

Návrh zabezpečení průmyslového areálu s komparací efektivnosti různých přístupů

René Grudnik



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	René Grudník
Osobní číslo:	A22133
Studijní program:	B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia:	Kombinovaná
Téma práce:	Návrh zabezpečení průmyslového areálu s komparací efektivnosti různých přístupů
Téma práce anglicky:	Security Proposal for an Industrial Area with a Comparison of the Effectiveness of Different Approaches

Zásady pro vypracování

1. Uveďte základní terminologii a základy řízení rizik.
2. Charakterizujte vybraný průmyslový areál.
3. Popište současný stav.
4. Proveďte analýzu rizik a její vyhodnocení.
5. Na základě výsledků analýzy rizik navrhnete tři návrhy bezpečnostních opatření a proveďte jejich komparaci.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management V. 5.* VeRBuM, 2015. ISBN 978-80-8750-067-5.
2. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II. 2.* VeRBuM, 2012. ISBN 978-80-8750-019-4.
3. KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií.* Komora podniků komerční bezpečnosti ČR, 2014. ISBN 978-80-260-7115-0.
4. ĎURICA, Jakub; BOROŠ, Martin a MACH, Vlastimil. *Bezpečnostné systémy – Mechanické zábranné systémy.* EDIS, 2022. ISBN 9788055418858.
5. MAREŠ, Miroslav; REKTOŘÍK, Jaroslav a ŠELEŠOVSKÝ, Jan. *Krizový management: Případové bezpečnostní studie.* Eko-press, 2013. ISBN 978-80-86929-92-7.

Vedoucí bakalářské práce: **Ing. Lukáš Kotek**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **23. listopadu 2024**

Termín odevzdání bakalářské práce: **2. června 2025**



doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 23. listopadu 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Bakalářská práce se zabývá analýzou rizik na vybraném objektu. Cílem práce je najít, analyzovat a vhodně ohodnotit rizika na objektu a najít vhodné zabezpečení s přihlédnutím na cenu všech řešení. Teoretická část je zaměřena na terminologii k řízení rizik. Následná část se zabývá aktuálním zabezpečením na objektu a vybranou analýzou. Praktická část představuje celý areál, vybranou analýzu a návrh opatření včetně cenových výpočtů ke každému opatření.

Klíčová slova: analýza rizik, řízení rizik, riziko, hrozba.

ABSTRACT

This thesis deals with the risk analysis of the selected object. The aim of the work is to find, analyze and evaluate the risks on the object and to find the most suitable security taking into account the cost of all solutions. The theoretical part focuses on the terminology to risk management. The subsequent part deals with the actual security on the object and the selected analysis. The practical part presents the whole site, the selected analysis and the design of the measures including cost calculations for each measure.

Keywords: risk analysis, risk management, risk, threat.

Chtěl bych poděkovat svému vedoucímu panu Ing. Lukáši Kotkovi za jeho cenné rady, trpělivost a odborné vedení mé bakalářské práce. Trpělivost, ochota pomoci a znalosti pana Ing. Lukáše Kotka byly klíčové pro úspěšné dokončení mé bakalářské práce. Dále bych chtěl poděkovat své ženě a rodině, která mě morálně podporovala při průchodu mým studiem. Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	13
1 ŘÍZENÍ RIZIK.....	14
1.1 TERMINOLOGIE ŘÍZENÍ RIZIK	15
1.1.1 Aktivum.....	16
1.1.2 Hrozba	17
1.1.3 Zranitelnost	17
1.1.4 Bezpečnostní opatření	18
1.1.5 Riziko	18
1.1.6 Zbytkové riziko	19
1.1.7 Narušení	19
1.2 ZÁKLADY ŘÍZENÍ RIZIK.....	20
1.2.1 Krok 1 – určení si oblasti řízení rizik.....	20
1.2.2 Krok 2 – vytvoření si detailního seznamu hrozeb.....	20
1.2.3 Krok 3 – identifikace a zhodnocení rizik	21
1.2.4 Krok 4 – vybrání ohrožujících rizik – prioritizace.....	21
1.2.5 Krok 5 – zvolení si postavení k rizikům	21
1.2.6 Krok 6 – reakce na situaci, stálé přehodnocování.....	21
1.3 ZÁVĚR KAPITOLY	22
2 SYSTÉMY TECHNICKÉ OCHRANY.....	23
2.1 MECHANICKÉ ZÁBRANNÉ SYSTÉMY	24
2.2 ELEKTRONICKÉ SYSTÉMY	25
2.3 FYZICKÁ OSTRAHA NA OBJEKTU.....	27
2.4 ZÁVĚR KAPITOLY	28
3 VYBRANÉ ANALÝZY RIZIK.....	29
3.1 HYBRIDNÍ METODA ANALÝZY RIZIK	29
3.2 KVALITATIVNÍ METODY ANALÝZY RIZIK	29
3.2.1 Metoda matice rizik.....	30
3.2.2 Kontrolní checklist.....	31
3.2.3 Metoda what if – co když.....	31
3.2.4 SWOT analýza	32
3.3 KVANTITATIVNÍ METODY ANALÝZY RIZIK.....	33
3.3.1 Analýza selhání a jejich dopadů – FMEA.....	34
3.3.2 Analýza stromu poruch (FTA)	35
3.3.3 Analýza stromu událostí (ETA)	37
3.3.4 Analýza lidské spolehlivosti (HRA)	38
3.3.5 Analýza ohrožení a provozuschopnosti (HAZOP)	39
3.4 ZÁVĚR KAPITOLY	40
II PRAKTICKÁ ČÁST	41

4	CHARAKTERISTIKA PRŮMYSLOVÉHO AREÁLU.....	42
4.1	SEVERNÍ ČÁST AREÁLU	48
4.2	JIŽNÍ ČÁST AREÁLU	51
4.3	VÝCHODNÍ ČÁST AREÁLU	54
4.4	ZÁPADNÍ ČÁST AREÁLU	55
4.5	STŘEDNÍ ČÁST AREÁLU	55
4.6	ZÁVĚR KAPITOLY	56
5	SOUČASNÝ STAV BEZPEČNOSTNÍCH OPATŘENÍ NA OBJEKTU	57
5.1	REŽIMOVÁ OPATŘENÍ	61
5.2	FYZICKÁ OSTRaha NA OBJEKTU	62
5.3	ZÁVĚR KAPITOLY	62
6	IDENTIFIKACE AKTIV A HROZEB NA OBJEKTU	63
6.1	IDENTIFIKACE AKTIV	63
6.1.1	Odhad hodnoty aktiv	65
6.2	IDENTIFIKACE HROZEB	65
6.2.1	Hrozby lidského faktoru	66
6.2.2	Technologické hrozby	66
6.2.3	Přírodní hrozby	66
6.2.4	Výpis identifikovaných hrozeb	67
6.3	ANALÝZA RIZIK METODOU KONTROLNÍHO SEZNAMU	69
6.4	ANALÝZA RIZIK METODOU FMEA	72
6.5	VYHODNOCENÍ ANALÝZY RIZIK	79
6.5.1	Vyřešení nalezených rizik	80
6.6	ZÁVĚR KAPITOLY	81
7	NÁVRH BEZPEČNOSTNÍHO OPATŘENÍ.....	82
7.1	NAVÝŠENÍ POČTU FYZICKÉ OSTRahY	82
7.2	ZABEZPEČENÍ POUZE TECHNOLOGIEMI	82
7.3	ZABEZPEČENÍ KOMBINACÍ FO A TECHNOLOGIEMI	84
7.4	KOMPARACE EFEKTIVNOSTÍ	86
7.5	ZÁVĚR KAPITOLY	87
	ZÁVĚR.....	88
	SEZNAM POUŽITÉ LITERATURY	90
	SEZNAM OBRÁZKŮ	94
	SEZNAM TABULEK.....	95
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	96

ÚVOD

Řešení bezpečnosti v průmyslových nebo bývalých průmyslových areálech je velmi složitá věc. Mnoho již bývalých průmyslových areálů se průběžně mění na lukrativní areály s možností rekreace, nákupu nebo i bydlení, a proto je potřeba se věnovat bezpečnosti v těchto nově zrenovovaných areálech. Jelikož průmyslové areály nebyly určeny pro obvyčejné návštěvníky, nedbalo se ani na bezpečnost s tím spojenou.

Úvodní část bakalářské práce se zaměřuje na řízení rizik a s ní spojenou terminologii, které jsou základem pro další části bakalářské práce a analýzu rizik v oblasti zabezpečení průmyslového areálu. Jsou zde vysvětleny pojmy jako aktivum, hrozba, zranitelnost, bezpečnostní opatření, riziko, zbytkové riziko a narušení. Na tuto část navazují základy řízení rizik, kde jsou vypsány základní kroky.

Dále se v teoretické části bakalářská práce zaměřuje na systémy technické ochrany jako celek. Následně jsou více dopodrobna rozepsané kapitoly týkající se mechanických zábranných systémů, elektronických systémů a fyzické ostrahy na objektu, jelikož toto jsou prvky, které se v areálu vyskytují. V závěru teoretické části se bakalářská práce zaměřuje na vybrané metody analýzy rizik, které jsou rozděleny na kvalitativní a kvantitativní metody včetně konkrétních příkladů.

Praktická část se již zabývá konkrétním popisem nejmenovaného již bývalého průmyslového areálu. Je zde popsán aktuální stav zabezpečení na objektu, charakterizace areálu a vypracovaná detailní analýza rizik. V rámci vypracované analýzy jsou identifikována aktiva hrozby a následně rizika, která mohou mít vliv na bezpečnost v tomto areálu. Pro analýzu byly vybrány dvě metody analýzy rizik, a to kontrolní seznam z kvalitativních metod a kvantitativní metoda FMEA (Failure Mode and Effect Analysis), která již zahrnuje i návrh opatření na nalezené riziko.

Poslední kapitola bakalářské práce se zaměřuje na návrh zabezpečení s rozdílným přístupem. V první části je zabezpečení řešeno pouze fyzickou ostrahou, dále pak pouze technologiemi a na závěr kombinací fyzické ostrahy a technologií, tak aby došlo ke zlepšení bezpečnostní situace s přihlédnutím na vložené prostředky k zajištění bezpečnosti.

Cílem této bakalářské práce je nalézt a identifikovat rizika v areálu a poskytnout tak přehledná a praktická doporučení pro zvýšení bezpečnosti, a to s důrazem na efektivnost při řízení rizik a implementaci nových moderních bezpečnostních řešení. Tato bakalářská práce

tak přispívá k porozumění problematiky včetně nalezení konkrétního řešení pro vybraný areál, který by dále mohl být uplatňován na obdobných areálech.

I. TEORETICKÁ ČÁST

1 ŘÍZENÍ RIZIK

Řízení rizik je jedním z nejdůležitějších procesů, které zajišťují stabilitu a dlouhodobou udržitelnost každé firmy. Tento obor je velmi specifický a přístup k němu se tak musí přizpůsobit individuálním potřebám v každé organizaci. V závislosti na typu výroby, případně charakteru činnosti konkrétní firmy nebo umístění výrobního závodu je třeba brát ohled na mnoho faktorů. Například pokud je výrobní závod v zátopové oblasti, pak je třeba řešit riziko spojené s povodněmi. Nebo naopak výrobní areály v průmyslových zónách musí často čelit hrozbám spojených s výpadky technologií nebo řešit dopad jejich činnosti na životní prostředí. Je tedy potřeba si určit hrozby a rizika a zamezit tak jejich existujícímu nebo i předpokládanému působení.

Prvním krokem je tedy vždy důkladná identifikace aktuálních i budoucích rizik a hrozeb, protože jen tak lze minimalizovat dopady již existujících, ale případně i potenciálních problémů.

Na základě výstupních dat z potřebných analýz rizik následně krizový management nebo vedení společnosti vypracuje potřebnou strategii a navrhne adekvátní řešení v podobě bezpečnostních řešení, která následně minimalizují nebo zcela eliminují dané riziko. [1][2]

Každá firma musí znát tři důležité parametry:

1. Identifikace hrozeb: Firma musí vědět, co jí může ochromit, ohrozit nebo i zcela zlikvidovat.
2. Preventivní opatření: Firma musí vždy dělat maximum, aby těmto situacím předcházela nebo zcela zabránila.
3. Plán reakce: Firma zcela přesně ví, co v takové situaci dělat, pokud taková situace již nastane a umí se zní co nejlépe zotavit, a to na základě připraveného plánu.[2][3]

Firmy se však často potýkají nejen s přírodními katastrofami, jako je povodeň, vichřice nebo bouře, ale i s problémy v systému. Například výpadek dodavatelského řetězce nebo lidské chyby – faktorů. Z tohoto důvodu je nutné na každý typ hrozby vyžadovat jiný přístup. Před povodněmi je možné investovat do odolnější infrastruktury nebo systémů varování. Problémy s lidským faktorem mohou být eliminovány pravidelnými školeními pracovníků. Problém s dodavatelským řetězcem může řešit řádná zásoba, případně mít více dodavatelů.

