontrola a posuzování kritických oblastí ve sledovaném systému. Je používán připravený seznam otázek a matice pro ohodnocení rizik.

Základní důvody pro systémový audit lze rozdělit následovně:

- Účel detektivní – zaznamenáváme vybrané události s tím, že záznamy uchováváme pro účely dohledání příčin zjištěných bezpečnostních incidentů někdy v budoucnu. Tento způsob je v praxi nejčastější.
- Účel proaktivní – pořizované záznamy jsou průběžně zpracovávány (strojově či manuálně), na základě této průběžné analýzy jsou odhalovány incidenty, podezřelé stavy a jiné anomálie^[18].

Jak uvádí skripta Krizový management III., můžeme oblasti, jimiž se bezpečnostní audit zabývá, rozdělit do 5 okruhů.

- objektová revize (object auditing) – jedná se asi o nejobsáhlejší oblast auditu, zabývá se operacemi s objekty (čtení, zápis, odstranění)
- procesní revize (process auditing) - se týká rozboru událostí související s životním cyklem procesu (vytvoření, průběh, ukončení,...)
- technologicky účetní revize (account auditing) – sledují se události vykonané jednotlivými uživateli systému (operace, výstup, přihlášení do systému, ...)
- kontrola postupů (action/event auditing) –sledují se a zaznamenávají speciální události jako např. start systému, zásahy do bezpečnostní politiky systému apod.;
- kontrola systémových volání (syscall auditing) - záznamu vybraných systémových volání, jejich monitorování, a kontrola parametrů (používá se spíše pro ladící než provozní účely)^[5].

Systémový audit může být pro krizový management velmi náročným nástrojem pro řízení. A to jak v rovině technické – netriviální konfigurace, zvýšená zátěž; tak v rovině organizační – pořizované záznamy je nutno průběžně vyhodnocovat a aktivně využívat při odhalování a řešení bezpečnostních incidentů.

2.3.6 Kontrolní seznam

Check List Analysis

Jedná se o relativně jednoduchou a rychlou metodu, řazenou mezi metody kvalitativní, která je založena na systematické kontrole splnění předem stanovených

podmínek a opatření. Základem pro stanovení těchto podmínek jsou normy a předpisy určené pro daný systém. Účelem je porovnání systému s praxí, který je standardem u stejně zaměřené organizace. Analýzu můžeme použít v jakémkoli stádiu života systému. Šetření je poté prováděno pomocí sestavovaných kontrolních seznamů, které se mohou lišit podle pracovních pozic:

- pracovní pozice vedoucího zaměstnance (např. mistr),
- pracovní pozice osoby odpovědné za správu objektu (např. technik správy budov),

Otázky	ANO	NE
Je označen hlavní uzávěr vody?		
Je označen hlavní uzávěr plynu?		
Je označen hlavní uzávěr topení?		
Je označen hlavní vypínač elektrického proudu?		
Jsou vyznačeny směry úniku osob a nouzový východ?		
Jsou přístupy k hlavnímu uzávěru vody, plynu, topení, hlavnímu vypínači elektrického proudu volné?		
Jsou chodby, schodiště, které jsou součástí únikových cest volné?		
Jsou značky pro označení únikové cesty a nouzového východu zhotoveny z fotoluminiscenčního materiálu?		
Jsou značky z fotoluminiscenčního materiálu instalovány na povrchu vnitřní komunikace nebo těsně nad její úrovní?		
Je v budově zřetelně označeno číslo tísňového volání? / Jsou dobře viditelné a trvale přístupné pro všechny osoby požární poplachové směrnice?		
Jsou zveřejněny platné požární poplachové směrnice?		
Je v budově k dispozici lékárnička pro poskytnutí první pomoci?		

- osoba odpovědná za vyhrazené technické zařízení (např. osoba odpovědná za provoz tlakových nádob stabilních),

nebo podle objektů a zařízení, kterých se týkají:

- stroj, zařízení, přístroj, nářadí (např. soustruh, jeřáb, tlakové nádoby na plyny),
- provozní budova, objekt, provoz (např. sklad, dílna, nízkotlaká kotelna).

Obrázek 4: Kontrolní seznam¹

¹ http://www.bozpinfo.cz/citarna/tema_tydne/kontrolseznamy08.html

2.3.7 ETA

Event Tree Analysis

(analýza stromu událostí)

ETA je vizuálně logický model, pomocí něhož se analyzují jak opatření a vnější vlivy, tak tzv. osy bezpečnosti, ovlivňující cestu v řetězci vedoucímu k havárii. Metoda sleduje průběh procesu od iniciační události přes konstruování událostí vždy na základě dvou možností – příznivé a nepříznivé. Strom se vytváří pomocí dedukce od hypotetické počáteční události k události, která končí chybou a poruchou. Je proto velmi efektivní při analýze vlivu času a domino efektu. Jedná se o kombinaci kvantitativní a kvalitativní metody. Kvalitativně jsou popsány potencionální problémy jako kombinace událostí vytvářející různé druhy výsledků, kvantitativně potom odhady četností výskytu a relativní důležitosti různých sledů poruch.

Postup při analýze pomocí stromu událostí:

1. definice zkoumaného systému

Určují se hranice a omezení systému, formulují se linie zabezpečení, přes které může porucha přerůst v havárii, a určí se počáteční podmínky.

2. identifikace sledované iniciační události

Iniciační událost je charakteristická tím, že představuje poruchu některého systému, poruchu zařízení nebo i chybu člověka. Pokud má iniciační událost bezprostřední následek, je vhodnější použití metody FTA pro odhalení příčin poruch. Analýza stromem událostí nachází uplatnění v případech, kdy rozvoji iniciační události (šíření poruchy) brání instalované systémy (signalizace, bariéry, odstavení) nebo předem přijatá opatření (postupy obsluhy a údržby), které zmírňují možné následky.

3. identifikace bezpečnostních funkcí bránících šíření iniciační události

Mezi systémy s bezpečnostní funkcí patří především :

- systémy automatického odstavení (shutdown systems, interlock systems, atd.)
- varovná signalizace pro obsluhu (upozorňující na výskyt iniciační události)

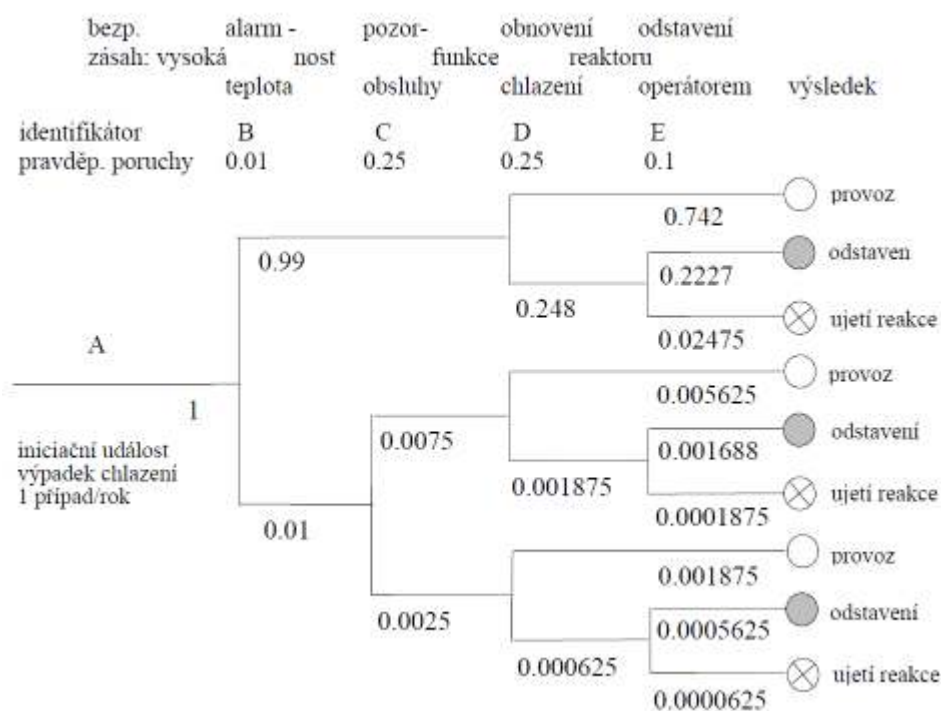
- zásah operátora po varovném signálu nebo na základě předpisů
- systémy zmírňující následky události (pojišťovací ventily, skrápěcí zařízení, hasicí zařízení atd.)
- bariéry a prostředky omezení následků iniciační události

4. sestavení stromu událostí

Sestavení stromu událostí vychází z iniciační události. Bezpečnostní funkce je nutno identifikovat ve správném chronologickém pořadí, ve kterém se podílejí na zmírňování následků případné události. Při sestavování stromu událostí je nutno kvalifikovaně posoudit, zda bezpečnostní funkce ovlivní průběh události. Pokud dojde ovlivnění události, sestrojí se větve pro úspěšný a neúspěšný zásah uvažovaného bezpečnostního systému. Obvykle je úspěšný zásah representován horní větví a neúspěšný zásah spodní větví grafu. Pokud nedojde k ovlivnění průběhu iniciační události, graf se nevětví a zvažuje se funkce dalšího bezpečnostního systému. Každé větvení zakládá novou větev, novou sekvenci událostí.