Firmy ovšem nemohou pouze brát v potaz například přírodní katastrofy, ale musí počítat i s finančními hrozbami, které jsou spojeny i právě s přírodními katastrofami. Mezi finanční hrozby patří ekonomická krize spojená s vysokou inflací, pádem ekonomiky v republice nebo i celosvětovou hospodářskou krizí, které se ovšem v některých situacích špatně předvídají, a ne vždy se na ně dá pružně reagovat. Příkladem toho byla pandemie viru Covid-19. Tato pandemie zasáhla celosvětovou ekonomiku a způsobila významné výpadky nejen ve výrobě, ale i v poskytování služeb. Na základě toho mnoho firem, zejména pak malých a středních podniků, nebylo na takovou situaci připraveno. Nedostatek zásob, uzavření provozoven a dlouhodobé omezení činnosti následně vedly ke krachu velkého množství firem nejen v České republice. Tato událost jasně ukázala, jak důležité je mít připravený plán pro nestandardní situace.[3]

S riziky jako takovými můžeme spojit každé oddělení, jako je marketingové oddělení, oddělení rozpočtů, technologické oddělení a další. Na všechny tyto oblasti musí být tedy z hlediska dlouhodobé udržitelnosti a udržení si dobrého jména firmy vytvořeny plány pro řízení rizik, která tak sníží následky vzniklé danou hrozbou, nebo tuto hrozbu eliminují. [1]

Celkově je tedy cílem řízení rizik zajistit kontinuitu podnikání, stabilitu firmy na trhu, minimalizovat dopady všech potenciálních hrozeb a vytvořit takové podmínky, aby organizace mohla i nadále efektivně fungovat. Úspěšné řízení rizik je tedy nejen otázkou bezpečnosti ve firmě, ale také zajištění dlouhodobé konkurenceschopnosti na trhu. Bez dobře navrženého a implementovaného systému řízení rizik by tak firmy nebyly schopny čelit výzvám dnešního podnikání. Efektivní řízení rizik navíc poskytuje firmě konkurenční výhodu, jelikož ji umožňuje rychleji se adaptovat na měnící se podmínky a minimalizuje tak ztráty spojené s neočekávanými situacemi, které mohou nastat. [1][2][3]

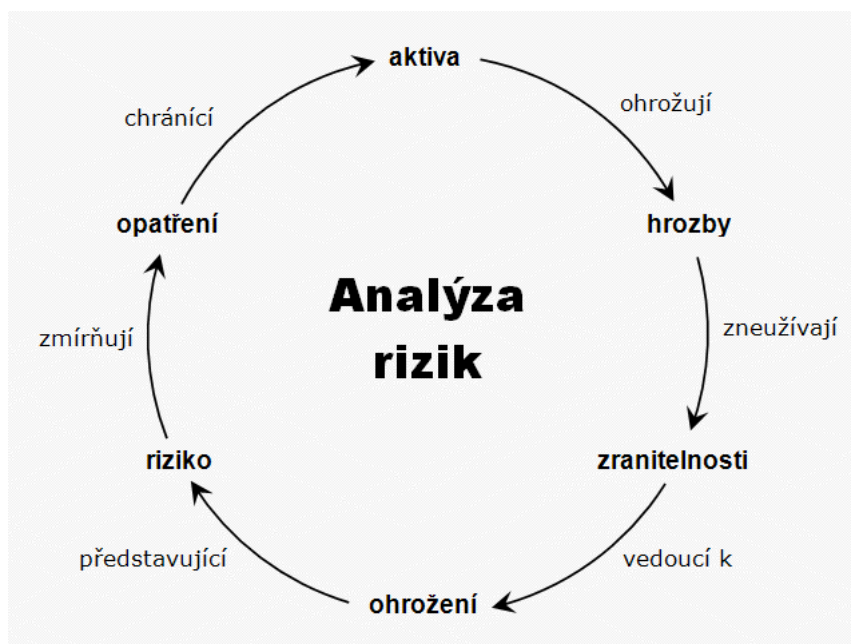
1.1 Terminologie řízení rizik

Aby bylo možné se dále věnovat analýze rizik, je potřeba si nejprve určit terminologii, která je pro téma řízení a analýzu rizik důležitá.

Bezpečnostní analýza je:

„Bezpečnostní analýza je proces objektivního zhodnocení stavu a funkčnosti opatření fyzické ochrany, který slouží jako základ pro nastavení účinného bezpečnostního systému. Tento proces zahrnuje identifikaci a hodnocení rizik, jež mohou ovlivnit bezpečnost osob, majetku nebo informací, a následně navržení opatření k minimalizaci těchto rizik.

Bezpečnostní analýza je klíčovým nástrojem pro tvorbu účinných bezpečnostních strategií a politik. “ [4] [5]



Obrázek 1 Obecné schéma analýzy rizik

(Zdroj: [5])

1.1.1 Aktivum

Prvním termínem, který je potřeba objasnit, je aktivum. Pro firmu je to veškerý majetek, know-how, informace, ale i zaměstnanci, nájemníci a jiné věci, které mají pro danou firmu nějakou hodnotu. Působením hrozby by tato hodnota mohla být ponížena, z tohoto důvodu ji firma chrání. [5]

Na analyzovaném objektu se jedná o budovy, služební vozidla, vybavení kanceláří a komerčních prostor, dále se jedná o autonomní brány, turnikety, zaměstnance, nájemníky, know-how a informacích potřebné pro fungování firmy. Celkové nacenění se pohybuje v desítkách miliónů korun.

Aktiva se mohou dělit na:

- Hmotná aktiva
 - Jedná se o fyzická aktiva jako jsou například nemovitosti, zboží, firemní vozidla, cenné papíry nebo finanční prostředky.
- Nehmotná aktiva

- Jedná se o nemateriální aktiva, fyzicky na ně nelze dosáhnout. Může jít o know-how firmy, prestiž firmy, autorská práva, kvalita personálu, výrobku nebo informace. [6]

1.1.2 Hrozba

„Hrozba je jakákoliv událost, síla, osoba nebo vlastnost, která působí přímo na aktivum nebo na bezpečnostní opatření, a to s cílem získat tak přístup k danému aktivu a poškodit nebo ho zcela zničit.“ [5]

Hrozby je možné rozdělit do dvou skupin – dle úmyslu a zdroje. [5]

Dělení dle úmyslu:

- Úmyslné hrozby
 - Tato hrozba je plánovaná a může být způsobena jedincem nebo i skupinou. Promyšlené hrozby mohou plánováním zabrat měsíce i roky a následně je spuštěna jedincem nebo skupinou, zpravidla se jedná o vraždy, krádeže většího rozsahu, teroristické útoky nebo ozbrojené konflikty. Ovšem může se jednat i o zneužití pravomocí výše postavené osoby, zpronevěření finančních prostředků firmy, neoprávněné užívání aktiv, neoprávněnému přístupu do nebo k aktivu nebo záměrné poškození firmy na trhu například snížením výroby nebo zásahem do zásobování výrobních linek.
- Neúmyslné hrozby
 - Jsou to hrozby, které nebyly nijak plánované a dochází k nim zcela náhodně. Zpravidla se jedná o přírodní katastrofy jako je požár, povodně, zemětřesení, pandemie. Dále se může jednat o výpadek elektrického proudu, odstávky nebo prasknutí vodovodního potrubí. Také může jít o lidskou chybu, kdy k hrozbě dojde nepozorností zaměstnance, popřípadě se může jednat o chybu obsluhy nebo dopravní nehodu. [7]

1.1.3 Zranitelnost

Zranitelnost pak vyjadřuje určitý nedostatek, slabinu, stav aktiva nebo i bezpečnostního opatření, které může být zneužito ve prospěch hrozby. Jednoduše řečeno se dá říct, že se

jedná o slabá místa, která jsou následně hrozbou využita k poškození nebo zničení aktiva. [8]

Zranitelnost se bere v potaz tam, kde dochází, nebo může docházet k vzájemnému působení mezi hrozbami a aktivy. [8][9]

Hodnota zranitelnosti je tvořena dvěma základními faktory:

- Citlivost
 - Citlivost vyjadřuje náchylnost aktiva být danou hrozbou poškozeno.
- Kritičnost
 - Kritičnost nám vyjadřuje, jak cenné aktivum pro firmu je. [10]

1.1.4 Bezpečnostní opatření

Bezpečnostní opatření je opatření na úrovni fyzické, logické nebo administrativní bezpečnosti (například nový postup nebo proces). Toto opatření pak vzniká na základě provedené analýzy rizik, zkušeností nebo jen pozorováním, které nám snižuje, nebo zcela odstraňuje zranitelnost či hrozbu a chrání tak aktivum, což následně vede ke snížení rizika. Účelem bezpečnostních opatření je předejít vzniku bezpečnostního incidentu a v případě již existujícího bezpečnostního incidentu zmírnit co nejvíce její následky. Při navrhování nového bezpečnostního opatření či vylepšování již stávajícího, by se nemělo zapomenout, že i toto bezpečnostní opatření má svou hodnotu, čímž nám zvyšuje hodnotu chráněných aktiv. Z tohoto důvodu by se nemělo zapomínat na zvážení nákladů vynaložených na toto bezpečnostní opatření a hodnotu chráněného aktiva. [11]

Příkladem je zabezpečení skladu, kdy bezpečnostní opatření bude stát 50.000 Kč, kdy ve skladu mám zboží za 5.000 Kč není ekonomicky příliš výhodné.

1.1.5 Riziko

„Pojem riziko nemá jasně uvedenou definici, jelikož v každém oboru může riziko znamenat něco jiného. Obecně se však riziko bere jako pravděpodobnost, že dojde hrozbou ke zneužití zranitelnosti, kde dojde k narušení důvěrnosti, integrity nebo i dostupnosti. Riziko se vždy dá odvodit a je přímo odvozené od konkrétní hrozby, přičemž míra rizik, jinak řečeno, jaká je pravděpodobnost škodlivých následků, které z hrozby a konkrétní zranitelnosti vyplývají vůči chráněnému aktivu, lze posoudit na základě provedené analýzy rizik.“ [12][13]

U rizik je nebezpečné to, že se s časem neustále mění.

Důležité charakteristiky pro rizika jsou:

- Ovlivnitelnost
 - Do jaké míry lze rizika ovlivnit.
- Předvídatelnost
 - Míra, do jaké je možné riziko předem předvídat a určit dané riziko nebo i jeho dopad na systém.
- Akceptovatelnost
 - Do jaké míry je firma ochotna dané riziko akceptovat a zda je pro firmu únosné.
- Pravděpodobnost vzniku a působení rizika
 - Jaká je pravděpodobnost, že dané riziko vznikne a jak bude působit na systém nebo firmu. [13]

1.1.6 Zbytkové riziko

Za zbytkové riziko se bere takové riziko, které již nebylo možné více ošetřit, případně po zavedení bezpečnostního opatření dané riziko stále zůstává nebo je pro firmu tak zanedbatelné, že jej vedení společnosti, které je odpovědné za zvládání rizik již dále nebere v potaz a nedochází tak k jeho snížení. Nemá-li firma vůbec zavedený management rizik, pak je zodpovědnost na vedení organizace, které určí, jak bude reagovat na dané zbytkové riziko. [14]

1.1.7 Narušení

Narušení je situace, kdy došlo vlivem negativních faktorů k narušení nebo oslabení důvěrnosti, integrity nebo dostupnosti bezpečnostních opatření. Tato situace představuje zranitelnost, které mohou být následně využity hrozbou k aplikování svých negativních vlastností – dosažení škodlivých cílů. Může se jednat o neoprávněnou manipulaci s daty, zneužití systémových zdrojů nebo neoprávněný přístup. Všechny tyto hrozby mohou mít negativní dopad na fungování organizace. [5]

1.2 Základy řízení rizik

Aby řízení rizik mělo pro firmu význam, je potřeba, aby tuto práci dělali lidé, kteří této problematice rozumí. Jelikož se jedná o cyklický proces, kde neustále probíhá identifikace rizik, analýzy rizik, zhodnocení, prioritizace a rozhodnutí, jak s jednotlivými riziky naložit případně se jim postavit.

Základem řízení rizik je určit si, pro jaké odvětví bude zavedeno nebo zda se bude jednat o celou firmu. V dalším kroku je pak potřeba se zaměřit na rozhodovací proces, který již vychází z analýzy rizik. Při rozhodování je potřeba se zaměřit na ovlivňující faktory, kterými může být technické řešení, ekonomika, ale i sociální nebo politický faktor, který může ovlivnit rozhodnutí. [1][2]

Výběr optimálního řešení je nejdůležitější a nejkritičtější fází v řízení rizik. Prvně je potřeba určit úroveň rizika, následně najít optimální řešení i z ekonomického hlediska. Vždy je potřeba mít i více možností k výběru, jak možné dané riziko ošetřit. Po zavedení bezpečnostních opatření je vhodné mít zpětnou vazbu, zda zavedené opatření zafungovalo, jak mělo. Zároveň je potřeba dbát na zbytkové riziko a mít k dispozici plán pro řešení nestandardních situací, který řeší případné vzniknutí bezpečnostního incidentu. [1][2]

1.2.1 Krok 1 – určení si oblasti řízení rizik

Prvním krokem tedy určit si oblast, kterou se bude řízení rizik zabývat.

Typicky to bývá:

- Rizika v rámci celé společnosti
- Rizika BOZP
- Rizika spojená s financemi
- Rizika informační bezpečnosti
- Rizika kybernetické bezpečnosti [2]

1.2.2 Krok 2 – vytvoření si detailního seznamu hrozeb

Krok číslo dva je vytvořit si seznam hrozeb, která mohou mít na společnost vliv a ohrozit je tak. K tomuto docílení je možné využít vhodnou metodu, která managementu rizik napomůže k vytvoření seznamu hrozeb. K tomuto mohou dopomoci aktiva, procesy nebo hrozby, která jsou již známá nebo jsou snadno zjistitelná.

Při zjišťování rizik je vhodné si tato rizika již ohodnotit, jelikož budou velmi nápomocná v dalším kroku.[2]

1.2.3 Krok 3 – identifikace a zhodnocení rizik

Krokem číslo tři je identifikovat a zhodnotit veškerá rizika, a to pomocí vhodné metody analýzy rizik, pokud tak nebylo učiněno již v kroku dva. Při zápisu rizik je potřeba si vždy zapsat detailní informace, jako je dopad na chod firmy nebo pravděpodobnost, že k dané hrozbě či zneužití hrozbou dojde. [2]

1.2.4 Krok 4 – vybrání ohrožujících rizik – prioritizace

Krok číslo čtyři může mít velký dopad na budoucí chod i celkové řízení rizik, pokud při výběru nebude zohledněna priorita nalezených rizik. Poté se může stát, že se bude řešit riziko, které nemá zvláštní dopad na chod či fungování ve firmě a na místo toho se vyskytne riziko, které je pro chod firmy závažné. [2]

Ačkoliv se toto může zdát jako automatické, mnoho manažerů, zaměstnanců i lidí řeší velmi často nezávažné nebo méně závažné problémy a závažnějším problémům se vyhýbají, dokud tento problém nedosáhne kritického bodu. V takovém případě již často bývá pozdě a následný dopad hrozby může mít až katastrofální následky pro firmu.

1.2.5 Krok 5 – zvolení si postavení k rizikům

Jakmile je dostupný seznam existujících rizik a určená priorita všech rizik, pak je potřeba si zvolit, jak se k jednotlivým rizikům zachováme.

Zpravidla je na výběr ze čtyř základních možností, jak se k rizikům postavit:

1. Předejít rizikům vhodným bezpečnostním opatřením
2. Zmírnění dopadu či vzniku rizik například vhodným stanovením procesů nebo postupů
3. Rizika přenesu na někoho jiného – subdodavatel, pojišťovna, zákazník
4. Rizika budou ignorována – například zbytkové riziko [2]

1.2.6 Krok 6 – reakce na situaci, stálé přehodnocování

V kroku číslo šest již existuje vytvořený seznam rizik s detailními informacemi, určenými prioritami a předem definovanými postupy, jak se zachovat při jednotlivých rizicích.

Je však třeba mít na paměti, že rizika se stále mění, a to jak v čase a rozsahu, tak i vlivu na organizaci. Nicméně je nezbytné mít na paměti, že rizika se neustále dynamicky mění a vyvíjejí v čase. Pro firmu to znamená, že je nutné pravidelně a systematicky přehodnocovat veškerá existující, aktuální i potenciální rizika. Důvodem je, že jak bezpečnostní hrozby, tak i opatření na jejich změnu nejsou statické, ale musí být dynamické. Staré riziko může v průběhu času zaniknout, na místo toho nám může vzniknout riziko nové, které si následně žádá okamžitou pozornost a reakci ze strany firmy.

Pro zajištění správného a aktuálního hodnocení rizik i hrozeb je velmi užitečný vnitřní audit, který pomáhá organizacím identifikovat slabiny v jejich nastavených systémech a procesech. Audity jsou pro firmu nástrojem, který může odhalit nejen technologické nedostatky, ale také lidské nebo procesní chyby, které mohou vést k novým rizikům. Velmi často audit ukáže na situace, kdy zaměstnanci nedodržují stanovené bezpečnostní předpisy nebo se jejich chování odchyluje od doporučených praktik, což může vést k vytvoření nových zranitelností a rizik. Z tohoto důvodu je nezbytné pravidelně provádět audity, školení zaměstnanců a testování systémů, aby se nejvíce minimalizovala pravděpodobnost vzniku nových rizik a hrozeb.

Dalším krokem ke zlepšení může být využívání analytických nástrojů a technologií, které firmám umožňují efektivnější sledování a vyhodnocování rizik. Průběžná aktualizace a včasná reakce na nově vzniklá rizika a hrozby je základním předpokladem pro udržení bezpečnosti a stabilní činnosti organizace. [2]

1.3 Závěr kapitoly

První kapitola se věnovala vysvětlení základní terminologie, která je pro řízení rizik typická. Dále se kapitola zabývala základními kroky pro řízení rizik.

2 SYSTÉMY TECHNICKÉ OCHRANY

Systémy technické ochrany představují důležitý prvek k zabezpečení osob, majetku, informací a dalších chráněných zájmů před neoprávněným zásahem, poškozením, krádeží, zneužitím nebo jinou škodlivou činností. Jedná se o soubor technických prostředků a zařízení, které slouží ke zvýšení bezpečnosti a k minimalizaci rizik. Systémy technické ochrany, dále jen STO, jsou často součástí širšího bezpečnostního systému, který zahrnuje také organizační a personální opatření, jako je pravidelné školení zaměstnanců, kontrolní a auditorská činnost nebo nastavení interních bezpečnostních politik ve firmě. Technická ochrana má preventivní i reaktivní charakter, tedy nejen snižuje pravděpodobnost incidentu, ale zvyšuje i schopnost efektivně reagovat v případě jeho výskytu. [15] [16] [17] [18]

Technická ochrana je typicky rozdělena na několik hlavních kategorií. Mezi nejčastěji využívané prostředky patří především poplachové zabezpečovací a tísňové systémy (dále jen PZTS), elektrické požární signalizace (dále jen EPS), kamerové systémy (CCTV), přístupové systémy (ACCESS), mechanické zábranné systémy (MZS) a systémy detekce a kontroly vstupu (ESKV). Kombinace těchto prvků pak vytváří vícevrstvou ochranu, která zajišťuje, že i v případě selhání jedné komponenty zůstane zajištěna ochrana jiným prostředkem STO. [15][19]

PZTS detekují neoprávněný vstup do objektu nebo vymezeného prostoru pomocí různých detektorů jako jsou pohybové, otřesové detektory nebo magnetické kontakty. Tyto detektory jsou často napojena na ústřednu PZTS, která následně zajišťuje signalizaci narušení a případné přivolání zásahové jednotky. [15]

EPS systémy monitorují prostředí z hlediska výskytu kouře, teploty nebo plamene a slouží k včasnému varování v případě vzniku požáru, čímž významně přispívají k ochraně života a zdraví osob a ke snížení materiálních škod.[15]

Kamerové systémy umožňují sledování potřebných ploch nebo méně frekventovaných míst a zaznamenávat tak události v reálném čase. Zvyšují nejen prevenci, ale i následnou vymahatelnost práva, protože poskytují důkazy o průběhu incidentu. V některých případech jsou kamery vybaveny i analytickými funkcemi, jako je detekce pohybu, počítání osob nebo rozpoznávání obličejů. [15]

Přístupové systémy zajišťují kontrolu a evidenci vstupu osob do objektů a prostor, přičemž mohou být kombinovány s identifikací pomocí karet, biometrie nebo PIN kódů. V

případě neoprávněného přístupu lze automaticky vyvolat poplach nebo zablokovat přístupové cesty. [15]

Mechanické zábranné systémy zahrnují fyzické bariéry typicky zámky, mříže, oplocení, zdi, bezpečnostní dveře nebo trezory. MZS tak tvoří důležitou součást celkové ochrany objektu, jelikož tvoří první překážku a zpomalují nebo znemožňují průnik pachatele do chráněného prostoru. Vzhledem k posunu v technologiích je dnes možné propojit MZS i s elektronickými systémy, které ještě více zvyšují šance odhalení neoprávněného vstupu nebo poškození. Tyto systémy mohou být velmi nápomocné u rozlehlých objektů nebo objektů, kde jsou některé části MZS hůře dostupné a zjištění neoprávněného vstupu nebo poškození by tam mohlo být velmi složité. [15]

Hlavním důvodem pro zavedení technických systémů ochrany je snížení rizika škod a zvýšení bezpečnosti. Napomáhají chránit osoby a majetek, odrazují potenciální pachatele a umožňují rychlou reakci při incidentu. Díky neustálému technologickému vývoji dochází ke zvyšování spolehlivosti a přesnosti těchto systémů. [15]

Moderní technické systémy ochrany se často integrují do komplexních inteligentních systémů řízení budov (tzv. Smart Building nebo Building Management System – BMS). Díky propojení se zajišťuje efektivní řízení nejen bezpečnosti, ale i energetiky, osvětlení, ventilace a dalších procesů. Tato integrace přináší zvýšený komfort pro uživatele, snižuje provozní náklady a umožňuje centralizovaný dohled. [15]

2.1 Mechanické zábranné systémy

MZS tvoří jednu z nejzákladnějších a nejdůležitějších součástí fyzické ochrany objektů. Jejich primárním účelem je fyzicky zabránit nebo výrazně ztížit neoprávněnému vstupu, narušení perimetru, vniknutí do chráněných prostor nebo odcizení majetku. Tyto systémy vytvářejí první linii obrany a mají za úkol zpomalit nebo odradit pachatele od pokusu o průnik, případně zcela znemožnit nelegální vstup, než dojde k aktivaci elektronických zabezpečovacích systémů a zásahu ostrahy nebo Policie ČR. [17] [20]

Mechanické zábranné systémy mohou být aktivní (uzamykací systémy) nebo pasivní (stěny, mříže). V rámci bezpečnostní praxe se dělí do několika hlavních kategorií. [17][19]

Perimetrické zábrany - tyto prostředky slouží k ochraně vnější hranice chráněného objektu nebo areálu. [19][20] Patří sem:

- Ploty, zdi a oplocení – ty tvoří základní bariéru proti neoprávněnému vstupu, které mohou být doplněny navíc ostnatým nebo žiletkovým drátem.
- Brány a závory – umožňují řízený a kontrolovatelný vstup a výstup osob nebo vozidel, často v kombinaci s kontrolním systémem.
- Překážky proti vniknutí vozidel – betonové zátarasy, výsuvné sloupky.[20]

Stavební prvky a konstrukce - zde patří prvky zajišťující zvýšenou odolnost objektu proti násilnému vniknutí, jako jsou.

- Bezpečnostní dveře a okna – vyrobené z pevnějších materiálů, vícebodové zamykání, odolné proti vypáčení nebo rozbití.
- Mříže a roletové systémy – aplikované především na okna, vstupní otvory, výlohy. Mříže mohou být pevné nebo sklopné, pohyblivé.
- Bezpečnostní zasklení – vrstvené bezpečnostní sklo odolné proti proražení, často doplněné fóliemi zabraňujícími tříštění. [20]

Uzamykací systémy a kování - tyto systémy chrání vstupy do objektu a jeho jednotlivých částí.

- Mechanické zámky a vložky – certifikované podle úrovně bezpečnosti. [19]
- Elektronicko-mechanické zámky – kombinují mechanické jištění s elektronickým ovládáním (PIN klávesnice, čipové karty). [21]
- Bezpečnostní kování – chrání samotný zámek proti odvrtání, vytržení nebo rozlomení. [19][21]

2.2 Elektronické systémy

PZTS na objektu tvoří klíčovou součást technické ochrany majetku a osob. Jsou navrhovány tak, aby detekovaly neoprávněné vniknutí, pokus o narušení nebo jinou nestandardní událost, a následně umožnily adekvátní reakci jako je spuštění poplachu, přivolání zásahu nebo aktivaci dalších prvků zabezpečení. V kombinaci s mechanickými zábranami tvoří vícevrstvý systém fyzické ochrany.[22]

Poplachový zabezpečovací a tísňový systém slouží k detekci narušení prostoru, rozbití skla, otevření dveří/oken, narušení perimetru. [22]

- **Prvky systému PZTS:**

- Ústředna – řídicí jednotka systému.
- Detektory – pohybové (PIR, mikrovlnné), magnetické kontakty, otřesové, infračervené závory, detektory tříštění skla.
- Ovládací klávesnice – pro aktivaci/deaktivaci systému.
- Sirény – vnitřní a venkovní, pro akustickou signalizaci.
- Záložní napájení – zajišťuje funkčnost i při výpadku proudu. [22]

Elektronický systém kontroly vstupu – k řízení a záznam přístupových oprávnění osob. [23]

- **Prvky ESKV:**

- Čtečky (karet, čipů, biometrie)
- Elektromagnetické zámky
- Řídicí jednotky a software pro správu přístupových práv [23]

Kamerový systém – slouží k dohledu a záznamu událostí v reálném čase, dále pak jako prevence a důkazní materiál.

Perimetrická ochrana – nachází se na hranici objektu (ploty, brány, přírodní bariéry tvořící hranici katastrálního pozemku). [19]

- **Technologie perimetrické ochrany:**

- Mikrovlnné bariéry
- Infračervené závory
- Vibrace na plotech
- Zemní detekční systémy [19]

Elektrická požární signalizace – slouží k včasné detekci kouře, tepla nebo plamene, dále pak pro evakuaci a včasný zásah. [22]

- **Prvky EPS:**

- Hlásiče – kouřové, teplotní, kombinované
- Signalizační zařízení – sirény, majáky

- Ústředna EPS
- Napojení na HZS ČR [22]

2.3 Fyzická ostraha na objektu

Fyzická ostraha na objektu představuje jednu z nejdůležitějších složek komplexního systému zabezpečení. Na rozdíl od technických a elektronických systémů, které detekují nebo zaznamenávají hrozby, fyzická ostraha aktivně působí preventivně i represivně, a je schopna okamžitě zasáhnout v případě jakéhokoliv incidentu.

Fyzická ostraha je soubor opatření prováděných fyzickými osobami (strážní, další pracovníci bezpečnostní agentury), jejichž cílem je zamezit nebo minimalizovat hrozby, jako je neoprávněné vniknutí, vandalismus, krádeže, násilné činy nebo jiné bezpečnostní hrozby. Ostraha zajišťuje kontrolu vstupu, obchůzky, monitoring osob a vozidel, případně zásah při nestandardní situaci. [24] [25] [26]

Základními činnostmi fyzické ostrahy jsou:

1. Kontrola vstupu a výstupu

- Identifikace osob a ověření oprávnění ke vstupu
- Kontrola návštěv, výdej a evidence návštěvnických karet
- Kontrola vozidel a zavazadel (pomocí zrcadel, detektorů kovů) [24] [26]

2. Obchůzková činnost

- Pravidelná fyzická kontrola celého objektu nebo jeho vymezené části
- Používání obchůzkových systémů pro evidenci provedení kontroly
- Odhalování případných poruch, podezřelých osob, otevřených dveří nebo požárů [24] [26]

3. Monitoring bezpečnostních systémů

- Práce s kamerovým systémem, sledování záznamů a živého přenosu
- Vyhodnocení poplachových signálů z PZTS nebo EPS
- Reakce na vzniklé incidenty [24] [26]

4. Zásahová činnost

- Zadržení pachatele při činu

- Zajištění místa činu do příjezdu policie
- Evakuace osob nebo poskytnutí první pomoci [24] [26]

5. Evidence událostí a vedení záznamů

- Vedení provozního deníku
- Záznamy o kontrolách, incidentech a podezřenech
- Včasné hlášení mimořádných situací správci objektu nebo Policii ČR [24] [26]

2.4 Závěr kapitoly

Druhá kapitola se zabývá systémy technické ochrany. Definiuje základní pojmy a rozdělení na mechanické zábranné systémy, elektronické systémy a fyzickou ostrahu na objektu.

3 VYBRANÉ ANALÝZY RIZIK

Analýza rizik se využívá k identifikaci, hodnocení a řízení rizik. Cílem analýzy je pak identifikace hrozeb, stanovení pravděpodobností výskytu a závažnosti dopadu hrozeb. Dále pak návrh vhodného opatření, minimalizaci negativních důsledků. Výstupem je pak seznam identifikovaných rizik, hodnocení a prioritizace rizik včetně návrhu opatření na snížení rizik.

Pro analýzy rizik je možnost vybrat z kvalitativních a kvantitativních metod, případně hybridní metodu, která je kombinací kvalitativní a kvantitativní metody. Kvalitativní metody se především zaměřují na slovní hodnocení rizik a často využívají jednoduché nástroje, jako je matice rizik nebo SWOT analýza. Jsou tedy vhodné tam, kde nejsou k dispozici přesná data nebo kde se jedná o předběžné zhodnocení stavu zabezpečení. Kvantitativní metody naopak pracují s konkrétními číselnými hodnotami a výpočty, díky čemuž umožňují přesnější odhad dopadů a pravděpodobností. Příkladem může být metoda FMEA nebo simulace Monte Carlo.

3.1 Hybridní metoda analýzy rizik

Hybridní přístup kombinuje výhody obou metod, kdy kvalitativní hodnocení je doplněno o numerické výpočty, což zvyšuje přesnost a přehlednost celkové analýzy rizik. Výběr metody by měl vždy odpovídat konkrétním podmínkám analyzovaného projektu nebo systému.[27]

3.2 Kvalitativní metody analýzy rizik

Kvalitativní analýza rizik při hodnocení používá slovní vyjádření různého stupně pravděpodobnosti výskytu rizika a závažnosti jeho důsledků. Jedná se o popisný přístup, který nepracuje s přesnými číselnými hodnotami, ale využívá kategorie jako například nízká, střední nebo vysoká pravděpodobnost, a obdobně hodnotí i dopady rizik. Tento způsob hodnocení je snadno pochopitelný a rychle aplikovatelný, což jej činí velmi užitečným zejména tam, kde není k dispozici dostatek kvantitativních údajů nebo dat. [27] [28]

Použití kvalitativní analýzy je vhodné především v jednodušších provozech, malých firmách, nebo při posuzování méně komplexních systémů. Také ji lze využít jako úvodní fázi při plánování bezpečnostních opatření, kde může sloužit jako základ pro podrobnější hodnocení. Výhodou je, že umožňuje zapojení pracovníků, kteří nemusí mít odborné znalosti v oblasti statistiky, ale znají provozní rizika z praxe. [27] [28]

Typickým nástrojem kvalitativní analýzy je matice rizik, která pomáhá vizuálně znázornit kombinaci pravděpodobnosti a dopadu jednotlivých rizik. To umožňuje jejich snadné seřazení podle závažnosti a stanovení priorit pro jejich ošetření. Dále se v kvalitativních metodách setkáme s what if, tedy co když, kontrolní checklist nebo SWOT analýzou. [27] [28]

3.2.1 Metoda matice rizik

Matice rizik je jedním z nejčastěji používaných nástrojů v rámci kvalitativní analýzy rizik. Jde o grafické znázornění rizik, které jsou rozděleny do jednotlivých skupin podle priorit. Tyto priority pak slouží jako vodítko pro další práci s riziky, například při plánování opatření nebo při rozhodování o alokaci zdrojů. Matice rizik umožňuje rychlé, přehledné a srozumitelné vyhodnocení jednotlivých hrozeb. To je výhodné jak v technických oborech, tak při řízení projektů nebo bezpečnostních analýzách.