5. vyhodnocení logického grafu a možných následků

Úplný sestavený logický graf umožňuje pravděpodobnostní hodnocení vývoje události. Vstupními hodnotami jsou pravděpodobnosti pro úspěšný či neúspěšný zásah bezpečnostního systému. Vyhodnocením se získají pravděpodobnosti uvažovaných konečných stavů. Takto lze stanovit pravděpodobnost nevratné posloupnosti poruch a navrhnout úpravy vedoucí ke zlepšení.^[13]



Obrázek 5: Strom událostí^[13]

Metoda ETA se omezuje jen na jednu iniciační událost. Z tohoto důvodu nezjistí celý výčet možných příčin havárie. Pro zjištění všech příčin havárie je proto nutné zvolit jiné metody (HAZOP, FMEA, Co – Kdyby).

2.3.8 FTA

Fault Tree Analysis

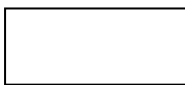
(analýza stromu poruch)

FTA je stejně jako metoda ETA vizuálním modelem logických vztahů mezi poruchami zařízení, lidskými chybami a vnějšími událostmi, které mohou způsobit havárii. Metoda FTA se stejně jako metoda FMEA řadí k preventivním metodám. Cílem metody FTA je analýza pravděpodobnosti selhání celého systému a s tím související preventivní opatření, která by měla spolehlivost systému zvýšit. Na rozdíl od metody ETA se pro sestavení stromu používá induktivní logika a začíná se hypotetickou poruchou. Metoda je nástrojem pro hledání spolehlivost rozsáhlých systémů.

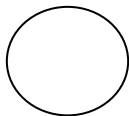
U metody FTA postupujeme následujícím způsobem^[8]:

1. Definování systému – viz ETA.
2. Určení specifického problému jako vrcholu stromu – top událost (Top Event)
 Popis musí být přesný a přiměřený , např. vysoká teplota v reaktoru, příliš vysoká hladina kapaliny v zásobníku . Naproti tomu se události typu „exploze reaktoru“ nebo „požár v procesu“ jeví jako příliš neurčitý, vágní popis události. Naproti tomu se událost „netěsnost ventilu“ jeví pro tuto analýzu jako příliš specifická, detailní.
3. Určení logické struktury – typy uzlů a vztahy mezi nimi.

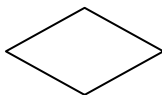
Nejčastěji se používají tyto grafické symboly:



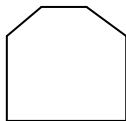
vyjadřuje vrcholovou, nejvyšší událost, kterou je havárie. Obdélník vyjadřuje rovněž přechodné události, jako jsou stavy systému nebo výskyt nějakého faktoru, který přispívá ke vzniku havárie



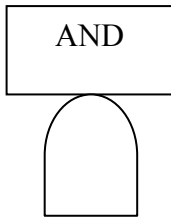
znázorňuje základní událost, která je nejnižší úrovní stromu poruch



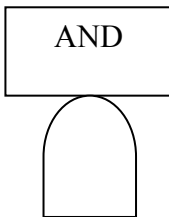
používá se k reprezentaci lidských chyb a události, které se dále v systému nerozvíjejí



znázorňuje vnější událost nebo omezující podmínku



výstupní událost se uskuteční, jestliže a pouze jestliže se vyskytnou všechny vstupní události



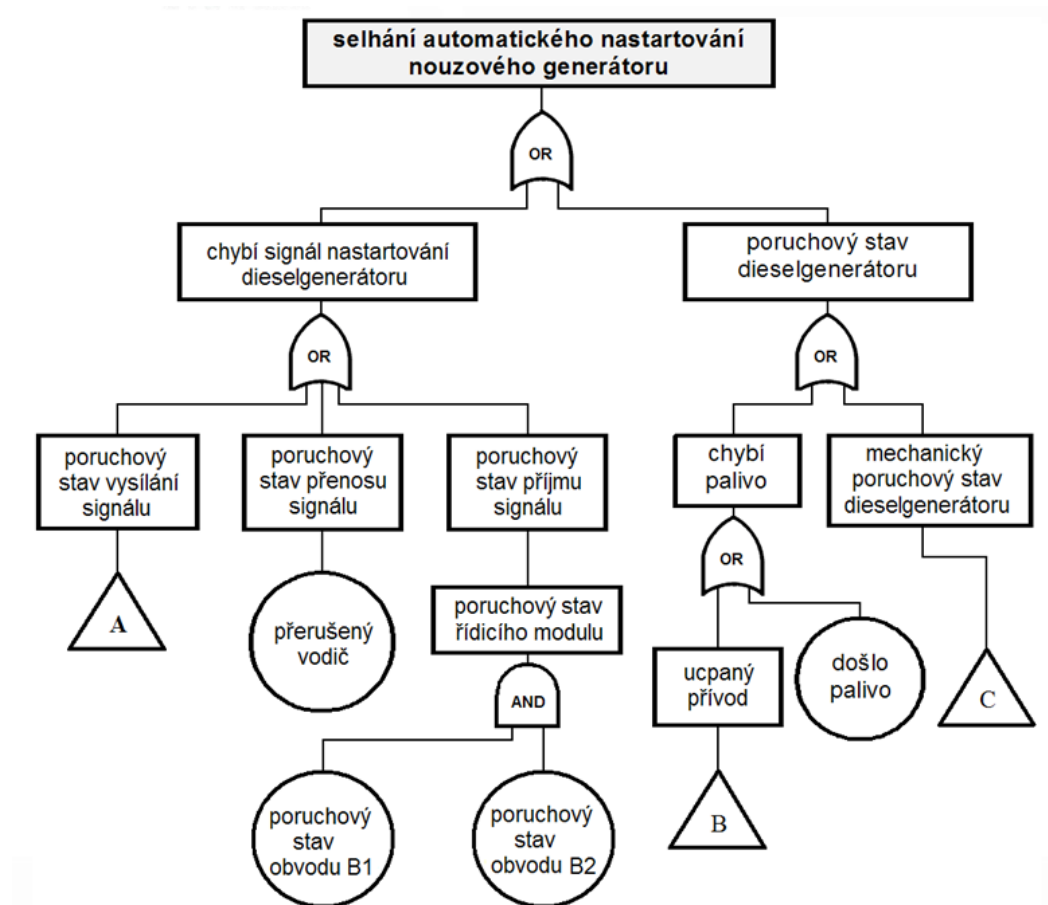
výstupní událost se uskuteční, jestliže se vyskytne nějaká vstupní iBji událost



uzel tlumení je případem uzlu AND a funguje, když podmínka je pravdivá a současně se vyskytne událost na vstupu

4. Prozkoumání každé větve stromu.
5. Řešení kombinace událostí.
6. Určení důležitých poruch a jejich závislostí.
7. Kvantitativní analýza četností a pravděpodobností výskytu.
8. Využití výsledků pro rozhodování.

U této metody je třeba znalost statistiky a relevantních dat. Úspěšnost výsledky závisí na kvalitních znalostech analytika. FTA se zaměřuje jen na jednu určitou havárii.



Obrázek 6: Strom poruch²

2.3.9 PHA

Preliminary Hazard Analysis

(předběžné posouzení nebezpečí)

PHA se používá **fázi koncepčního návrhu** projektu provozu, ve fázi dislokace nebo ve fázi vývoje procesu s cílem **vytvořit seznam všech nebezpečí**, která se mohou v procesu vyskytnout. Účelem PHA je sestavit seznam zdrojů rizik, přičemž nebezpečné situace v tomto seznamu budou seřazené v závislosti na míře rizika. Nejvíce pozornosti se poté věnuje nebezpečím na začátku tohoto seznamu. Vychází se z brainstormingu skupiny expertů. Proto je důležité, aby tento tým, měl dostatečné

² www.rss.tul.cz/download/rjs/09-RJSPrednaska4S08n.ppt

znalosti o daném problému. Pro zvýšení objektivitu a kvality výsledků je následně nutná detailnější analýza zjištěných hrozeb.

Aplikační kroky jsou následující:

1. hledání souvislostí mezi událostmi;
2. kladení dotazů (Co by kdyby ... člověk, prostředí, řízení, výroba, situace);
3. klasifikace činitelů vedoucí k hazardům;
4. klasifikace nehod, nouzových stavů;
5. klasifikace chyb v systému;
6. výrok o riziku a protipatření^[5].

2.3.10 RR

Relative Ranking

(relativní klasifikace)

Jde spíše o analytickou strategii než metodu. Jejích hlavním cílem je stanovit relativní důležitost procesů a činností z hlediska bezpečnosti a na jejím základě posoudit potřebu dalších analýz. Relativní klasifikace může být použita rovněž pro srovnání několika návrhů umístění procesu nebo zařízení a zajistit tak informaci o tom, která z alternativ je nejlepší nebo méně nebezpečná^[20].

2.3.11 HRA

Human Reliability Analysis

(analýza spolehlivosti lidského činitele)

Analýza lidské spolehlivosti je postup na posouzení vlivu lidského činitele na výskyt živelných pohrom, nehod, havárií, útoků apod. či některých jejich dopadů. Zahrnuje přístupy mikroergonomické (vztah „člověk – stroj“) a makroergonomické (vztah systému „člověk – technologie“). Výsledkem je seznam chyb, které se můžou

vyskytnout během procesů, faktorů přispívajících k těmto chybám a návrh změn v systému, které přispějí ke snížení pravděpodobnosti vzniku takovýchto chyb. Analýza HRA má těsnou vazbu na aktuálně platné pracovní předpisy především z hlediska bezpečnosti práce. Hra se často kombinuje s metodami, které odhalují zdroje rizika (např. ETA, FTA, HAZOP alebo FMEA)^[20].