Základní vlastností matice rizik je, že zobrazuje dvě osy hodnocení. [29]

- **pravděpodobnost výskytu rizika** – například od velmi nepravděpodobné po velmi pravděpodobné
- **dopad rizika** – pokud k němu dojde, například od zanedbatelné po katastrofální [29]

Průsečík těchto dvou parametrů určuje umístění konkrétního rizika v matici a tím i jeho prioritu.

Výchozí nastavení úrovně rizik:

- **Nízké riziko** – Má malý dopad a nízkou pravděpodobnost. Jde o zanedbatelné riziko, které nevyžaduje bezprostřední zásah. Obvykle se pouze monitoruje, ale není nutné aktivně podnikat žádné kroky. [29]
- **Střední riziko** – Jedná se o rizika, která mají buď střední dopad nebo střední pravděpodobnost výskytu. Tato rizika je vhodné řešit po eliminaci rizik s vyšší prioritou. Jsou často předmětem pravidelného přezkoumání. [29]
- **Vysoké riziko** – Riziko s vážnými důsledky nebo vysokou pravděpodobností výskytu. Vyžaduje aktivní zásah a plán konkrétních opatření. Je třeba ho řešit, jakmile je to možné. [29]

- **Katastrofální riziko** – Představuje extrémní ohrožení s velmi závažnými dopady a vysokou pravděpodobností výskytu. Je nutné okamžité řešení. Může ohrozit celý projekt, zdraví osob nebo samotnou existenci organizace. [29]

Matice rizik tedy slouží nejen jako nástroj hodnocení, ale i jako komunikační prostředek, jelikož pomáhá vizualizovat, kterým rizikům se je třeba věnovat prioritně a která mohou zůstat pod dohledem bez nutnosti akutního zásahu. Metoda matice rizik se využívá napříč obory. [29]

3.2.2 Kontrolní checklist

Analýza pomocí kontrolního seznamu (CLA – Check List Analysis) je časově méně náročná a velmi jednoduchá, ale přitom účinná metoda, která se využívá pro ověřování správnosti, úplnosti nebo souladu určitého postupu, stavu zařízení či organizační činnosti. Základem CLA je předem připravený seznam položek, otázek, činností nebo kritérií, podle kterých pracovník kontroluje sledovaný proces nebo zařízení. Jedná se o metodu, která je intuitivní, snadno srozumitelná a vhodná pro široké spektrum použití. [30] [31]

Kontrolní seznam bývá zpravidla sestaven na základě dobré praxe, zkušeností z provozu, platných norem či standardů. Pomocí něj lze systematicky zkontrolovat, zda byly splněny všechny požadované kroky, zda je zařízení v požadovaném stavu, nebo zda jsou splněny veškeré bezpečnostní požadavky. Výsledek kontroly může být zaznamenán ve formě ano/ne, nebo lze použít i stupnici hodnocení – například splněno, částečně splněno, nesplněno, případně nutná opakovaná kontrola. [30] [31]

Typickým příkladem využití CLA je kontrola stavu zařízení před uvedením do provozu, kontrola údržby, nebo předletová příprava v letectví, kdy piloti ověřují všechny klíčové kroky pomocí seznamu. Tato metoda tím pomáhá minimalizovat lidské chyby, zlepšit dohledatelnost a posílit zodpovědný přístup pracovníků. [30] [31]

3.2.3 Metoda what if – co když

Co když analýza (*What-if Analysis*) je jednoduchá, avšak velmi účinná analytická technika využívaná při rozhodování, řízení rizik a zvyšování bezpečnosti procesů. Jejím základem je hledání možných scénářů a jejich důsledků prostřednictvím otázek typu Co se stane, když...? V praxi jde o formu strukturovaného brainstormingu, během kterého se skupina odborníků snaží identifikovat rizika, navrhnout preventivní opatření a předejít nežádoucím situacím. [31] [32] [33]

Na rozdíl od přísně formalizovaných metod, jako je HAZOP nebo FMEA, je metoda co-když analýza více flexibilní a snadněji přizpůsobitelná konkrétním potřebám. Hodí se jak pro technické procesy, tak i pro organizační rozhodování. [31] [32] [33]

Postup analýzy:

1. Vymezení analyzované oblasti
2. Stanovení cílových témat (např. bezpečnost, finance, životní prostředí)
3. Tvorba otázek typu, co když...
4. Identifikace možných dopadů – odpověď co se může stát
5. Návrh preventivních a reaktivních opatření

Využívá se napříč průmyslovými i neindustriálními obory při zavádění nových technologií, reorganizaci, krizovém řízení nebo při přípravě havarijních plánů. Výstupem je přehled potenciálních problémů a doporučená opatření, jak jim předejít nebo je efektivně řešit. [31] [32] [33]

3.2.4 SWOT analýza

SWOT analýza je jedním z nejčastěji používaných nástrojů pro strategické plánování a rozhodování. Název SWOT je zkratkou ze čtyř anglických slov a to: Strengths (silné stránky), Weaknesses (slabé stránky), Opportunities (příležitosti) a Threats (hrozby). Tato metoda umožňuje komplexní pohled na situaci organizace, projektu, produktu nebo osoby tím, že propojuje vnitřní faktory (silné a slabé stránky) s faktory vnějšími (příležitosti a hrozby). Vnitřní faktory. [34]

- **Silné stránky (Strengths)** představují oblasti, ve kterých má subjekt konkurenční výhodu. Může jít např. o know-how, technologie, lidské zdroje, finanční stabilitu, dobrou reputaci nebo kvalitní zákaznický servis. [34]
- **Slabé stránky (Weaknesses)** jsou oblasti, které organizaci nebo projektu snižují výkonnost nebo konkurenceschopnost. Mohou zahrnovat nedostatek odborníků, špatné procesy, slabou infrastrukturu nebo nízkou inovativnost. [34]

Vnější faktory.

- **Příležitosti (Opportunities)** představují pozitivní trendy nebo okolnosti ve vnějším prostředí, které může subjekt využít pro svůj růst. Může jít o nové trhy,

technologický pokrok, legislativní změny ve prospěch činnosti nebo změny v chování zákazníků. [34]

- **Hrozby (Threats)** označují vnější negativní faktory, které mohou ohrozit úspěšnost, stabilitu nebo přežití organizace. Patří sem např. nová konkurence, ekonomická krize, změna zákonů, nebo negativní změny v tržním prostředí. [34]

SWOT analýza je důležitým nástrojem pro stanovení realistické strategie. Pomáhá vedení identifikovat, na co se zaměřit a co je třeba zlepšit. Na základě analýzy lze:

- využít silné stránky k získání výhody
- omezit dopad slabých stránek
- plánovat využití příležitostí
- připravit se na potenciální hrozby

Výhodou SWOT analýzy je její jednoduchost a přehlednost včetně univerzálního použití v různých oborech. Dále pak zapojení více úrovní organizace do analýzy, která tvoří základ pro tvorbu následné strategie, rozhodování a plánování. [34]

SWOT analýza by měla být pravidelně aktualizována, protože faktory ovlivňující úspěšnost daného subjektu se v čase mění. V praxi je často SWOT analýza doplňována o další metody, jako jsou PEST analýza nebo Porterova analýza konkurence, aby poskytla maximálně komplexní pohled na celou situaci. [34]

3.3 Kvantitativní metody analýzy rizik

Kvantitativní analýza rizik je metoda, která se zaměřuje na numerické vyjádření rizik, tedy na měření pravděpodobnosti výskytu určité události a jejího dopadu pomocí čísel. Oproti kvalitativní analýze, která pracuje se slovním hodnocením a relativními pojmy, kvantitativní metoda usiluje o přesnější, objektivnější a opakovatelné výsledky. Je vhodná především pro komplexní, technologicky nebo finančně náročné projekty, kde je nezbytné přesně odhadnout potenciální dopady rizik na projekt, organizaci nebo investici. [27] [28]

Kvantitativní analýza rizik spočívá v matematickém modelování rizik. Základem je identifikace rizik, následované odhadem pravděpodobnosti jejich výskytu a výpočtem finančních nebo jiných dopadů, které mohou způsobit. Rizika jsou poté vyjádřena jako

číselná hodnota, například očekávaná finanční ztráta, pravděpodobnost zpoždění nebo poruchy systému. [27] [28]

Výsledkem kvantitativní analýzy je často tzv. hodnota rizika (Risk Value), která se vypočítá jako součin pravděpodobnosti a dopadu. [27] [28]

- $\text{Riziko} = \text{Pravděpodobnost} \times \text{Dopad}$ [27] [28]

Používané techniky v rámci kvantitativní analýzy se používá řada specifických nástrojů a metod.

- Metoda Monte Carlo – metoda využívající náhodné generování scénářů pro modelování nejistoty a výpočtu pravděpodobnostních rozdělení výsledků.
- Strom rozhodování – grafické znázornění možností rozhodnutí a následných důsledků s přiřazenými pravděpodobnostmi a náklady/zisky.
- Analýza očekávané peněžní hodnoty (EMV) – metoda využívaná především v projektovém řízení k hodnocení investičních a provozních rizik.
- Analýza citlivosti a scénářů – slouží k posouzení, jak změny v jednotlivých proměnných ovlivňují výsledné riziko. [27] [28]

Výhody a nevýhody kvantitativní metody analýzy rizik.

- Výhody kvantitativní metody spočívají v její objektivnosti, přesnosti a schopnosti poskytovat tvrdá data pro rozhodování. Je velmi vhodná pro ekonomické a inženýrské projekty, plánování rozpočtu nebo bezpečnostní hodnocení složitých systémů.
- Nevýhody spočívají zejména v náročnosti na vstupní data – potřebujete mít k dispozici přesné statistiky, historické údaje a kvalitní odhady. Bez těchto dat může být výsledek zavádějící. Dále je potřeba odborné znalosti a sofistikovaný software, což může zvyšovat náklady a časovou náročnost analýzy. [27] [28]

3.3.1 Analýza selhání a jejich dopadů – FMEA

Analýza selhání a jejich dopadů, známá také pod zkratkou FMEA (Failure Mode and Effects Analysis), je systematický a strukturovaný přístup k identifikaci možných způsobů selhání jednotlivých částí zařízení, systému nebo procesu a k hodnocení důsledků těchto selhání na celkový provoz či funkčnost systému. Cílem této metody je včasné odhalení potenciálních

problémů, které by mohly způsobit významné škody, a následné navržení opatření, která minimalizují riziko jejich výskytu či dopadů. [31][35]

FMEA je jednou z nejrozšířenějších metod pro hodnocení spolehlivosti a bezpečnosti v různých odvětvích průmyslu, zejména tam, kde jsou kladeny vysoké nároky na bezpečnost a funkčnost, jako jsou automobilový průmysl, letectví, strojírenství, zdravotnictví nebo energetika. Tato metoda se zaměřuje na detailní rozbor jednotlivých prvků systému a posuzuje možné způsoby jejich selhání a dopady těchto selhání na celý systém či proces. [31][35]

Proces FMEA zahrnuje několik kroků, mezi které patří identifikace jednotlivých komponent, určení možných způsobů jejich selhání, posouzení pravděpodobnosti výskytu každého typu selhání, hodnocení závažnosti dopadu tohoto selhání a schopnosti detekce či odhalení selhání předtím, než dojde k vážným následkům. Výsledkem je tzv. rizikové číslo (Risk Priority Number, RPN), které pomáhá určovat priority řešení jednotlivých rizik. Vyšší hodnoty RPN signalizují závažnější rizika, kterým je třeba věnovat větší pozornost. [31][35]

FMEA je především metodou kvantitativního přístupu k řešení rizik, kde jsou kladeny důrazy na přesné a měřitelné parametry. Tato metoda se často využívá v případech, kdy jsou rizika vážná a jejich možné dopady mohou mít kritický vliv na bezpečnost, kvalitu nebo provozuschopnost. Metoda FMEA je nezbytnou součástí řízení kvality, bezpečnosti a spolehlivosti systémů, a to zejména v prostředích, kde selhání může znamenat finanční ztráty, ohrožení zdraví či životů. [31][35]

Metoda FMEA umožňuje předcházet nehodám, poruchám a nežádoucím událostem tím, že poskytuje systematický nástroj pro identifikaci a eliminaci rizik již v raných fázích návrhu či provozu zařízení. Díky tomu je možné zlepšit spolehlivost a bezpečnost, optimalizovat údržbu a snížit náklady spojené s opravami a případnými haváriemi.

Metoda FMEA tedy představuje nezbytný nástroj pro každou organizaci, která se chce efektivně vypořádat s možnými riziky a zajistit bezpečný a bezproblémový provoz svých systémů. Její systematickост a kvantitativní přístup umožňují přesné a cílené řízení rizik, což je v současné době nezbytné v rámci moderních průmyslových procesů. [31][35]

3.3.2 Analýza stromu poruch (FTA)

Analýza stromu poruch, známá také pod anglickou zkratkou FTA (Fault Tree Analysis), je jednou z klíčových metod používaných v oblasti bezpečnosti, spolehlivosti a řízení rizik.