2.3.12 CPQRA

Chemical Proces Quantitative Risk Analysis

(kvantitativní analýza rizika chemického procesu)

Tato metoda v praxi nepatří mezi často používané, ovšem do své práce jsem jí zařadil s ohledem na sledování rizik v podniku Synthesia a. s. v praktické části, ve kterém chemické procesy probíhají. Tato metoda je velice podrobná. Představuje kompletní bezpečnostní studii a klade velké nároky na čas a kvalifikaci analytiků. Umožňuje identifikovat a určit prioritu individuálních nebezpečí, které přispívají k celkovému riziku procesu.

Tuto metodu můžeme rozdělit do následujících etap:

- stanovení cíle analýzy
- popis analyzovaného systému
- vypracování seznamu havárií a výběr závažných havárií
- odhad důsledků havárií
- modifikace systému s cílem snížit následky havárií
- odhad četnosti havárií
- modifikace systému s cílem snížit četnost havárií
- odhad rizika na základě četnosti a následků
- modifikace systému s cílem snížení rizika

2.3.13 QRA

Process Quantitative Risk Analysis

(analýza kvantitativních rizik procesu)

Kvantitativní posuzování rizika je systematický a komplexní přístup pro predikci odhadu četnosti a dopadu nehod pro zařízení nebo provoz systému. Analýza kvantitativních rizik procesu je koncept, který rozšiřuje kvalitativní (zpravidla verbální) metody hodnocení rizik o číselné hodnoty. Algoritmus využívá kombinaci (propojení) s jinými známými koncepty a směřuje k zavedení kritérií pro rozhodovací proces, potřebnou strategii a programy k efektivnímu zvládnání (řízení) rizika. Vyžaduje náročnou databázi a počítačovou podporu^[20].

2.3.14 What – If Analysis

(analýza toho, co se stane když, Co - Kdyby)

Analýza „Co - Kdyby“ se zabývá zkoumáním odchylek od návrhu. Jedná se o kvalitativní metodu. V podstatě je to spontánní diskuse a hledání nápadů, ve které skupina zkušených lidí dobře obeznámených s procesem klade otázky nebo vyslovuje úvahy o možných nehodách. Má tedy brainstormingové a užívá obsáhlé, volně strukturované otázky, jejichž formulaci může napomoci HAZOP nebo FMEA. Není to vnitřně strukturovaná technika a není příliš časově náročná. Neformální struktura neumožňuje audit úplnosti a důkladnosti postupu a existuje možnost přehlédnout nějaký potenciální problém. Účelem analýzy je identifikovat ohrožení, zvážit obecné typy havárií, které mohou v procesu nastat, zhodnotit kvalitativně účinky těchto havárií a určit zda ochranná opatření proti možným havarijním situacím jsou přiměřená. Pro určení příčinných faktorů se musejí používat jiné metody

„Co - Kdyby“ se skládá ze sedmi kroků^[8]:

1. Určení oblasti zájmu (systém a jeho ohraničení, stanovení klíčových činností).
2. Určení typu problému k analýze.
3. Rozložení systému, činností (systém na prvky, činnost na operace).

4. Formulace otázek „Co - Kdyby“ pro každý prvek činnosti nebo systému.
Postup formulace otázek je následující:
 - Připomenout analytickému týmu záměry a cíle
 - Umožnit členům týmu uspořádání myšlenek během deseti minut
 - Vysvětlit, jak se otázky budou shromažďovat (brainstorming, brainwriting apod.)
 - Vysvětlit pravidla pro formulaci otázek. Například kombinace otázek nebo nová stylizace obecnější otázky apod.
 - Zaznamenávat nápady a náměty
 - Uspořádat otázky do logických skupin a odstranit překrývající se otázky
5. Odpovědi na otázky. Odpovědi obecně definují doporučení na změny (scénáře změn), bezpečnostní opatření (bezpečnostní úroveň), konečné důsledky a bezprostřední systémovou odezvu a systémové podmínky.
6. Detailnější specifikace, je-li potřebná, na základě odpovědí.
7. Využití výsledků pro rozhodování: posouzení přijatelnosti, určení toho, co lze zlepšit, zdůvodnění přidělení zdrojů pro zdokonalení.

2.3.15 CCA

Cause-Consequence Analysis

(analýza příčin – následků)

Analýza příčin a dopadů je směs analýzy stromu poruch a analýzy stromu událostí. Největší předností CCA je její použití jako komunikačního prostředku: diagram příčin a dopadů zobrazuje vztahy mezi koncovými stavy nehody (nepřijatelnými dopady) a jejich základními příčinami. Protože grafická forma, jež kombinuje jak strom poruch, tak strom událostí do stejného diagramu, může být hodně detailní, užívá se tato technika obvykle nejvíce v případech, kdy logika poruch analyzovaných nehod je poměrně jednoduchá. Jak už napovídá název, účelem analýzy příčin a dopadů je odhalit základní příčiny a dopady možných nehod. Analýza příčin a dopadů vytváří diagramy s nehodovými sekvencemi a kvalitativními popisy možných koncových stavů nehod.^[20]

2.3.16 Matice rizik a kritéria přijatelnosti rizika

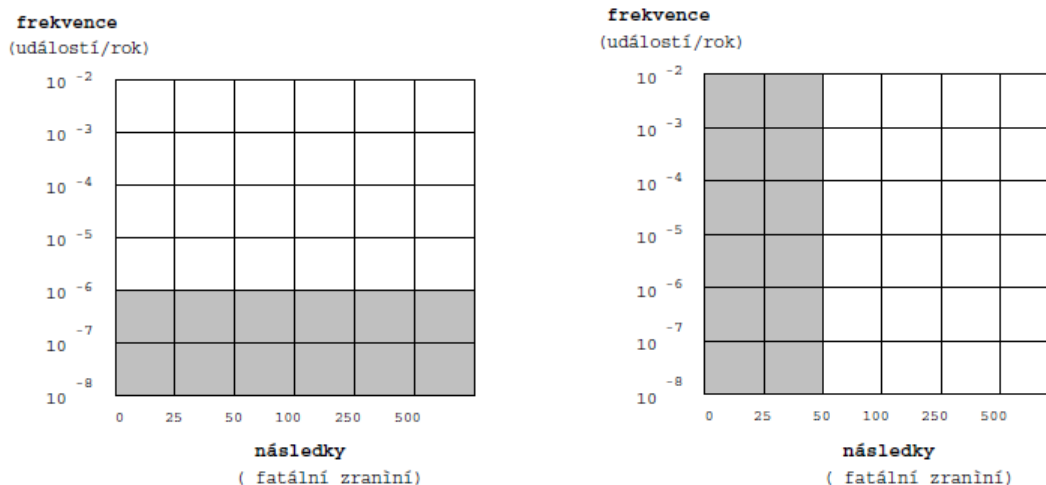
Jedná se o relativně jednoduchou a časově nenáročnou metodu. Proto se používá spíše pro orientaci v systému.

Postup:

1. klasifikace události podle:
třídy následků – možno vyjádřit slově (popis rozsahu škod), nebo číselnou stupnicí v absolutních nebo relativních hodnotách
třídy pravděpodobnosti: podle řádu hodnoty vyjadřující počet havárií/časové období
2. bodové ohodnocení jednotlivých tříd
3. znázornění všech zdrojů rizika v matici rizik (třídy následky versus třídy pravděpodobností)
4. zařazení jednotlivých událostí do příslušné kategorie míry rizika, dle bodového součinu tříd, do kterých sledovaná událost náleží

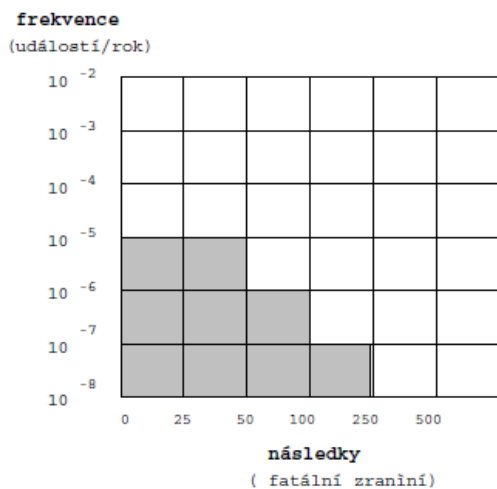
Existují 2 varianty matic:

- jednoduchá jednostranná kritéria přijatelnosti (nevystihují realitu problému rizika)



Obrázek 7: Matice rizik^[13]

- pro praxi - kombinovaná kritéria přijatelnosti rizika



Obrázek 8: Matice rizik^[13]

2.3.17 SFERA

(Systém, fenomén, efekt, riziko, analýza)

Tato metoda je základem další části mé práce, a proto jí bude věnována pozornost dále.

3 Analýza rizik v Synthesia, a. s. metodou SFERA

3.1 Základní údaje o společnosti Synthesia a. s.

<i>Název subjektu:</i>	Synthesia, a.s.
<i>Sídlo:</i>	Pardubice, Semtín č.p. 103, PSČ 53217
<i>Vznik společnosti</i>	01.01.1994

Synthesia, a. s. je výrobcem kvalifikované chemie. Společnost má 1 900 zaměstnanců a její obrat v roce 2008 přesáhl 126 milionů EUR. Podnikatelské aktivity jsou zacíleny do tří tržních segmentů pokročilých organických intermediátů, derivátů celulózy a pigmentů a barviv. Produkce Synthesie je zaměřena nejen na tuzemský trh, tři čtvrtiny výroby jsou určeny pro export na vyspělé evropské trhy či do zámoří.

V závislosti na širokém sortimentu je založena i organizační struktura firmy – ta je rozdělena do tří strategických výrobně obchodních jednotek (SBU – Strategic Business Unit). Obchodní jednotky (SBU - strategic business unit) jsou do velké míry samostatné útvary zaměřené na výrobu a obchod v jasně definovaném produktovém segmentu. Každé SBU řídí manažer přímo podřízený generálnímu řediteli společnosti. Synthesia je rozdělena do tří SBU^[27]:

- **Organická chemie** Tato obchodní jednotka produkuje škálu různých výrobků, které jsou používány v oblasti farmacie, výroby pesticidů a jiných účinných látek, nebo jako polotovary (např. stabilizátory střelného prachu). Výzkum a vývoj v této oblasti zajišťuje dceřiná společnost Výzkumný ústav organických syntéz, a.s.
- **Nitrocelulóza** Obchodní jednotka byla vytvořena v roce 2002, ale výroba nitrocelulózy má ve společnosti více než 80letou tradice. Výroba je soustředěna na segment derivátů celulózy, rozpouštědel, anorganických kyselin a solí. Výrobky jsou dodávány do 25 zemí světa.

- Pigmenty a barviva V současné době je Synthesia jediným výrobcem organických barviv v České republice. Tato barviva vyváží do 50 zemí světa. O oblast vývoje nových výrobků se stará Výzkumný ústav organických syntéz, a.s.

Počátkem roku 2006 byla zřízena Bezpečnostní rada Synthesia, složená ze starostů okolních obcí, zástupců města, kraje i HZS, která společně řeší potenciální rizika a hodnotí postupy Synthesie z pohledu bezpečnosti dotčených oblastí i celého regionu. Bezpečnost práce se ve společnosti řídí především těmito právními předpisy:

- zákon č. 262/2006 Sb., zákoník práce ve znění pozdějších předpisů
- zákon č. 309/2006 Sb., o zajištění podmínek bezpečnosti a ochrany zdraví při práci
- zákon č.353/1999 Sb., o prevenci závažných průmyslových havárií způsobených vybranými nebezpečnými chemickými látkami a chemickými přípravky
- nařízení vlády č. 406/2004 Sb., o bližších požadavcích na zajištění BOZP v prostředí s nebezpečím výbuchu

3.1.1 Areál společnosti Synthesia, a.s.

Areál společnosti rozloze 4,4 km² se nachází na severozápadním okraji krajského města Pardubice o na okraji Pardubic. Nachází se přímo v bezprostřední blízkosti komunikace I/37 na Hradec Králové a Chrudim a zároveň leží přímo na silnici I/36 přivádějící nákladní dopravu na dálnici D11 směrem na Prahu. Areál je také výhodně napojen i na dopravní infrastrukturu města Pardubic, k areálu jezdí několik spojů městské hromadné dopravy. V rámci průmyslové zóny Semtín působí více než 50 externích firem.



Obrázek 9: Poloha areálu Synthesia, a. s.³

3.2 Historie společnosti^[26]

1920 - Historie společnosti začíná založením Československé akciové továrny na látky výbušné, která byla v roce 1934 přejmenována na Explosii.

1928 - V Pardubicích - Semtíně byla založena Synthesia, sesterský závod Expolosiie. Produkce se zaměřila na anorganické produkty pro výrobu výbušnin.

1994 - Proběhla transformace na akciovou společnost Synthesia. Akciová společnost SYNTHESIA a.s. byla založena jednorázově Fondem národního majetku ČR dne 17. 12. 1993 Společnost byla zapsána do obchodního rejstříku ke dni 1. ledna 1994.

1999 - Fúze Synthesia, a. s. se společnostmi Fatra, a. s., Moravské chemické závody, a. s. a Technoplast, a.s., zároveň dochází ke změně obchodního názvu na ALIACHEM a. s. V rámci společnosti ALIACHEM a. s. zároveň vznikají čtyři odštěpné závody, jedním z nich je odštěpný závod SYNTHESIA

³ <http://www.mapy.cz>

2001 - Majoritními vlastníky ALIACHEMU se stávají společnosti Agrofert a Unipetrol.
2003 - Vznik strategických obchodních jednotek (SBU)
2004 - Fúze se společností Ostacolor, a.s., vzniká SBU Pigmenty a Barviva
2006 - Završení procesu vnitřních změn společnosti ALIACHEM a. s. , formou vyčlenění části podniku – odštěpného závodu FATRA do dceřiné společnosti Fatra, a. s. a zrušení odštěpného závodu SYNTHESIA. Zaniká ALIACHEM a.s., Synthesia se vrací k tradičnímu obchodnímu názvu Synthesia, a.s.
2008 – Synthesia se stává členem skupiny Agrofert. Jediným majoritním vlastníkem Synthésie se stává Agrofert Holding.

Agrofert Holding, a.s. je společnost vlastnící významné majetkové účasti ve zpracovatelských, výrobních a distribučních podnicích zemědělského, potravinářského a chemického průmyslu.⁴

3.3 Analýza rizik ve společnosti Synthesia, a. s.

Pro vyhodnocení analýzy byla použita metoda SFERA. Metoda je založena na porovnávání rizik mezi sebou prostřednictvím kontingenční tabulky s následným expertním odhadem pravděpodobností možných rizik vyvozených z četnosti a možných ztrát na majetku dle předem stanovených kritérií odvozených ze zvažovaného územního celku ve správním území.

3.3.1 Přehled rizik

Metodu SFERA jsou hodnocena rizika, která si definovala společnost ve své vnitřní směrnici OS 65/6 s názvem Identifikace a hodnocení rizik (Příloha 2) vydané 1. července 2007⁵. Tato rizika, společně se zkratkami, které budou použité v dalších krocích analýzy, a podrobnějším popisem jednotlivých rizik, jsou uvedena v následující tabulce:

⁴ <http://www.justice.cz/xqw/xervlet/insl/getFile?listina.@slCis=6044426&listina.@rozliseni=pdf&listina.@klic=fa724548e5d143272c13d2cf607a5d44>

⁵ dostupné na: <http://www.synthesia.eu/cz/Legislativa>

Riziko	Zkratka	Popis
Uklouznutí, klopýtnutí, chybné našlápnutí	UKCHN	<ul style="list-style-type: none"> • uklouznutí nebo chybné našlápnutí na rovném nebo šikmém povrchu • uklouznutí nebo chybné našlápnutí na schodištích nebo žebřících • uklouznutí nebo chybné našlápnutí vlivem kluzkého povrchu
Transport, manipulace	TRMAN	<ul style="list-style-type: none"> • najetí, naražení, přimáčknutí, rozdrcení • přejetí, převálcování, pád nákladu
Pád z výšky, pád předmětu	PADVP	<ul style="list-style-type: none"> • v důsledku nezajištěného nebo špatně zajištěného pracoviště • nesprávným postupem při práci ve výškách nebo pádu do hloubky
Snížená průchodnost	SNIPR	<ul style="list-style-type: none"> • při chůzi po určených trasách nebo při překonávání průlezů
Montáž	MONTZ	<ul style="list-style-type: none"> • zařízení a jeho součástí, údržba zařízení
Požár, únik plynu, výbuch	PUPVY	<ul style="list-style-type: none"> • technologická příčina (chyba zařízení, lidská chyba)
Kontakt s nebezpečnou látkou	KNBZL	<ul style="list-style-type: none"> • požití látky • kontakt s kůží a očima • vdechnutí aerosolu nebo plynné látky (prachu) • dlouhodobé působení látek
Nedostatečné osvětlení	NEOSV	<ul style="list-style-type: none"> • Nedostatečná intenzita, nerovnoměrnost osvětlení

Klimatické podmínky	KLPOD	<ul style="list-style-type: none"> • Působení venkovních klimatických podmínek (horko, chlad, vítr, déšť, slunce apod.)
Mikroklimatické podmínky	MIKPO	<ul style="list-style-type: none"> • Vliv mikroklimatických podmínek na pracovišti (teplota, vlhkost, prašnost,...)
Ohrožení opakovanou činností	OOCIN	<ul style="list-style-type: none"> • Ohrožení opakovanou jednotvárnou činností – ztráta koncentrace, nedodržení bezpečnosti práce
Zasažení energiemi	ZASEN	<ul style="list-style-type: none"> • elektrickou energií • tepelnou energií (horká média, horké povrchy) • mechanickou energií (úder, pořezání, přimáčknutí, rozdrčení, ustřížení, píchnutí, naražení, zachycení, vtažení, kontakt s pohyblivými rotujícími částmi apod.) • magnetickým polem • vibracemi • hlukem • zářením

Tabulka 5: Přehled rizik⁶

Z mého pohledu není výčet rizik úplný. Chybí zde taková rizika, jako jsou zemětřesení, povodně, pád letadla, teroristický útok a další. Dá se tedy říci, že analýza je zaměřená pouze na vnitřní rizika, která ohrožují podnik a jeho činnost. Některá rizika v seznamu jsou příliš obecná. Například únik plynu, nebo kontakt s nebezpečnou látkou zde není podrobněji specifikován. Ovšem cílem této analýzy bylo hodnotit ta rizika, která si společnost definovala sama, a jejich seznam uvedla v již zmíněné směrnici.