Tento postup se zaměřuje na systematický zpětný rozbor událostí a příčin vedoucích k vybrané vrcholové (nežádoucí) události, která představuje hlavní problém či selhání v daném systému. Cílem je podrobné pochopení toho, jak různé faktory a poruchy mohou vzájemně působit a vyústit ve vážné selhání, které může mít závažné následky. [36] [37]

Metoda FTA je především graficko-analytickou či graficko-statistickou technikou, jejíž základem je stromová struktura, která vizuálně zobrazuje vztahy mezi jednotlivými příčinami a následky. Tento strom poruch je tvořen rozvětveným grafem, kde vrchol reprezentuje nežádoucí událost. Pod touto vrcholovou událostí jsou znázorněny jednotlivé příčiny, které k ní mohou vést, a to buď samostatně, nebo ve vzájemné kombinaci. Graf využívá dohodnutou symboliku, která zahrnuje různé logické brány, jež popisují vztahy mezi příčinami a umožňují tak přesně modelovat různé scénáře vzniku problému. [36] [37]

Hlavním cílem analýzy stromu poruch je posoudit pravděpodobnost výskytu vrcholové události, tedy zjistit, jak pravděpodobné je, že dané nežádoucí selhání nastane v důsledku určitých kombinací poruch, chyb nebo jiných nežádoucích událostí. Pro tento účel se využívají analytické a statistické metody, které umožňují kvantifikovat riziko a určit kritické oblasti systému, na které je třeba se zaměřit při zavádění opatření ke snížení rizika. [36] [37]

Proces dedukce v rámci FTA začíná právě od vrcholové události a pokračuje směrem dolů, kde se identifikují všechny možné příčiny jejího vzniku. Tento deduktivní přístup znamená, že se postupuje od následku zpět k příčině, což umožňuje systematické prozkoumání všech možných faktorů, které by mohly přispět ke vzniku problému. Dedukce pomáhá odhalit různé kombinace hardwarových a softwarových poruch, ale také lidských chyb, které mohou společně způsobit selhání. [36] [37]

Analýza stromu poruch tak poskytuje důležitý vhled do komplexních vzájemných vztahů mezi jednotlivými prvky systému a pomáhá identifikovat slabá místa a kritické faktory. Díky tomu je možné lépe plánovat preventivní opatření, údržbu a bezpečnostní zásahy, které minimalizují riziko nežádoucích událostí a zvýší celkovou spolehlivost systému. [36] [37]

Tato metoda se široce využívá v mnoha průmyslových odvětvích, včetně letectví, energetiky, chemického průmyslu, výroby, dopravy či zdravotnictví. V každém z těchto oborů pomáhá FTA systematicky snižovat rizika a zajišťovat bezpečnost provozu. [36] [37]

3.3.3 Analýza stromu událostí (ETA)

Analýza stromu událostí (Event Tree Analysis, ETA) je systematická a přehledná metoda používaná při hodnocení rizik, která sleduje možný vývoj situace od iniciační události až po různé možné výsledky, jež mohou nastat v důsledku řady následných událostí. Základní princip metody spočívá v rozvětřování průběhu procesu podle dvou základních možností u každé události na příznivé (pozitivní) nebo nepříznivé (negativní). Tímto způsobem umožňuje ETA identifikovat možné scénáře, které mohou vést k různým důsledkům, včetně těch nejzávažnějších, a zároveň vyhodnotit pravděpodobnosti jednotlivých scénářů. [31] [38]

Metoda ETA je graficko-statistická technika, která kombinuje vizuální znázornění událostí v podobě stromu s kvantitativním vyhodnocením pravděpodobností jednotlivých cest stromem. Tento systémový strom událostí začíná iniciační událostí, což je obvykle nějaký aktivující faktor, například technická závada, lidská chyba, selhání systému či externí vliv. Od této iniciační události se postupně odvíjejí další události, které mohou nastat buď v důsledku předchozí události, nebo mohou představovat ochranná opatření či zásahy do systému. [31] [38]

Názorné zobrazení stromu událostí je tvořeno rozvětveným grafem, který připomíná větve stromu. Každá větev reprezentuje jednu z možných cest, kterou může systém při daném vývoji událostí projít. Tento strom je sestaven pomocí dohodnuté symboliky, která jasně označuje jednotlivé typy událostí, stavů a vztahů mezi nimi. Díky této grafické podobě lze snadno sledovat celý řetězec událostí od počátečního momentu až po konečné důsledky. Hlavní výhodou ETA je její schopnost detailně analyzovat všechny možné průběhy situace, přičemž umožňuje kombinovat jak příznivé, tak i nepříznivé výsledky jednotlivých událostí. To pomáhá odborníkům pochopit komplexnost daného systému a identifikovat klíčové body, kde může dojít k selhání nebo kde je třeba zavést opatření pro zvýšení bezpečnosti a spolehlivosti. [31] [38]

ETA je využívána především v průmyslových odvětvích, kde je nezbytné předcházet haváriím a minimalizovat dopady poruch. Díky své přehlednosti a možnosti kvantifikace rizik patří analýza stromu událostí k velmi efektivním nástrojům pro podporu rozhodování v oblasti bezpečnosti a řízení rizik. Pomáhá organizacím lépe pochopit dynamiku možných havarijních scénářů a přijmout opatření, která minimalizují pravděpodobnost nežádoucích událostí a jejich následků. [31] [38]

3.3.4 Analýza lidské spolehlivosti (HRA)

Analýza lidské spolehlivosti (Human Reliability Analysis, HRA) představuje systematický postup, jehož cílem je posoudit vliv lidského činitele na vznik nežádoucích událostí, jako jsou živelná neštěstí, nehody, havárie nebo i úmyslné útoky. HRA se zaměřuje především na identifikaci a hodnocení rizik, která vyplývají z lidských chyb, a to jak v rámci běžného provozu, tak i v krizových situacích. Tato metoda je zásadní pro pochopení toho, jak lidský faktor ovlivňuje bezpečnostní systém a jak jej lze optimalizovat, aby došlo ke snížení počtu a závažnosti incidentů. [31] [39]

HRA zkoumá nejen samotné lidské chyby, ale také související faktory, které tyto chyby ovlivňují. Význam HRA je podpořen také tím, že metoda úzce koresponduje s platnými pracovněprávními předpisy, zejména s těmi, které regulují bezpečnost práce. Provozovatelé zařízení a manažeři bezpečnosti jsou díky HRA schopni lépe porozumět tomu, jakým způsobem lidský faktor přispívá k rizikům, a na základě toho přizpůsobit školení, pracovní postupy, či systém řízení bezpečnosti tak, aby minimalizovali chyby a zvyšovali spolehlivost personálu. [31] [39]

Aby byla analýza lidské spolehlivosti efektivní, je nutné, aby byla integrována do širšího rámce řízení rizik. HRA by proto neměla být prováděna izolovaně, ale paralelně a nezávisle vedle dalších metod rizikové analýzy jako jsou HAZOP, FMEA nebo Event Tree Analysis. Tento integrovaný přístup umožňuje komplexně vyhodnotit bezpečnost provozu i v extrémních havarijních scénářích, kdy může být lidský faktor klíčovým prvkem vedoucím k selhání nebo naopak k jeho odvrácení. [31] [39]

HRA tedy poskytuje nejen analýzu chyb, ale i podklady pro navržení opatření, která vedou ke zvýšení spolehlivosti lidského faktoru, například formou školení, redesignu pracovních procesů, nebo zavedením podpůrných systémů. Výsledkem je snížení rizika nehod a zvýšení bezpečnosti celého provozu, což je nezbytné zejména v kritických odvětvích jako jsou energetika, doprava, zdravotnictví či průmyslová výroba. [31] [39]

Celkově lze říci, že analýza lidské spolehlivosti představuje klíčový nástroj moderního řízení bezpečnosti, který pomáhá minimalizovat dopady lidských chyb a zvyšovat efektivitu a bezpečnost složitých technických i organizačních systémů. [31] [39]

3.3.5 Analýza ohrožení a provozuschopnosti (HAZOP)

HAZOP, anglicky Hazard and Operability Study, neboli analýza ohrožení a provozuschopnosti, patří mezi jednu z nejvíce rozšířených a zároveň nejefektivnějších metod používaných při identifikaci a hodnocení rizik v technických a průmyslových procesech. Tato metoda je velmi cenná zejména v situacích, kdy je potřeba systematicky zkoumat možné nebezpečné stavy a problémy spojené s provozem složitých zařízení či procesů. HAZOP je strukturální, týmová a expertní metoda, jejímž hlavním cílem je odhalit potenciální rizika, která by mohla ohrozit bezpečnost provozu, zdraví pracovníků, životní prostředí nebo samotný technický systém. [40]

Princip HAZOP je založen na detailním rozboru zkoumaného systému, kdy se tým odborníků, složený z více disciplín, systematicky zaměřuje na jednotlivé části procesu nebo zařízení. Během této analýzy se využívá brainstorming a další metody, které pomáhají generovat možné scénáře selhání nebo odchylek od normálního stavu. Tyto scénáře jsou následně analyzovány z hlediska jejich příčin, možných důsledků a potenciálních rizik, která mohou nastat. Klíčovou roli v metodě hraje hledání tzv. kritických míst, tedy oblastí procesu nebo zařízení, kde je pravděpodobnost výskytu problému zvýšená a kde by případný problém mohl mít vážné následky. [40]

Proces HAZOP začíná pečlivým rozdělením zkoumaného zařízení nebo procesu na menší části, tzv. studijní uzly. Pro každý z těchto uzlů tým postupně klade specifické otázky, které vycházejí z předem definovaných vodítek, jako jsou například co když se zvýší tlak?, co když dojde k úniku média? nebo co když dojde k poruše ventilu?. Tyto otázky mají stimulovat tým k identifikaci možných odchylek od standardního provozu. Následně se diskutují možné příčiny těchto odchylek, jejich důsledky a rizika, která z nich mohou vzejít.

Výsledkem metody HAZOP je souhrnná zpráva nebo dokument, který obsahuje detailní popis všech zjištěných rizik, jejich příčin, možných důsledků a navržených opatření. Tento dokument slouží jako podklad pro bezpečnostní management, plánování údržby a další rozhodování v oblasti řízení rizik. [40]

Výhodou HAZOP je její systematickost, která minimalizuje riziko přehlédnutí kritických situací, a zároveň týmový přístup, který zajišťuje široký pohled na daný problém z různých odborných úhlů. Díky tomu je možné lépe porozumět složitým vztahům v procesu a připravit efektivní opatření k minimalizaci rizik. [40]

Na druhé straně, metoda může být časově i personálně náročná, protože vyžaduje zapojení odborníků z různých oblastí a podrobnou analýzu každého uzlu procesu. Přesto je HAZOP často považována za jednu z nejúčinnějších metod pro zajištění bezpečnosti a provozní spolehlivosti v náročných průmyslových provozech. [40]

V dnešní době je HAZOP standardní součástí procesu řízení bezpečnosti a kvality ve velkých firmách, jelikož principy HAZOP jsou často zakomponovány i do dalších metodik a softwarových nástrojů pro správu rizik. Význam metody roste zejména v souvislosti se zvyšující se složitostí technických systémů a požadavky na vyšší úroveň bezpečnosti a environmentální ochrany. [40]

3.4 Závěr kapitoly

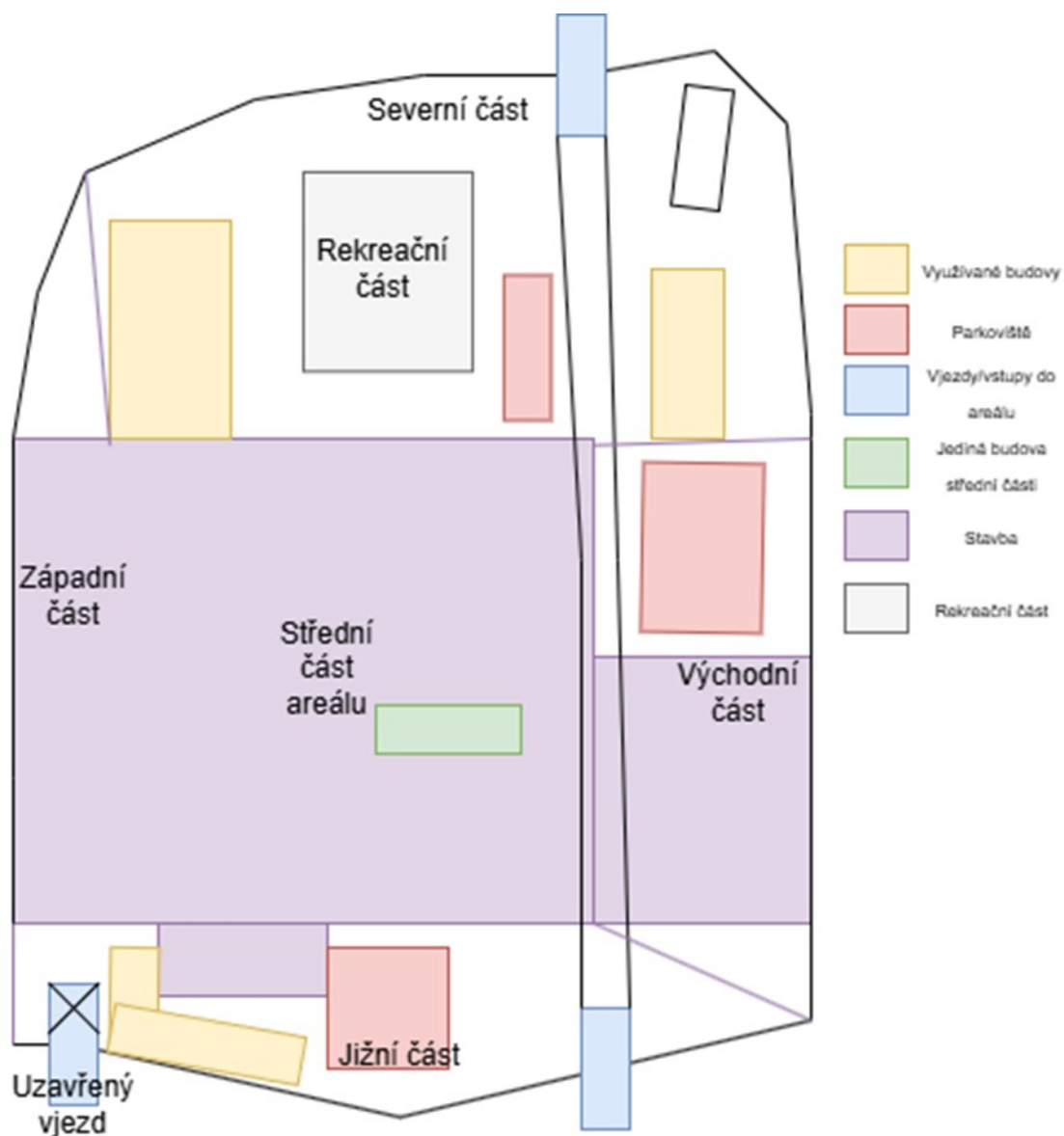
Třetí kapitola se zabývala vybranými analýzami. Celá tato kapitola je dále rozdělena na dvě části a to kvalitativní a kvantitativní část včetně několik příkladů daných metod pro každou část. Na závěr každé části byly ještě zhodnoceny výhody a nevýhody každé metody analýzy rizik.

II. PRAKTICKÁ ČÁST

4 CHARAKTERISTIKA PRŮMYSLOVÉHO AREÁLU

Tato kapitola se zabývá charakteristikou areálu, kterým se bude dále zabývat praktická část bakalářské práce. Cílem je poskytnout čtenáři základní přehled o jeho uspořádání, významu jednotlivých částí a jejich funkčním využití. Areál představuje komplexní prostředí, jehož správné pochopení je klíčové pro další analýzu a navrhovaná řešení. Názvy všech částí areálu i budov byly z důvodu anonymizace pozměněny, aby nebylo možné přesně identifikovat skutečný objekt a zároveň byla zachována důvěrnost citlivých informací spojených s daným místem.

Areál se nachází v oblasti bývalých továren, které v této chvíli uvolňují prostor modernějším kancelářským a bytovým prostorům. Areál o rozloze cca 22,5 hektaru je nyní postupně modernizován a přestavován. V blízkosti areálu se nachází vlakové nádraží, které spojuje tuto část s centrem města a cesta vlakem netrvá déle než 5 minut (za standardních podmínek). Přičemž je zde k dispozici i spojení městskou hromadnou dopravou, kdy je možné se dostat do samotného centra města během patnácti minut.