⁶ zpracováno autorem

V následující tabulce jsou uvedena veškerá vstupní data potřebná k namodelování sledovaného systému. Pro vysvětlení je potřeba definovat si pár pojmů:

Procenta celkové kritériální váhy musí v součtu nabývat hodnoty 100 %. **Maximální možnou škodu** se myslí stoprocentní poškození ohrožených aktiv. **Počet dnů** udává, za jaký časový interval znovu nastane daná událost. **Pravděpodobnost** nastání jevu se počítá jako převrácená hodnota počtu dnů, za které událost nastane.

Tabulka kritérií možných ztrát			Ohrožená aktiva				
			Ztráty na zaměstnancích	Ztráty na majetku společnosti	Ekologické ztráty	Ztráty na obyvatelstvu	Ztráty na okolním majetku
Celková kritériální váha			30 %	10 %	10 %	40 %	10 %
Maximální možná škoda			1900 zaměstnanců	Úplné zničení majetku	Zasažení okolí do 10 km	Počet obyvatel do 10 km	Úplné zničení objektu do 10 km
Zkratka	Pravděpodobnost	Počet dnů	Procentuální ztráta z maximální možné škody				
UKCHN	0.033333	30	0,08	0,0001	0	0	0
TRMAN	0.016667	60	0,8	0,025	0,006	0	0
PADVP	0.011111	90	0,08	0,001	0	0	0
SNIPR	0.001389	720	0,08	0,0001	0	0	0
MONTZ	0.000926	1080	1,6	0,01	0,006	0	0
PUPVY	0.000111	9000	35	15	25	30	15
KNBZL	0.000556	1800	20	5	15	5	3
NEOSV	0.000926	1080	0,08	0	0	0	0
KLPOD	0.005556	180	0,8	0,001	0	0	0
MIKPO	0.005556	180	3,2	1	5	0	0
OOCIN	0.016667	60	0.08	0,0001	0	0	0
ZASEN	0.005556	180	3,2	5	3	0	2

Tabulka 6: Kritéria rizik⁷

⁷ zpracováno autorem

3.4 Zadání dat do programu SFERA

3.4.1 SFERA

Metoda byla vyvinuta na pracovišti krizového řízení v Institutu ochrany obyvatelstva. Stanovují se v ní možné hrozby, jejich vzájemné ovlivňování, pravděpodobnosti jejich vzniku a nakonec zranitelnosti základních aktiv objektu. Výstupem je hierarchický řetězec příčin a následků s ohodnocením nebezpečí vlivu jednotlivých hrozeb, který zohledňuje vzájemné podmíněnosti hrozeb.

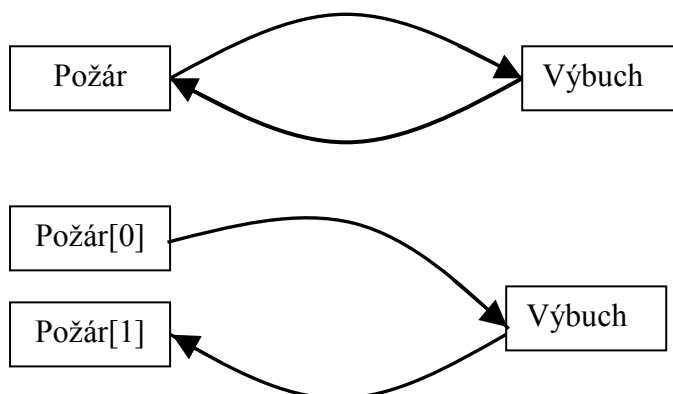
I když je program SFÉRA explicitně určen pro analytické účely, je **s výhodou využitelný prakticky ve všech případech**, kdy lze daný systém identifikovat jeho strukturou a chováním, a kdy lze v návaznosti na předchozí popsat určité parametry vstupů a výstupů v jednotné škále vzájemné měřitelnosti porovnávaných prvků. Program SFÉRA lze například využít pro rychlé kriteriální rozhodování, kdy zpravidla nepracujeme s velkým množstvím prvků a kdy časové dispozice řešitelnosti nelze přesně předvídat.⁵

SFERA obsahuje 6 oken, která na sebe navazují v časové posloupnosti při provádění analýzy rizik.

- **Matice** – zde se tvoří vztahy mezi jednotlivými prvky systému pomocí kontingenční tabulky
- **Vztahy** – v tomto okně jsou vytvořené vztahy přehledně zobrazeny, což umožňuje kontrolu správnosti zadaných dat v předchozím okně
- **Průvodce zadáním dat** – zde je možnost pracovat s jednotlivými prvky systému (např. přidávat, mazat, přejmenovávat, ...)
- **Hodnoty prvků** – okno slouží k zadání parametrů potřebných pro namodelování sledovaného systému
- **Výsledky** – zde se zobrazují výsledky v grafické podobě nebo v podobě influenčního stromu
- **Soubor projektu** – v tomto okně je možnost importovat prvky z námi vytvořeného systému do systému jiného

3.4.2 Matice

V okně Matice utváříme vztahy a vazby mezi námi definovanými riziky. Tyto vazby tvoříme v kontingenční tabulce, do které zadáváme buď hodnotu 0, která znamená, že riziko uvedené v daném řádku, není podmíněno rizikem uvedeným v daném sloupci. Hodnota 1 naopak znamená, že dané riziko v řádku ovlivněno rizikem v daném sloupci je. Po zadání všech hodnot použijeme tlačítko Přepočítat pro dekompozici prvků. Tato dekompozice znamená rozdělení takových prvků, které mohou způsobit konkrétní riziko a zároveň jím jsou způsobeny. Tento krok je pro algoritmus metody zásadní. Bez něho by došlo k zacyklení prvků a ke zkreslení výstupních hodnot. Uvedené vazby jsou pro názornost ukázány na obr. 10.



Obrázek 10: Dekompozice prvků^[28]

Na obrázku 11 je matice, kterou jsem vytvořil z výše uvedených rizik a z logicky odvozených vazeb mezi prvky. U matice je již provedena výše zmiňovaná dekompozice, která některé prvky rozděluje na Prvek[0] a Prvek[1], a můžeme si všimnout, že prvky nad „úhlopříčkou tabulky“ nabývají pouze hodnoty 0. Hodnoty kritérií jsou pro tyto dekomponované prvky stejné.

	TRMAN[1]	KNEZL[1]	ZASEN[1]	MONTZ[1]	PADVP[0]	UKCHN[0]	TRMAN[1]	SNUPR[0]	KLPOD[1]	NEOSV[1]	MIKPO[1]	MONTZ[1]	KNEZL[0]	PUPVY[0]	ZASEN[0]	NEOSV[0]	MIKPO[0]	OOCIN[0]	KLPOD[0]
PUPVY[1]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TRMAN[1]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
KNEZL[1]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ZASEN[1]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MONTZ[1]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PADVP[0]	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
UKCHN[0]	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
TRMAN[0]	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
SNUPR[0]	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
KLPOD[1]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NEOSV[1]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MIKPO[1]	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
MONTZ[0]	1	0	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0
KNEZL[0]	0	0	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	0	0
PUPVY[0]	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0	0
ZASEN[0]	0	0	0	0	0	1	1	1	1	1	0	1	1	1	1	0	0	0	0
NEOSV[0]	0	0	0	0	0	1	1	1	1	0	0	1	1	1	1	0	0	0	0
MIKPO[0]	0	0	0	0	0	1	1	1	1	0	0	1	1	1	1	1	0	0	0
OOCIN[0]	0	0	0	0	0	1	1	1	1	0	0	1	1	1	1	1	0	0	0
KLPOD[0]	0	0	0	0	0	1	1	1	1	0	0	1	1	1	1	1	0	0	0

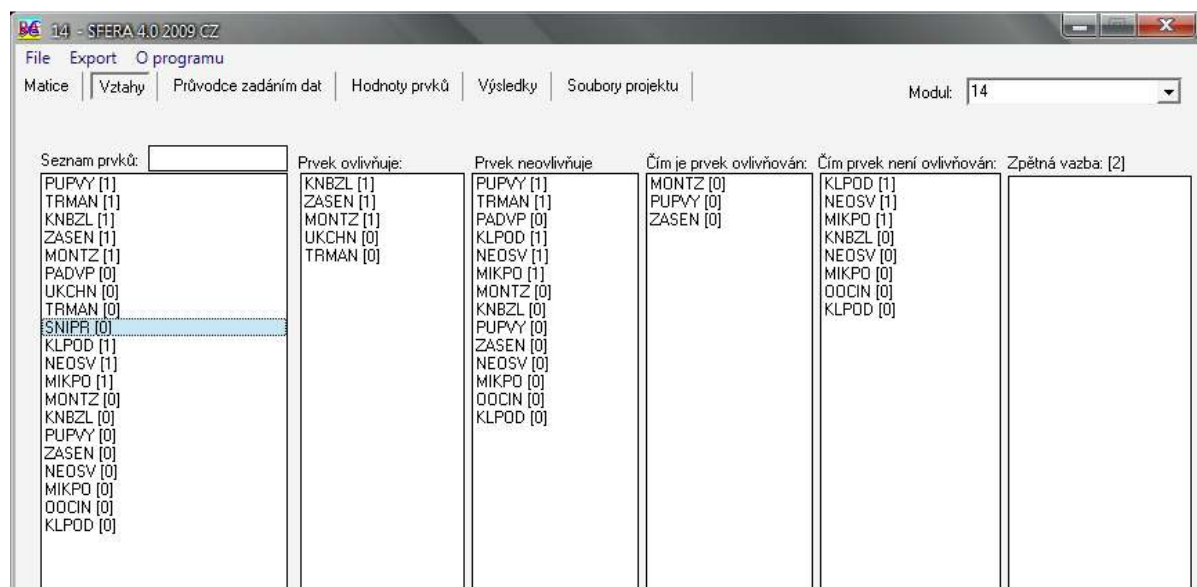
Obrázek 11: Kontingenční tabulka⁸

3.4.3 Vztahy

V tomto okně vidíme přehledně zobrazeny vztahy mezi prvky. Jsou zde uvedeny vazby, které jsme zadali do okna Matice pomocí hodnot 0 a 1, tedy prvky, které

⁸ zpracováno autorem

ovlivňují nebo neovlivňují vybraný prvek a zároveň jakými prvky je či není námi vybraný prvek ovlivňován. Toto okno slouží hlavně pro kontrolu vazeb, protože při větším počtu rizik je kontingenční tabulka značně nepřehledná a je zde proto velký prostor pro chybu.



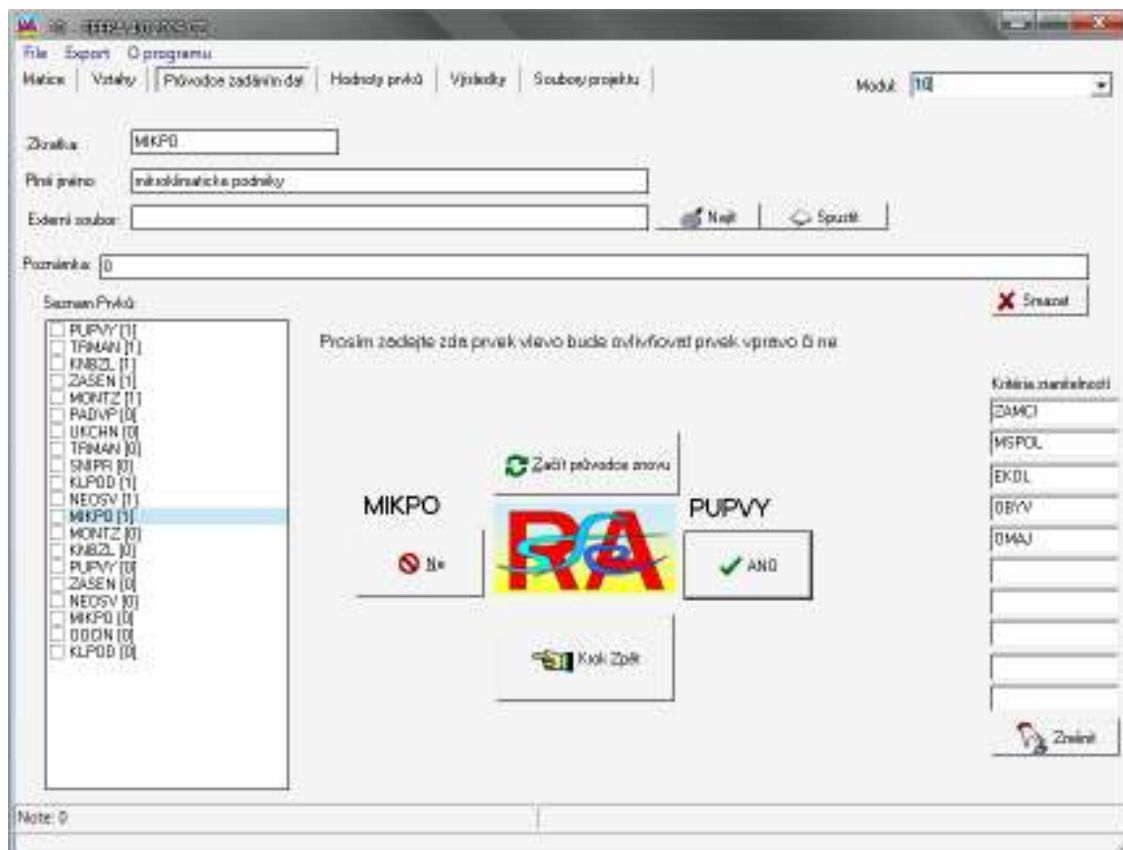
Obrázek 12: Okno vztahy⁹

3.4.4 Průvodce zadáním dat

Zde můžeme k jednotlivým rizikům přepisovat potřebné poznámky, popřípadě vkládat externí soubor. Prvky zde může upravovat, přidávat i mazat. Při této činnosti musíme však být velmi obezřetní, protože při práci s prvky může dojít ke zkreslení jednotlivých vztahů mezi riziky v kontingenční tabulce. K jednotlivým rizikům lze přiřadit libovolný soubor (textový, obrázek, graf, tabulku, ...). V tomto okně můžeme také vytvořit kontingenční tabulku pomocí tlačítek, která určují, zda prvek na levé straně ovlivňuje prvek na straně pravé.

V tomto okně se také definují ohrožená aktiva – Kritéria zranitelnosti, tedy o aktiva ohrožená uvedenými riziky. Osobně jsem zvolil kritérií zranitelnosti 5, a to: ztráty na zaměstnancích (ZAMCI), ztráty na majetku společnosti (MSPOL), ekologické ztráty (EKOL), ztráty na obyvatelstvu (OBYV) a ztráty na okolním majetku (OMAJ).

⁹ zpracováno autorem



Obrázek 13: Okno Průvodce zadáním dat¹⁰

3.4.5 Hodnoty prvků

Do tohoto okna se zadávají parametry systému. Konkrétně se jedná o pravděpodobnost, že daná událost nastane x -tý den. Počítá se tedy jako převrácená hodnota počtu dní, za které nastane znovu. Takto vypočtené pravděpodobnosti pak zapisujeme do sloupce tabulky s názvem Vstupní(P).

Pro další sloupec tabulky s názvem Koeficient(P) je nutné zvolit koeficient (buď 10, 100, 1000, které program nabízí, nebo námi zvolený s libovolnou hodnotou). Tento koeficient nám vyjadřuje nepřímé působení rizik vůči systému. Po zaškrtnutí, nebo vyplnění koeficientu se nám sloupce vyplní automaticky.

Dále je nutné zadat data do tabulky ve spodní části okna. V této tabulce má každé ohrožené aktivum svůj sloupec, jehož zkratka je uvedena v prvním řádku. Do druhého

¹⁰ zpracováno autorem

řádku poté vkládáme tzv. celkovou kritériální váhu, která znamená, kolik procent ze stoprocentního celku přiřadíme danému chráněnému aktivu, kde uvedené procento znamená, jak si chráněného aktiva vážíme v porovnání s ostatními sledovanými. Do třetího řádku pak vkládáme počet procent, která vyjadřují, kolik procent z chráněného aktiva bude zničeno v případě, kdy nastane sledovaná událost. Program nám pak spočítá řádek čtvrtý. Hodnoty v tomto řádku jsou sečteny a automaticky zapsány do sloupce v horní tabulce s názvem Zranitelnost.

Po zadání všem údajů můžeme spočítat zbylé hodnoty pomocí tlačítka Počítej. Program vyplní zbývající sloupce tabulky. Z hlediska výsledků analýzy je pro nás nejdůležitější poslední sloupec, který udává, z kolika procent daná hrozba ohrožuje sledovaný systém (součet tohoto sloupce je roven 100). Pro další práci je ovšem nutné uvědomit si provedenou dekompozici prvků a tyto rozdělené prvky je nutné znovu sloučit, tedy sečíst jejich výsledné hodnoty.