Obrázek 2 Plánek rozložení objektu

(zdroj: vlastní)

V této chvíli dochází k větším úpravám v jižní části areálu, kde dochází k rozšiřování hlavního vjezdu a infrastruktury pro pozdější větší vytíženost a zároveň dochází k úpravě pro stavební techniku, aby mohla volně projíždět. Z tohoto důvodu došlo k přemístění automatické brány, která již není ihned za vjezdem do areálu, ale je posunuta asi o 150 m dále do areálu. Zároveň se zde rozšiřuje první budova o další čtyři sektory, které následně budou sloužit jako kancelářské prostory pro další i stávající firmy.



Obrázek 3 Jižní komplex budov včetně provizorního parkoviště

(zdroj: vlastní)

V severní části se nachází hlavní železobetonová moderní kancelářská budova, která nahradila původní výrobní linku. Zde se nachází několik desítek firem včetně školky, je zde zázemí s občerstvením a nachází se zde hlavní velín fyzické ostrahy. Tato budova má celkově osm nadzemních pater a jedno podzemní patro, kde se nachází technické místnosti. Například ovládání stabilního hasicího zařízení, přívod plynu nebo elektrická rozvodna.



Obrázek 4 Opravená hlavní budova v severní části

(zdroj: [vlastní])

Budova dále disponuje dvěma patry vnitřního parkování, které je ovládáno automatickou závorou a vjezd je tak povolen pouze držitelům parkovacího oprávnění – otevření závor funguje automaticky pomocí čtení registrační značky.

Dále na sever za touto budovou se nachází nejnovější budova v celém areálu. Zde se nachází distribuční středisko automobilky s vlastním parkováním. Nedaleko této budovy se nachází severní vjezd, který je totožný, jako je v jižní části, tedy automatické závory se čtením registrační značky. V případě poruchy či nepříznivého počasí je na všech závorách umístěn interkom, který slouží pro komunikaci s recepcí. Celá tato část je ukončena oplocením, které zároveň odděluje areál od obydlených prostor města.



Obrázek 5 Automatické závory v severní části

(zdroj: [vlastní])

V severozápadní části se nachází bývalá výrobní hala, která byla uvnitř zmodernizovaná a nachází se zde středisko pro konání festivalů, trhů a dalších akcí.

Ve východní části se nachází v této chvíli dvě parkoviště a travnaté plochy, kde se uskládá nepotřebný i potřebný materiál ze stavby. V blízké budoucnosti zde bude docházet k úpravám jednoho parkoviště a k úpravě travnatých ploch, aby zde mohli trávit volný čas zaměstnanci i návštěvníci areálu.

Západní část se postupně přestavuje a navazuje tak na jižní část. Nyní se zde nachází nové restaurační prostory a v budoucnu zde budou stát obytné prostory společně s komerčními prostory a množstvím parkovacích míst.



Obrázek 6 Uzavřená střední část z důvodů probíhajících staveb

(zdroj: [vlastní])

Celý areál je oplocený a vjezdy jsou dle režimového opatření v určitou dobu uzamčeny bránou. Dle ročního období se doba uzamčení mění.



Obrázek 7 Narušení MZS z důvodů stavby v západní části areálu

(zdroj: [vlastní])

Celé prostory areálu jsou pod neustálým kamerovým dohledem, který je vyveden na velín fyzické ostrahy, která se zde nachází dvacet čtyři hodin denně.

V této chvíli dochází k a bude docházet k velkým stavebním úpravám ve střední části celého areálu, kde budou postupně vznikat nové obytné a komerční zóny.

4.1 Severní část areálu

Severní část areálu je tvořena dvěma hlavními budovami, které budou pojmenovány jako E a T, přičemž budova E je distribuční středisko pro vozidla a ve druhé budově T se nachází komerční prostory se zhruba 400 zaměstnanci. V budově T se zároveň nachází hlavní středisko a velín pro fyzickou ostrahu, která se na objektu nachází.

Budova T disponuje osmi nadzemními podlažími a jedním podzemním patrem. V této budově, ve které se v této chvíli nachází několik firem a školka byla jednou z prvních modernizovaných v celém areálu. Tato budova dále disponuje dvěma patry vnitřního parkoviště pro zaměstnance. Ve spodní části se nachází malá restaurace, přičemž naproti je dětské hřiště. Budova E je v neustálém provozu, tedy v režimu 24/7 a po celou dobu se na

objektu nachází i fyzická ostraha. Každá budova má svou vlastní ústřednu EPS a nejsou nijak propojené v celém areálu. PZTS je v každé budově řešen zvlášť a nejsou propojeny mezi stanovišti ostrahy.

Kamerové systémy jsou propojeny a na obou stanovištích je možnost sledovat záznamy kamer z celého areálu.



Obrázek 8 Ovládací tablo ústředny EPS

(zdroj: [vlastní])

Naproti budově T se nachází menší parkoviště pro návštěvy a pracovníky, přičemž ve vzdálenosti asi 20 metrů od parkoviště se nachází venkovní posezení s možností se

odreagovat, přičemž toto místo je volně přístupné. Nedaleko od parkoviště se nachází i zastávka pro autobusy městské hromadné dopravy.

Zároveň se zde nachází vjezd pro osobní vozidla, který je zajištěn pomocí automatických závor, která jsou pod kamerovým dohledem a s možností komunikace přes interkom na recepci. Vjezd je umožněn vozidlům po nahrání registrační značky do systému nebo odebrání si parkovacího lístku přímo na vjezdu. V nočních hodinách je zde i brána, která se dle nastaveného režimu uzavírá.

4.2 Jižní část areálu

V jižní části se nachází soubor několika budov, dále jen D, které jsou propojeny hlavním vstupem. Od hlavní silnice je areál částečně oddělen komerčními budovami a následně po obvodu pozemku plotem.



Obrázek 9 Perimetr areálu ukončen budovami

(zdroj: [vlastní])

V komerčních budovách D, jelikož se nenachází fyzická ostraha v režimu dvacet čtyři hodin denně, je zde elektrická požární signalizace, dále jen EPS, napojena na hasičský

záchranný sbor a z venkovní části se nachází klíčový trezor požární ochrany, dále jen KTPO a obslužné pole požární ochrany.



Obrázek 10 KTPO umístěné v plášti objektu

(Zdroj: [vlastní])



Obrázek 11 OPPO včetně central a total stopu

(zdroj: [vlastní])

Vedle budovy se nachází vjezd do západní části areálu a zároveň na parkoviště pro zaměstnance, které je situované na nádvoří a je pod neustálým kamerovým dohledem. Tento vjezd je opět vybaven automatickou závorou s možností komunikace přes interkom na recepci v případě potřeby.



Obrázek 12 Aktuálně demontovaná automatická brána z důvodu probíhajících prací

(zdroj: [vlastní])

Na jižní části se ještě nachází druhý vjezd, který je i pro nákladní vozidla a autobusy městské hromadné dopravy, která do areálu zajiždí. I zde se nachází automatická závara s interkomem. Vjezd je umožněn na nahrání registrační značky do systému nebo odebrání si parkovacího lístku přímo na vjezdu. Všechny vjezdy jsou uzavíratelné bránou, která je uzavřena dle režimového opatření.



Obrázek 13 Rozšířený hlavní vjezd do areálu pro MHD a nákladní dopravu

(zdroj: [vlastní])

V důsledku stavebních prací a rozšíření vjezdové brány je druhá brána nyní odpojena a areál je tak z jedné části vždy volně průchozí i v nočních hodinách.

4.3 Východní část areálu

Ve východní části se nachází dvě velké parkoviště, přičemž jedno z nich patří k budově E. Druhé parkoviště je využíváno ostatními nájemníky dle potřeby. Obě tyto parkoviště jsou pod kamerovým dohledem.

Dříve zde byla i upravená místa, kde se scházela školka nebo se pořádaly firemní akce, jelikož se jedná o travnatou plochu. Po rekonstrukcích v jiných částech se tato část přestala udržovat a bohužel se do těchto míst pravidelně stahují osoby bez domova či sběrači kovu, kteří se pokouší vykopat kabely v zemi. Z tohoto důvodu byly do těchto míst umístěny dvě nové kamery, které tak zjednodušily práci bezpečnostním pracovníkům.

4.4 Západní část areálu

Západní část prochází v poslední době velkou rekonstrukcí a vzniká zde mnoho nových prostor pro komerční budovy, přičemž v nejsevernější části se nachází budova, kde se pravidelně konají různé akce, jako jsou trhy. Nově se zde nachází nové restaurační prostory a v budoucnu zde budou stát obytné prostory společně s komerčními prostory.



Obrázek 14 Ruiny v západní části před opravou

(zdroj: [vlastní])

4.5 Střední část areálu

Střední část v budoucích letech bude kompletně přeměněna na nové obytné a komerční budovy, přičemž v této chvíli jsou potřebná místa již obestavěna plotem z důvodu výkopových a jiných prací.



Obrázek 15 Poslední budova ve střední části areálu (před rekonstrukcí)

(zdroj: [vlastní])

Dále zde vzniká i nová infrastruktura a rozšíření již stávající. Do budoucna by zde mělo dojít i k posílení spojů městské hromadné dopravy právě kvůli výstavbě nových obytných částí.

4.6 Závěr kapitoly

Čtvrtá kapitola se zabývá popsáním charakteristiky objektu, která je rozdělena dle umístění podle severní, jižní, východní a západní části. Celá tato kapitola je zároveň doplněna o fotky z aktuálních míst.

5 SOUČASNÝ STAV BEZPEČNOSTNÍCH OPATŘENÍ NA OBJEKTU

Perimetr areálu je kompletně uzavřen a je tvořen kombinací plotu, komerčních budov a uměle vytvořených zábran. Uměle vytvořená bariéra se nachází na východní straně areálu, kde je prudký svah z betonu. Tato část je zároveň součástí blízkého nádraží, jelikož jde o zpevnění původního přírodního svahu. V severní i jižní části na konce svahu navazuje plot.



Obrázek 16 Špatný stav MZS v severozápadní části

(zdroj: [vlastní])



Obrázek 17 Betonový svah oddělující východní část a přilehlé nádraží

(zdroj: [vlastní])

Kolem celé západní strany se navíc vyskytuje řeka, která tak tvoří přírodní bariéru mezi tímto areálem a dalšími, které se nachází na druhé straně břehu. I přes řeku se po celé délce nachází plot, ale vzhledem k hustému porostu, který se okolo plotu nachází je velmi obtížné se do těchto míst kolem řeky dostat. Plot je zde navíc zakončen ostnatým drátem, aby se zvýšila ochrana před možným průnikem pachatele.



Obrázek 18 Řeka podél západní části areálu

(zdroj: [vlastní])

Po celém areálu jsou rozmístěny kamery, které mají základní funkce jako několika násobný zoom nebo noční vidění. Zároveň je poměrně velká část areálu dobře osvětlena, a tedy není příliš problém, zahlédnout potenciálního pachatele i pouze běžnou kamerou. Kamer je zde několik typů, a to dle umístění a rozsahu, v jakém kamera funguje. Nejlépe vybavené kamery se nachází na vyvýšených místech v areálu a je z nich možné kontrolovat větší část areálu.

V budově D se nachází na všech oknech magnetické kontakty z důvodu uzavření po pracovní době a sepnutí poplachového zabezpečovacího systému. V případě otevřeného okna dojde k vyhlášení poplachu na velínu fyzické ostrahy, která může celou věc řešit a kontrolovat náhledem kamer a vysláním bezpečnostního pracovníka, dále jen BP, na patrolu.

Budova E i D je vybavena elektrickou požární signalizací. Budova E ovšem není napojená na hasičský záchranný sbor a v případě vyhlášení poplachu musí dojít k fyzické kontrole v místě, kde k poplachu došlo. Z tohoto důvodu jsou k dispozici vždy dva bezpečnostní pracovníci. Budova D, jelikož nemá stálou fyzickou ostrahu je napojena

napřímo na hasičský záchranný sbor a v případě vyhlášení poplachu dojde automaticky k otevření KTPO. U obou budov v případě vyhlášení požárního poplachu ihned chodí poplachové zprávy i na telefon bezpečnostních pracovníků a určených osob vlastníka areálu.

Budova E má u vstupu turnikety, které je možné otevřít pouze kartou, kterou má každý zaměstnanec v budově nebo přes recepci. V případě evakuace dochází k odjištění a otevření všech turniketů pro volný průchod, přičemž dojde k odjištění dvou únikových východů u hlavního vstupu. V celé budově se zároveň nachází vzduchotechnika pro odvětrávání a odčerpání kouře ze všech místností.



Obrázek 19 Přístupový systém pro ovládání výtahů

(zdroj: [vlastní])

5.1 Režimová opatření

Režimová opatření jsou pevně daná vlastníkem areálu. Režimová opatření pro celý areál se mění dle ročního období. V určitou hodinu tak dochází k uzavření všech vjezdových bran a do areálu následně vjíždí pouze vozidla, respektive osoby, které mají dálkový ovladač pro otevření těchto bran.

V případě vzniku mimořádné události, jako je požár, dojde k automatickému otevření bran i závor, aby byl zajištěn volný průjezd pro integrovaný záchranný systém. V případě, že by se nejednalo o mimořádnou událost požáru, ale i tak bylo třeba otevřít brány nebo závory, mohou tak učinit BP z velínu.

Budova E má také svůj vlastní režim. Po sedmé hodině večer dojde k uzavření objektu a vstup je následně možný pouze pomocí vstupní karty, případně danou osobu musí vpustit ostraha objektu. Jedná-li se o návštěvu, pak si tuto návštěvu musí vyzvednout navštěvovaná osoba, pokud se tato osoba nedostaví, pak není možné návštěvu vpustit a je vyzvána k opuštění objektu – v takovém případě si návštěva musí vyřešit nastalou situaci sama.

Budova D se takto uzavírá v šest hodin večer, kdy je v objektu přítomen bezpečnostní pracovník. V případě obchůzky musí dojít k uzamčení zázemí pro BP a kontroly uzamčení hlavního vstupu. V této době dochází i k sepnutí poplachového zabezpečovacího systému v kancelářských prostorech.

V případě, že se v areálu vyskytují tržby, dochází k navýšení ostrahy, která kontroluje případné návštěvníky, kteří se nachází mimo vyhrazená místa. Zároveň dochází k oblepení míst dvojbarevnou páskou s popisem zákazu vstupu.

5.2 Fyzická ostraha na objektu

Na objektu se nachází vždy tři bezpečnostní pracovníci na směnu. Areál je tak střežen v režimu 24 hodin denně.

Na denní službě se zde nachází vždy dva bezpečnostní pracovníci a recepční. Jeden z bezpečnostních pracovníků vždy sedí na velínu ostrahy, kde ovládá veškeré kamery v areálu včetně dalších technologií budovy.