Jméno	Vstup(P)	Koeficient(P)	Zranitelnost	Hroz(P)	Váha pořadí	Pořadí	% Vliv
PUPVY[1]	0.000111	1.11E-5	28	0.00288	0.0805	2	29.5 %
TRIPAN[1]	0.026667	0.00167	0.2431	0.005	0.00122	30	0.446 %
KVBZL[1]	0.000556	5.56E-5	10.3	0.00307	0.0336	4	11.6 %
ZASEM[1]	0.000556	0.000556	1.96	0.00697	0.0137	5	5.01 %
HONTZ[1]	0.000926	9.26E-5	0.4816	0.000232	0.000112	36	0.041 %
PADVPE[0]	0.011111	0.00111	0.0241	0.00965	0.00233	12	0.0952 %
UKCHN[0]	0.033333	0.00333	0.02401	0.00874	0.0021	13	0.0768 %
TRIPAN[0]	0.026667	0.00167	0.2431	0.00541	0.00132	9	0.483 %
SNIPR[0]	0.001389	0.000139	0.02401	0.000799	1.92E-5	38	0.00702 %
KLPOD[1]	0.000556	0.000556	0.2401	0.000612	0.000147	14	0.0538 %
MEOGV[1]	0.000926	9.26E-5	0.024	0.000104	2.9E-6	20	0.000915 %
HIKPOE[1]	0.000556	0.000556	1.56	0.000716	0.00132	11	0.41 %
HONTZ[0]	0.000926	9.26E-5	0.4816	0.00359	0.00173	7	0.633 %
KVBZL[0]	0.000556	5.56E-5	10.3	0.0035	0.0361	3	13.2 %
PUPVY[0]	0.000111	1.11E-5	28	0.00345	0.0996	1	25.3 %
ZASEM[0]	0.000556	0.000556	2.92	0.00344	0.00674	6	2.47 %

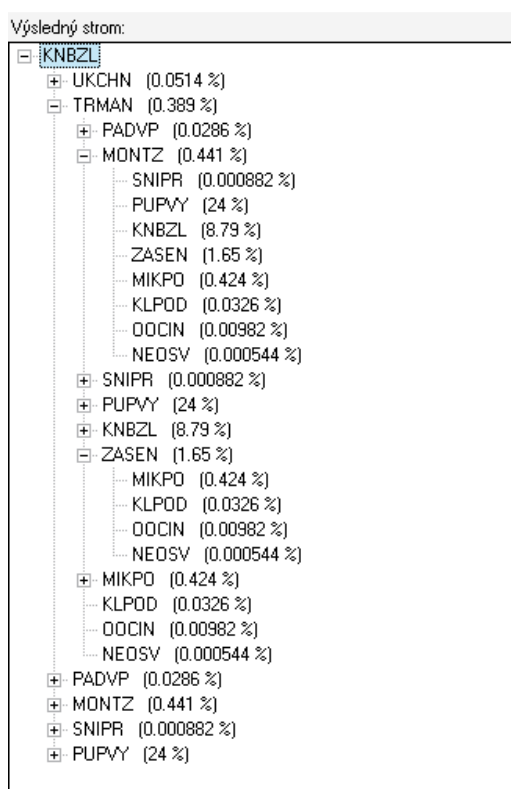
0%	HSPOL	EKOL	OBYV	OMAJ					
	30	10	40	10	0	0	0	0	
	15	25	30	15	1	0	0	0	
	1.5	2.5	12	1.5	11	0	11	0	28

Obrázek 14: Okno Hodnota prvků¹¹

¹¹ zpracováno autorem

3.4.6 Výsledky

Okno výsledky nám umožňuje zobrazit provedené výpočty v grafické podobě. A to buď ve formě výsledného stromu, který si můžeme nechat zobrazit pro každou událost. Zde jsou pak uvedeny všechny události, které jsou příčinou vzniku dané události (včetně uvedení počtu procent jejich vlivu).



Obrázek 15: Výsledný strom¹²

Dále je možno zobrazit výsledky v podobě bodového grafu, kde je možné nechat zakreslit všechny sledované parametry (tedy pravděpodobnost vzniku, procentuální vliv, procento zranitelnosti atd.). Zde se ovšem projevuje, podle mého názoru, velký nedostatek programu SFERA. V případě více hrozeb, nanesených na ose x, nejsou tyto hrozby zobrazeny všechny, protože program neumí „roztáhnout“ okno s grafem do příslušné velikosti. Z tohoto důvodu je potom uživatel nucen přenést data do jiného programu, který je schopen výsledky zobrazit správně (v mém případě se jedná

¹² zpracováno autorem

o program MS Excel). Pro tyto účely slouží záložka Export, která je umístěna v liště nástrojů, kde je možno si vybrat, do jakého typu souboru data přeneseme.

3.4.7 Soubory projektu

Toto okno je určeno pro ukládání zpracovaného projektu a je zde také možnost vypočítaná data importovat do jiného, již existujícího projektu.

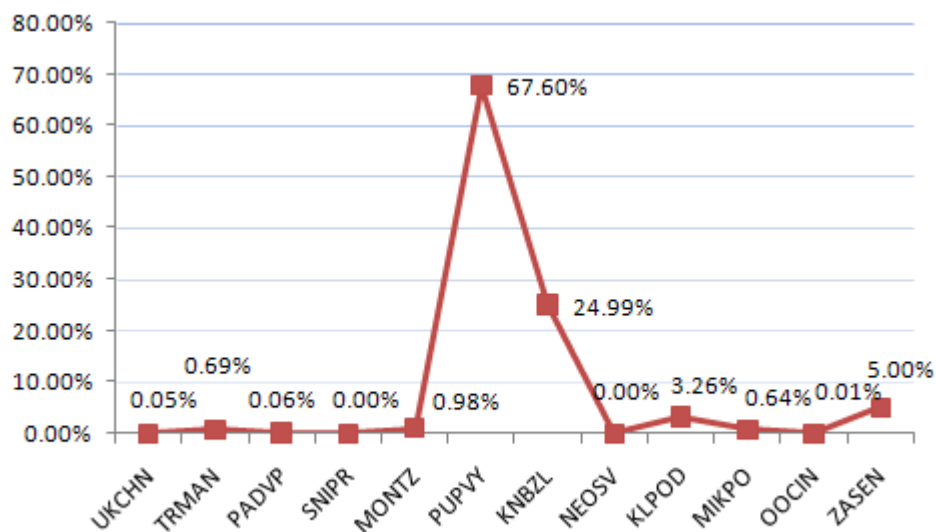
3.5 Vyhodnocení výsledků

V následující tabulce jsou sledovaná rizika rozdělena do tří kategorií podle procentuálního vlivu na systém. Kritická jsou ta, na která by měl mít podnik vždy vypracovaná opatření, u netolerovatelných pak opatření zvážit a zpracovat preventivní opatření následně. Respektovatelná rizika jsou ta, o kterých uvažujeme zpravidla v rámci preventivní přípravy na řešení rizik kritických a netolerovatelných.

Zkratka rizika	Vstupní (P)	Koeficient (P)	Zranitelnost	Nová (P)	Váha pořadí	Procentuální vliv
Kritická rizika						
PUPVY	0.00022	2.22E-05	56	0.00985	0.276	67.6
KNBZL	0.00611	0.000612	10.5401	0.00405	0.03603	12.05
ZASEN	0.01111	0.001112	3.92	0.0104	0.02042	5
Netolerovatelná rizika						
KLPOD	0.00556	0.000556	0.2401	0.00056	0.00013	3.26
MONTZ	0.00185	0.00016	0.9632	0.00826	0.00398	0.975
TRMAN	0.03333	0.003334	0.4862	0.01152	0.00281	0.688
MIKPO	0.01111	0.001112	3.12	0.00168	0.00262	0.641
Respektovatelná rizika						
PADVP	0.02222	0.00222	0.0482	0.01096	0.00026	0.0646
UKCHN	0.03333	0.00333	0.02401	0.00874	0.00021	0.0514
OOCIN	0.01667	0.00167	0.02401	0.00167	4.00E-05	0.00982
SNIPR	0.00139	0.00014	0.02401	0.00015	3.60E-06	0.00088
NEOSV	0.00185	0.000185	0.048	0.0002	4.70E-06	1.20E-05

Tabulka 7: Výsledné hodnoty analýzy¹³

¹³ zpracováno autorem



Obrázek 16: Procentuální vliv sledovaných rizik na systém¹⁴

Jak je patrné z tabulky xxx a grafu xxx, nejvýraznějším rizikem je pro společnost riziko požáru, úniku plynu a výbuchu. Jeho vliv dosahuje téměř 68 %. Tento fakt je způsoben tím, že jednotlivá tato rizika zahrnutá do jedné kategorie by byla pro podnik závažná pouze samostatně.

Podnik má pro tato rizika zpracovány samostatné směrnice (Práce s otevřeným ohněm a rozpálenými předměty, Zajištění bezpečnosti a ochrany zdraví při práci v prostředí s nebezpečím výbuchu, Únik nebezpečných plynů¹⁵), ale ve své směrnici Identifikace a hodnocení rizik k nim přistupuje jako k celku.

Naopak zde můžeme sledovat rizika (např. snížená průchodnost, nebo nedostatečné osvětlení), která mají na systém tak malý vliv, že jejich výsledné hodnoty jsou zanedbatelné.

Výsledné hodnoty bohužel není možno porovnat s výsledky společnosti Synthesia. Rizika uvedená ve směrnici Identifikace a hodnocení rizik nejsou žádným způsobem ohodnocena a je zde uvedena pouze matice, která udává jakým způsobem jsou rizika ve firmě ohodnocována, ovšem konkrétní zařazení sledovaných rizik není ve směrnici sděleno.

¹⁴ zpracováno autorem

¹⁵ dostupné na: <http://www.synthesia.eu/cz/Legislativa>

3.6 Zhodnocení metody SFERA

Analýza rizik metodou SFERA má své kladné i záporné stránky. Mezi klady patří relativně rychlé zpracování celé analýzy a snadné pochopení fungování programu. Jako největší zápor bych označil technické zpracování programu. Program je velice nestabilní a často dochází k jeho „zamrznutí“. Z tohoto důvodu je potřeba si jednotlivé provedené kroky ukládat. Dále je nutné vyvarovat se diakritiky a místo desetinných čárek je nutné používat tečku. Dalším technickým nedostatkem je již výše zmíněná nemožnost upravit si velikost okna grafu. Chybí mi zde také automatické sečtení dekomponovaných prvků při závěrečném vyhodnocování dat.