Na noční službě se nachází pouze 3 bezpečnostní pracovníci, kteří fungují v režimu jeden operátor kamer a technologií a dva bezpečnostní pracovníci, kteří provádí kontrolní obchůzky v areálu.

5.3 Závěr kapitoly

V pátek kapitole byl popsán současný stav bezpečnostních opatření na objektu. Prvotně bylo popsáno celkové shrnutí. Dále se kapitola věnovala režimovým opatřením a poslední část kapitoly se věnuje fyzické ostraze na objektu.

6 IDENTIFIKACE AKTIV A HROZEB NA OBJEKTU

Aby bylo možné provést analýzu rizik na objektu, je potřeba si určit aktiva, která se na objektu nachází a je potřeba je chránit před hrozbami, které je nutné identifikovat. Po identifikaci všech aktiv a hrozeb je možné provést analýzu rizik. K analýze rizik bude využita metoda ETA, která je více popsána v teoretické části práce.

6.1 Identifikace aktiv

Objekt je velmi rozsáhlý a členitý, proto je nutné, aby nedošlo k zanedbání při identifikaci aktiv. Jelikož zde není jenom jeden typ budovy, budou aktiva více rozepsána do kategorií, pod která budou spadat daná aktiva.

Identifikovaná aktiva

- **Lidé**
 - Zaměstnanci na objektu
 - Zaměstnanci soukromé bezpečnostní služby
 - Děti ve školce
 - Návštěvníci
 - Kurýři
 - Taxikáři
- **Objekt**
 - Kanceláře
 - Obchody
 - Restaurace
 - Dětský koutek
 - Holičství
 - Parkoviště venkovní
 - Parkoviště vnitřní
 - Velín fyzické ostrahy
 - Plášť budovy

- Technické místnosti
 - Zázemí údržby
 - Místnost s ovládáním SHZ
- **Finanční prostředky na objektu**
 - Stravenky
 - Hotovost
- **Technické vybavení**
 - Přístupové systémy
 - Kamerové systémy
 - Závory
 - Výtahy
 - Rozvaděče
 - Vzduchotechnika
 - Spotřebiče
 - Tiskárny
 - Počítače
 - Telefony
- **Majetek**
 - Osobní majetek návštěvníků
 - Osobní majetek zaměstnanců
 - Služební vozidla
 - Budovy
 - Vybavení zahrádek
 - Pozemky
 - Služební vozidla dalších firem
 - Zboží prodejných jednotek

- Technické vybavení (viz kategorie Technické vybavení)
- **Informace**
 - Dokumentace objektu
 - Plány budov
 - Data a zálohy
 - Informace o zaměstnancích
 - Informace o zákaznících
 - Osobní údaje
 - Plány firem
 - Určení strategií na další roky
 - Investiční plány
 - Smlouvy se zaměstnanci

6.1.1 Odhad hodnoty aktiv

Cenový odhad aktiv je shrnut v následující tabulce. V tabulce jsou shrnuty 3 hlavní kategorie, u kterých lze odhadnout přibližnou hodnotu aktiv.

Tabulka 1 Odhad hodnoty aktiv

(zdroj: vlastní)

Aktiva	Odhad hodnoty aktiv
Majetek	250 milionů
Technické vybavení	35 milionů
Objekt	900 milionů

6.2 Identifikace hrozeb

Tato kapitola se zabývá identifikací hrozeb, které by mohli ohrozit bezpečnost v objektu.

6.2.1 Hrozby lidského faktoru

Lidský faktor bývá velmi častým a významným zdrojem hrozeb, který může být způsoben více faktory, jako jsou nedbalost, neznalost nebo nezodpovědnost. Velký význam může mít i chybovost při rozhodování v kritických okamžicích nebo i nedostatečným školením zaměstnanců či informováním pracovníků a návštěvníků. V rámci areálu je nejčastější hrozbou vstup podnapilých a agresivních osob na soukromá místa pozemku případně obtěžování návštěvníků v areálu. Dalšími hrozbami jsou napadení, krádeže osobního majetku nebo i majetku firem, vandalismus, úrazy v areálu, podvody a loupeže. Velmi závažnou hrozbou pro areál je z hlediska lidského faktoru způsobení požáru, a to ať už úmyslně nebo neúmyslně. Vzhledem k provozu v areálu je možnou hrozbou i možnost způsobení dopravní nehody nebo srážky s lidmi v areálu. Velmi závažnou hrozbou by mohlo být úmyslné či neúmyslné spuštění samostatného hasicího zařízení případně při stavebních úpravách náhodné spuštění poškozením a následné vytopení objektu.

6.2.2 Technologické hrozby

Technologické hrozby jsou pro objekt závažnou hrozbou. Může jít o výpadek elektrického proudu, problémy s bezpečnostními systémy, osvětlením budovy a areálu, případně problémy s SHZ. Jelikož se v objektu nachází restaurace a obchody, mohl by zde být i problém s únikem plynu nebo prasknutím plynového potrubí včetně následného vznícení. Další hrozbou pro objekt je přerušení nebo prasknutí vodovodního potrubí. Vzhledem k aktuálnímu dění ve světě je potřeba myslet i na hrozbu kybernetických útoků, které by se mohli zaměřit na různé firmy, které sídlí v areálu nebo na bezpečnostní systémy. Další hrozbou je blízké vlakové nádraží, kde by mohlo dojít k vykolejení vlakové soupravy, případně i jiné větší katastrofě, kdy by došlo k únikům nebezpečných látek do okolí, které by následně mohli ohrozit areál.

6.2.3 Přírodní hrozby

Pod pojmem přírodní hrozby se myslí požáry, záplavy, povodně, bouřky, silný vítr nebo tornádo. Jelikož se celý areál nachází v přímé blízkosti řeky je zde zvýšena hrozba záplav. Dále by pro areál mohly být hrozbou požáry, silné bouřky nebo i možnost výskytu tornáda, jelikož se v republice tornáda vyskytují. Protože v okolí nejsou zaznamenány žádné zemětřesení, nejsou brána ani jako hrozba pro areál, ale není možné tuto hrozbu nikdy zcela vyloučit.

6.2.4 Výpis identifikovaných hrozeb

Hrozby způsobené lidským faktorem

- Vandalismus
 - Grafity
 - Ničení, poškození majetku
- Loupež
- Požár
- Užívání návykových látek
- Podvody
- Napadení
- Krádež
- Neúmyslné poškození zaparkovaných vozidel
- Úmyslné poškození zaparkovaných vozidel
- Krádež vozidel
- Žhářství
- Sebevražda
- Poškození přístupových systémů
- Poškození mechanických zábranných systémů
- Kolaps zaměstnanců, návštěvníků
- Dopravní nehoda
- Zablokování nouzových východů
- Úmyslné poškození majetku
- Neúmyslné poškození majetku

Technologické hrozby

- Výpadek elektrického proudu
- Poškození záložních zdrojů elektrického proudu

- Únik vody
- Problémy s SHZ
- Problémy se vzduchotechnikou
- Nefunkčnost přístupových systémů
- Nefunkčnost závor
- Zásah elektrickým proudem
- Vykolejení vlakové soupravy
- Kybernetický útok
 - Napadení databází
 - Narušení bezpečnostních systémů
 - Odcizení osobních údajů

Přírodní hrozby

- Silné deště
- Povodně
- Bouřky
- Požár
- Tornádo
- Zemětřesení

6.3 Analýza rizik metodou kontrolního seznamu

Metoda kontrolního seznamu může velmi dobře sloužit k rychlé kontrole, zda je splněno vše z hlediska zajištění bezpečnosti v areálu. Aby kontrolní seznam nebyl hektický, je možné jej rozdělit do kategorií, jako lidské faktory, technologické faktory a faktory pro přírodní hrozby.

Kontrolní seznam pro lidské faktory

Otázka (kontrolní bod)	Stav ANO	Stav NE	Návrh opatření
Byly dodrženy všechny předpisy a bezpečnostní předpoklady, aby nedošlo k vandalizmu?	x		žádné
Byly naplněny veškeré bezpečnostní předpoklady, aby nedošlo k loupeži v areálu?	x		žádné
Byly naplněny veškeré bezpečnostní předpoklady, aby nedošlo k napadení v areálu?	x		žádné
Byly naplněny veškeré bezpečnostní předpoklady, aby nedošlo ke krádeži vozidla v areálu?	x		žádné

Byly naplněny veškeré bezpečnostní předpoklady, aby nedošlo k loupeži v areálu?	x		žádné
Byly zajištěny revize a pravidelné kontroly EPS, aby nedošlo k požáru v objektu?	x		žádné
Byly naplněny veškeré bezpečnostní předpoklady, aby nedošlo k užívání návykových látek v areálu?	x		žádné
Byly naplněny veškeré bezpečnostní předpoklady, aby nedošlo ke zhářství v areálu?	x		žádné
Byly naplněny veškeré bezpečnostní předpoklady a kontroly rizikových míst, aby nedošlo k sebevraždě v areálu?	x		žádné
Byly provedeny revize a kontroly přístupových systémů, aby nedošlo k jejich poškození?	x		žádné
Byly naplněny bezpečnostní předpoklady, umístěno dopravní značení, aby nedošlo k dopravní nehodě v areálu?		x	Zajištění označení hlavní a vedlejší silnice, v případě zvýšení dopravy v areálu zavedení světelné signalizace
Byly naplněny bezpečnostní předpoklady, včetně školení a předpisů pro zaměstnance, tak aby nedošlo k zablokování únikových východů?		x	Opětovné proškolení zaměstnanců v areálu, povinné školení dodavatelů 1x za rok v areálu, vyvěšení informačních cedulí
Byly dodrženy všechny předpisy a bezpečnostní předpoklady, aby nedošlo k poškození MZS?	x		žádné

Kontrolní seznam pro technologické hrozby

Otázka (kontrolní bod)	Stav ANO	Stav NE	Návrh opatření
Byly zajištěny bezpečnostní předpoklady a dodržování předpisů pro eliminaci výpadku elektrického proudu?	x		žádné

Byly zajištěny revize a pravidelné kontroly náhradního zdroje, aby nedošlo k poruše náhradního zdroje elektrické energie?	x		žádné
Byly zajištěny revize a pravidelné kontroly vodovodního potrubí, aby nedošlo k úniku vody?	x		žádné
Byly naplněny bezpečnostní předpoklady pro zjištění úniku plynu?	x		žádné
Byly zajištěny revize a pravidelné kontroly SHZ, aby nedošlo k technickým problémům s SHZ?	x		žádné
Byly zajištěny revize a pravidelné kontroly vzduchotechniky, aby nedošlo k technickým problémům u vzduchotechniky?	x		žádné
Byly zajištěny revize a pravidelné kontroly osvětlení, aby nedošlo k výpadku osvětlení?	x		žádné
Byly zajištěny revize a pravidelné kontroly automatických závor, aby nedošlo k výpadku funkčnosti?		x	Zajistit pravidelné revize, provádět kontroly funkčnosti systému nejméně 1x za měsíc
Byly zajištěny bezpečnostní předpoklady a revize u zařízení v areálu, aby nedošlo k zásahu elektrickým proudem?	x		žádné

Kontrolní seznam pro přírodní hrozby

Otázka (kontrolní bod)	Stav ANO	Stav NE	Návrh opatření
Byly dodrženy veškeré bezpečnostní postupy aby nedošlo k ohrožení aktiv, při výskytu silných bouřek?	x		žádné
Byly zajištěny bezpečnostní předpoklady při silných deštích?	x		žádné
Byly zajištěny bezpečnostní předpoklady při výskytu záplav?	x		žádné
Byly zajištěny bezpečnostní předpoklady při výskytu povodní?	x		žádné
Byly zajištěny bezpečnostní předpoklady a stanoveny postupy při výskytu požáru?	x		žádné

Byly zajištěny bezpečnostní předpoklady a stanoveny postupy při výskytu tornáda?		x	Doporučeno školení zaměstnanců, jak se chovat při výskytu tornáda, zajistit kontroly střešních kritin.
Byly zajištěny bezpečnostní předpoklady a stanoveny postupy při výskytu zemětřesení?		x	Doporučeno školení zaměstnanců, jak se zachovat při výskytu zemětřesení.

6.4 Analýza rizik metodou FMEA

Jako druhý typ vhodné metody analýzy rizik pro vybraný areál byla vybrána metoda FMEA. Hlavním cílem vybrané metody je jednoznačná identifikace vztahu mezi identifikovanými hrozbami a chráněnými aktivy. Identifikovaný vztah následně představuje riziko. V průběhu vypracování metody je zapotřebí pracovat se třemi faktory. Těmi jsou výskyt, význam a odhalitelnost. Výsledek součinu těchto faktorů je risk priority number (dále jen RPN), které dále představuje číselné ohodnocení závažnosti rizika. V analýze rizik se již pracuje s identifikovanými hrozbami, jejich příčinou vzniku a dopadu hrozby na objekt nebo aktiva, která se na objektu nachází. Dále jsou zde vypsána aktuální opatření a následně nová bezpečnostní opatření, která snižují aktuální hrozby. Hodnota RPN je určena při aktuálně zavedených opatřeních a následně znovu po zavedení nových bezpečnostní opatření na snížení hodnoty RPN.

Aby byla aplikace metody FMEA správná, pak je zapotřebí si určit hodnotící tabulky již dříve zmíněných faktorů, se kterými se následně pracuje v analýze rizik. První tabulka určuje výskyt dané hrozby v areálu, dále pak jen na objektu.

Tabulka 2 Tabulka výskytu hrozeb.

(Zdroj: upraveno z [35])

Výskyt		
Úroveň	Označení	Pravděpodobnost výskytu
1	Velmi vzácné	Méně než 1x za 5 let
2	Vzácné	Přibližně 1x za 3-5 let
3		Přibližně 1x za 2-3 roky
4	Časté	Přibližně 1x za rok
5		Přibližně 2 - 3x za rok
6		Přibližně 4 - 5x za rok
7	Pravděpodobné	Přibližně 6 - 9x za rok
8		Přibližně 10 - 20x za rok
9	Téměř jisté	Přibližně 21 - 49x za rok
10		Více než 49x za rok

V další tabulce je rozepsán význam hrozeb s jejich dopadem na areál nebo chráněné aktivum. Dopad na areál je určen i omezením provozu a slovním ohodnocení možných finančních ztrát v areálu.

Tabulka 3 Tabulka významu hrozeb s dopadem na areál.

(Zdroj: upraveno z [35])

Význam		
Úroveň	Označení	Dopad na průmyslový areál
1	Velmi nízký	Žádný dopad na provoz areálu, žádná finanční ztráta
2	Nízký	Minimální dopad na provoz areálu, minimální finanční ztráta
3		Nízký dopad na provoz areálu, nízká finanční ztráta
4	Střední	Vyšší dopad na provoz areálu, překonatelná finanční ztráta
5		Značný dopad na provoz areálu, značná finanční ztráta
6		Velký dopad na provoz areálu, velká finanční ztráta
7	Vysoký	Významný dopad na provoz areálu, velmi vysoká finanční ztráta
8		Kritický dopad na provoz areálu, extrémní finanční ztráta
9	Velmi vysoký	Téměř zničující dopad na provoz areálu, nesmírná finanční ztráta
10		Zničující dopad na provoz areálu, zastavení provozu, nezvratné škody

Poslední tabulka se již zabývá možností odhalení dané hrozby. Pokud by došlo k projevu hrozby, dle hodnot v tabulce je pak ukázána její pravděpodobnost odhalení.