3.7 Doporučení

Jak již bylo výše zmíněno, je především potřeba věnovat prevenci vzniku požáru, výbuchu, úniku nebezpečných plynů, kontaktu s nebezpečnou látkou a zasažení energiemi. Z tohoto důvodu je potřeba, aby byla kladena zvýšená pozornost na dodržování příslušných směrnic, které se týkají těchto rizik. Je potřeba, aby byly v podniku konány pravidelné i nahodilé kontroly dodržování bezpečnosti práce, a také je nutné neopomenout klást důraz na vzdělávání zaměstnanců v oblasti bezpečnosti práce. Důležitým faktorem je kontrola používání ochranných pomůcek a dodržování schválených technologických postupů ve výrobě. Dále je nutná pravidelná a důkladná kontrola technických zařízení, která mohou tato rizika způsobit,

Je také potřeba, aby podnik vzal v úvahu rizika jako jsou zemětřesení, pád letadla do areálu společnosti, popřípadě hrozba teroristického útoku. Jejich pravděpodobnost se sice zdá být miziva, ale v případě jejich nastání mohou být následky velice rozsáhlé. Proto je potřeba, aby společnost tato rizika zapracovala do svého seznamu potencionálních rizik a učinila konkrétní opatření pro případ jejich vzniku. Konkrétně mám na mysli zpracování krizového plánu. Krizový plán by pak zajistil, že vedení podniku a jeho zaměstnanci budou vědět, jak se v takové mimořádné události zachovat, a co udělat proto, aby byly následky této události co nejmenší.

Závěr

Diplomová práce byla zaměřena na analýzu rizika a provedení konkrétní analýzy ve vybraném podniku. Prevence rizik musí být chápána jako trvalý a nepřetržitý proces a to nejen vrcholovým managementem podnikatelských subjektů, ale také vlastními zaměstnanci a v neposlední řadě také kompetentními orgány státní správy, a proto je této problematice potřeba věnovat zvýšenou pozornost.

Práce měla stanoveny tyto dva cíle. Tím prvním bylo seznámit čtenáře s teoretickou rovinou daného problému. Tomu cíli byla věnována část s názvem Teorie rizika, kde jsou definovány a popisovány základní pojmy, které se této oblasti týkají, a dále část nazvaná Analýza rizik obecně, v níž byla pozornost věnována podrobněji pojmu analýza rizik, a uvedeny příklady vybraných metod k analýze používaných.

Druhým cíle byla stanovena analýza rizik v Synthesii a. s. metodou SFERA. V této části byla podrobně představena společnost a metoda SFERA, kterou byla analýza rizika provedena. Byla nastavena potřebná kritéria potřebná pro provedení analýzy, zadána data do programu. Výsledky byly interpretovány jak v textové tak grafické podobě. Ze získaných údajů byly poté vyvozeny logické závěry. Nakonec jsou v práci uvedena doporučení, která z analýzy vyplynula.

Domnívám se, že cíl práce, deklarovaný v úvodu, jsem splnil.

Seznam použité literatury

Literatura

- [1] SMEJKAL, V., RAIS, K.: Řízení rizik, 1. vyd., Praha: Grada, 2003, 270 s., ISBN 80-247-0198-7.
- [2] TICHÝ, M.: Ovládání rizika. 1. vyd., Praha: C. H. Beck, 2006, 396 s., ISBN 80-7179-415-5.
- [3] MACH, J., KLAVÍK, J., Pojištění průmyslových a podnikatelských rizik, bakalářská práce, Pardubice: Univerzita Pardubice, 1996.
- [4] WALTER, J.: Teorie rizika, Praha: Vysoká škola ekonomická, 1994, 83 s., ISBN 80-7079-401-1.
- [5] ROUDNÝ, R., LINHART, P.: Krizový management III. Teorie a praxe rizika, Pardubice: Univerzita Pardubice, 2007, 174 str., ISBN 80-7194-924-8.
- [6] FARAZMAND, A.: Handbook of crisis and emergency management, New York: Marcel Dekker Inc., 2001, 788 s., ISBN 0-8247-0422-3.
- [7] MARSHALL, V. C.: Major chemical hazards, Chichester: Ellis Horwood, 1987, 587 s., ISBN 0470208139.
- [8] MOZGA, J., VÍTEK, M.: Udržitelný rozvoj a řízení rizik, pohrom a krizí, Hradec Králové: Gaudeamus, 2002, 331 s., ISBN 80-7041-293-3
- [9] ŠEBESTA M., SCHWARZ R.: Management rizik s pravděpodobnostním přístupem ke stanovení rizik, Brno: Vojenská akademie v Brně, 2003, 63 s.
- [10] ŠIMÁK, L., Krizový manažment vo verejnej správe, Žilina: Žilinská univerzita v Žiline, 2004, 243 s., ISBN 80-88829-13-5.

[11] ROUDNÝ, R., LINHART, P. Krizový management I. ochrana obyvatelstva, mimořádné události. 1.vyd. Pardubice: Univerzita Pardubice, 2004. 97 s., ISBN 80-7194-674-5.

[12] SMEJKAL, V., RAIS, K.: Řízení rizik ve firmách a jiných organizacích, Praha: Grada Publishing, a. s., 2006, 300 s. ISBN 80-247-1667-4

Internet

[13] BABINEC, F., Management rizika

URL: <<http://www.math.slu.cz/studmat/AnalyzaRizik/AnalyzaRizik-1.pdf>>

[cit. 18.3. 2010].

[14] Metoda FMEA

URL: < <http://www.komora-khk.cz/business/documents/?soubor=moduly/5-jakost/12-neustale-zlepsovani/12-2-fmea.pdf>> [cit. 15.3. 2010].

[15] Agrofert, a. s. Výroční zpráva 2008

URL:

<<http://www.justice.cz/xqw/xervlet/insl/getFile?listina.@slCis=600168785&listina.@rozliseni=pdf&listina.@klic=58a5661a77166742bcc29012cd8801c4>> [cit. 3.3. 2010].

[16] MÍKA, O., Analýzy rizika v procesu prevence závažných havárií

URL:

<http://www.egozlin.cz/upload.cs/a/a45a3244_1_mika_isatech_bрно_2002_b.pdf>

[cit. 12.3. 2010].

[17] HZS Moravskoslezského kraje

URL: <<http://www.hzsmsk.cz/index.php?a=cat.74>> [cit. 16.3. 2010].

[18] MIKO, K. Systémový bezpečnostní audit

URL: < http://www.dcit.cz/files/bezpecnost/ITS_syst_bezp_audit.pdf> [cit. 21.3. 2010].

[19] FMEA a Risk Management.

URL: <<http://www.ikvalita.cz/tools.php?ID=51>> [cit. 21.3. 2010].

[20] MINISTERSTVO VNITRA, Generální ředitelství HZS, Seznam – Přehled metodik pro analýzu rizik

URL: <<http://aplikace.mvcr.cz/archiv2008/hasici/planovani/metodiky/mzprakp.pdf>> [cit. 6.3. 2010].

[21] MINISTERSTVO VNITRA, Generální ředitelství HZS, Řešení mimořádných událostí a krizových situací

URL: <http://aplikace.mvcr.cz/archiv2008/udalosti/prirucky/obce/reseni_mu.pdf> [cit. 13.3. 2010].

[22] STUHLÁ, K., Analýza rizika a havarijní plánování

URL:

<http://www.google.cz/url?sa=t&source=web&ct=res&cd=1&ved=0CAYQFjAA&url=http%3A%2F%2Fwww.hzsmsk.cz%2Fsklad%2Fkrao%2Fpublikace%2FIOO_Analyza_rizika_HP.doc&ei=cHDUS7K1OtGoOIKX1YMO&usg=AFQjCNF635hoaD6emEHZCamGWqGcX6Wi1A> [cit. 9.3. 2010].

[23] Metodiky hodnocení rizik

URL: <www.movoz.cz/download/metud.doc> [cit. 6.3. 2010].

[24] 240/2000 Sb. krizový zákon

URL:

<http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=240/2000&PC_8411_p=2&PC_8411_l=240/2000&PC_8411_ps=10#10821> [cit. 19.3. 2010].

[25] Gubka, K. Riziko, jeho zdroje a možnosti ochrany proti riziku

URL:<http://www.fce.vutbr.cz/veda/dk2004texty/pdf/05_Ekonomika%20a%20rizeni%20stavebnictvi/5_01_Ekonomika%20investic/Gubka_Karol.pdf> [cit. 27.2. 2010].

[26] Synthesia, a. s., historie

URL: < <http://www.synthesia.eu/cz/O-nas/Historie> > [cit. 27.2. 2010].

[27] Synthesia, a. s., obchod

URL: < <http://www.synthesia.eu/cz/Obchod> > [cit. 27.2. 2010].

Ostatní

[28] SVOBODA, O. Vícekriteriální analýza rizik. In Sborník Krizový management.

Lázně Bohdaneč : IOO. 2008. s. 4. ISBN 978-80-7194-951-0.