Tabulka 4 Pravděpodobnost odhalení hrozby.

(Zdroj: upraveno z [35])

Odhalitelnost		
Úroveň	Označení	Pravděpodobnost odhalení hrozby
1	Velmi vysoká	Hrozba je téměř vždy odhalena
2	Vysoká	Hrozba má velmi vysokou pravděpodobnost odhalení
3		Hrozba má vysokou pravděpodobnost odhalení
4	Střední	Hrozba má středně vysokou pravděpodobnost odhalení
5		Hrozba má střední pravděpodobnost odhalení
6		Hrozba má nízkou pravděpodobnost odhalení
7	Nízká	Hrozba má velmi nízkou pravděpodobnost odhalení
8		Hrozba má minimální pravděpodobnost odhalení
9	Velmi nízká	Hrozba není téměř nikdy odhalena
10		Hrozbu není možné odhalit

Po identifikaci hrozeb, aktiv a současných opatření následuje vyhodnocení rizik, které je určeno již dříve zmíněnou hodnotou RPN, a to po součinu výskytu, významu a odhalitelnosti hrozby. V níže uvedené tabulce je rozsah přijatelnosti hodnot RPN.

Tabulka 5 Přijatelnost hodnot RPN

(zdroj: vlastní)

Přijatelnost hodnot RPN					
Úroveň rizika	Bezvýznamné riziko	Přijatelné riziko	Střední riziko	Vysoké riziko	Nepřijatelné riziko
Rozsah RPN	1-150	151-300	301-600	601-800	801-1000

Aktivum	Hrozba	Příčina hrozby	Dopad hrozby	V ý s k y t	V ý z n a m	O d h a l i t e l n o s t	RPN	Současná opatření	Nalezené nedostatky	Doporučená opatření	V ý s k y t	V ý z n a m	O d h a l i t e l n o s t	RPN
Objekt	Vandalismus	Příležitost	Poškození pláště objektu	6	4	2	48	Kontrola osamocených prostor pomocí CCTV, obchůzky celého areálu	Nedostatečné pokrytí pomocí CCTV	Analýza v kamerách na inkriminovaných místech	2	4	1	8
Lidé	Napadení	Alkohol, drogy, příležitost	Újma na zdraví pracovníka	2	4	2	16	Školení, ochranné prvky	Fyzická zdatnost BP	žádná	2	4	2	16
			Újma na zdraví návštěvníka	1	6	5	30	BP ve službě	žádné	žádné	1	6	5	30
Majetek	Krádež	Alkohol, drogy, příležitost	Ztráta aktiv, poškození firmy	3	4	6	72	BP ve službě, CCTV na objektu	Volný, nekontrolovaný vstup do areálu	Využití AI v kamerách	2	4	2	16
Reputace	Poškození zaparkovaných vozidel	Alkohol, drogy	Ztráta reputace, důvěryhodnosti, žaloba	4	3	4	48	CCTV na parkoviště, obchůzky	Selhání BP	Využití AI v kamerách	2	3	2	12
Majetek		Nezodpovědnost při manipulaci s vozidlem (parkování)	Poškození majetku	10	4	5	200	CCTV na parkoviště, obchůzky	Selhání BP, selhání CCTV	Využití AI v kamerách	2	4	2	16
Majetek, reputace	Krádež vozidel	Alkohol, drogy, příležitost	Ztráta majetku, reputace, důvěryhodnosti, žaloba	1	7	6	42	CCTV na parkoviště, obchůzky	Selhání BP, selhání CCTV, chybné zabezpečení vozidla	Využití AI v kamerách	2	7	2	28

Obrázek 20 Vypracovaná tabulka metodou FMEA

(zdroj: vlastní)

Aktivum	Hrozba	Příčina hrozby	Dopad hrozby	V ý s k y t	V ý z n a m	O d h a l i t e l n o s t	RPN	Současná opatření	Nalezené nedostatky	Doporučená opatření	V ý s k y t	V ý z n a m	O d h a l i t e l n o s t	RPN
Majetek	Loupež	Alkohol, drogy, příležitost	Ztráta aktiv, poškození firmy	6	8	9	432	BP ve službě, CCTV, pravidelné obchůzky BP	Setrnutí BP, selhání CCTV, nedodržení obchůzek, chybné zabezpečení ze strany síťového	využití AI v kamerách, častější obchůzky BP - kontrola uzamčení prostor, doporučení	4	8	2	64
Objekt, majetek, lidé	Požár	Neúmyslné založení	Újma na zdraví, poškození aktiv	3	7	7	147	BP ve službě, CCTV, pravidelné obchůzky BP, EPS v budovách	žádné	AI analýza v kamerách	3	7	3	63
		Úmyslné založení s cílem poškození	Újma na zdraví, poškození aktiv	1	8	8	64	BP ve službě, CCTV, pravidelné obchůzky BP, EPS v budovách	žádné	AI analýza v kamerách	1	8	3	24
	Žhářství	Úmysl poškodit objekt nebo firmu	Újma na zdraví, poškození aktiv, poškození objektu	1	10	8	80	BP ve službě, CCTV, pravidelné obchůzky BP, EPS v budovách	žádné	žádné	1	10	8	80
Lidé	Užívání návykových látek	Drogová závislost, finanční krize	Újma na zdraví, poškození firmy	2	3	3	18	Pravidelné obchůzky BP	Nedodržení obchůzek BP, výpadek CCTV, slepá místa CCTV	Nové kamery na inkriminovaná místa, častější obchůzky BP, AI v kamerách	2	3	2	12
	Podvody	Finanční krize, příležitost	Ztráta aktiv, poškození jména firmy, újma na zdraví	1	4	5	20	Školení pracovníků, varovné emaily	žádné	žádné	1	4	5	20
	Sebevražda	Zkrat jedince, ztráta zaměstnání	Újma na zdraví, poškození firmy	1	8	3	24	Kontrola vstupu na vyhlídku nejvyšší budovy, obchůzky BP, bariéry na	žádné	žádné	1	8	3	24

Aktivum	Hrozba	Příčina hrozby	Dopad hrozby	V ý s k y t	V ý z n a m	O d h a l i t e l n o s t	RPN	Současná opatření	Nalezené nedostatky	Doporučená opatření	V ý s k y t	V ý z n a m	O d h a l i t e l n o s t	RPN
Objekt, majetek	Bouřky	Přírodní jev	Poškození pláště budov, poškození areálu	8	3	3	72	Sledování meteorogických předpovědí	žádné	žádné	8	3	3	72
	Tornáda	Přírodní jev	Poškození pláště budov, poškození areálu	1	10	7	70	Sledování meteorogických předpovědí	žádné	žádné	1	10	7	70
	Zemětřesení	Přírodní jev	Poškození pláště budov, poškození areálu	1	10	10	100	žádné	žádné	žádné	1	10	10	100
Lidé	Bouřky	Přírodní jev	Újma na zdraví	8	3	3	72	Sledování meteorogických předpovědí	žádné	žádné	8	3	3	72
	Tornáda	Přírodní jev	Újma na zdraví	1	10	5	50			žádné	1	10	5	50
Objekt, majetek, lidé	Povodně	Přírodní jev	Újma na zdraví, poškození pláště objektu, poškození majetku	1	10	8	80		žádné	Školení pro zaměstnance, protipovodňové bariéry	1	10	4	40

Aktivum	Hrozba	Příčina hrozby	Dopad hrozby	V ý s k y t	V ý z n a m	O d h a l i t e l n o s t	RPN	Současná opatření	Nalezené nedostatky	Doporučená opatření	V ý s k y t	V ý z n a m	O d h a l i t e l n o s t	RPN
Objekt, majetek	Poškození přístupových systémů	Neúmyslné poškození, chyba zaměstnanec, chyba úklidu	Nekontrolova ný vstup osob do objektu	3	3	10	90	Pravidelné kontroly softwaru	žádné	žádné	3	3	10	90
Lidé	Kolaps zaměstnanec, návštěvníka	Vysoká teplota, zdravotní stav	Újma na zdraví pracovníka	8	3	8	192	Hlídání teplot uvnitř objektu (klimatizace), pravidelné zdravotní prohlídky BP	žádné	Varovné značení před výkyvy teplot, AI v CCTV	4	3	2	24
Lidé, majetek	Dopravní nehoda	Nepozornost řidiče, drogy, alkohol	Újma na zdraví, poškození aktiv	8	5	6	240	CCTV na inkriminovaná místa areálu	Nedostatky v lidských zdrojích	Dopravní značení, AI v CCTV	1	5	3	15
Lidé	Zablokování nouzových východů	Nepozornost, úmysl	Újma na zdraví	4	10	2	80	Kontrola únikových východů při obchůzce BP	žádné	Varovné značení pro neblokovaní únikových východů. AI v CCTV	2	10	2	40
Lidé, majetek	Dopravní nehoda	Alkohol, drogy	Poškození majetku, újma na zdraví	8	5	6	240	CCTV na inkriminovaná místa areálu	žádné	AI v CCTV	1	5	3	15
Objekt, majetek	Výpadek elektrického proudu	Nezodpovědn ost při manipulaci s vozidlem (parkování)	Poškození objektu, či majetku, ztráta dat	5	7	8	280	Záložní zdroje pro potřebné systémy	Selhání záložních zdrojů	Pravidelné revize a kontroly záložních zdrojů	3	7	2	42
Objekt, majetek	Únik vody	Nedbalost, neprovádění revizí, kontrol	Poškození objektu a majetku	3	9	10	270	Revize vodovodního potrubí, kontrola tlaku v potrubí	Selhání čidel tlaku v potrubí	Pravidelné revize a kontroly čidel včetně vodovodního potrubí	2	9	2	36

Aktivum	Hrozba	Příčina hrozby	Dopad hrozby	V ý s k y t	V ý z n a m	O d h a l i t e l n o s t	RPN	Současné opatření	Nalezené nedostatky	Doporučená opatření	V ý s k y t	V ý z n a m	O d h a l i t e l n o s t	RPN
Lidé, majetek	Kybernetický útok	Nedodržení rychlosti, chyba na straně strojvedoucího, úmysl	Ztráta osobních dat, narušení soukromí	2	5	5	50	Školení zaměstnanců, antivirové ochrany, blokování domén	žádné	Pravidelné školení pracovníků	1	5	3	15
	Vykolejení vlakové soupravy	Nedodržení rychlosti, chyba na straně strojvedoucího, úmysl	Poškození aktiv, újma na zdraví	1	7	10	70	žádné	žádné	žádné	1	7	10	70
	Požár	Nedodržení předpisů	Újma na zdraví, poškození aktiv	2	7	7	98	CCTV na inkriminovaná místa areálu	žádné	AI v CCTV	1	5	3	15
Objekt, majetek	Problémy s SHZ	Nedodržení revizí, pravidelných kontrol systému	Poškození majetku, objektu	4	10	8	320	Pravidelné revize a kontroly SHZ	žádné	Měsíční kontroly funkčnosti SHZ	2	10	2	40
Majetek, informace	Kybernetický útok	Slabá ochrana	Ztráta dat firem, narušení bezpečnostních systémů,	2	5	5	50	Školení zaměstnanců, antivirové ochrany, blokování domén	žádné	žádné	1	5	5	50
Objekt	Vykolejení vlakové soupravy	Nedodržení rychlosti, chyba na straně strojvedoucího, úmysl	Poškození objektu	1	7	10	70	žádné	žádné	žádné	1	7	10	70
	Nefunkčnost závor	Nedodržení revizí, pravidelných kontrol systému	Zablokování průjezdnosti v objektu, vznik kolon	7	4	5	140	žádné	žádné	Pravidelné revize a testování funkčnosti závor	3	4	3	36

6.5 Vyhodnocení analýzy rizik

Vypracováním analýzy rizik bylo nalezeno celkem 31 rizik na objektu. Použitím analýzy rizik byly nalezeny pouze dvě rizika, která mají střední závažnost. Těmito riziky jsou loupež a problémy se samostatným hasícím zařízením.

6.5.1 Vyřešení nalezených rizik

V této kapitole bude popsáno řešení u nalezených rizik, u kterých bylo potřeba navrhnout patřičná opatření. Rizika, která nejsou dále uvedena a řešena jsou brána jako bezvýznamná nebo přijatelná rizika a to dle jejich výsledku RPN.

Střední riziko

- Loupež (aktivum majetek), RPN: 432
- Problémy s SHZ (aktivum objekt, majetek), RPN: 320

Přijatelné riziko

- Poškození zaparkovaných vozidel (aktivum majetek, reputace), RPN: 200
- Kolaps zaměstnance, návštěvníka (aktivum lidé), RPN: 192
- Dopravní nehoda (aktivum lidé, majetek), RPN: 240
- Výpadek elektrického proudu (aktivum objekt, majetek), RPN: 280
- Únik vody (aktivum objekt, majetek), RPN: 270

Bezvýznamné riziko

- Vandalismus (aktivum objekt), RPN: 48
- Krádež (aktivum majetek), RPN: 72
- Poškození zaparkovaných vozidel (majetek, reputace), RPN: 48
- Krádež vozidel (aktivum majetek, reputace), RPN: 42
- Požár neúmyslně založen (aktivum lidé, objekt, majetek), RPN: 147
- Požár úmyslně založen (aktivum lidé, objekt, majetek), RPN: 64
- Užívání návykových látek (aktivum lidé), RPN: 18
- Povodně (aktivum objekt, majetek, lidé), RPN: 80
- Zablokování nouzových východů (aktivum lidé), RPN: 80
- Kybernetický útok (aktivum majetek, informace), RPN: 50
- Požár (aktivum lidé, majetek), RPN: 98
- Nefunkčnost závor (aktivum objekt), RPN: 140

6.6 Závěr kapitoly

Šestá kapitola se zabývala metodou analýzy rizik FMEA. Z výsledků analýzy bylo odhaleno celkem 31 rizik, z toho pouze 2 rizika byla zjištěna se závažností jako střední rizika. Ostatní rizika byla brána jako přijatelná nebo bezvýznamná. Návrh opatření byl proveden na taková rizika, u kterých se očekává jejich výskyt.

7 NÁVRH BEZPEČNOSTNÍHO OPATŘENÍ

Návrh bezpečnostního opatření vychází z provedené analýzy rizik FMEA, kde byla nalezena rizika, které lze minimalizovat pro zajištění vyšší bezpečnosti v celém areálu. Celý návrh bezpečnostního opatření je zaměřen na rizika v kapitole 6.5.1. Opatření budou rozdělena do kategorií včetně možného cenového důsledku pro majitele areálu.

7.1 Navýšení počtu fyzické ostrahy

Při aktuálním stavu 3 členů fyzické ostrahy na den i noc je objekt strážěn v režimu 24 hodin, 7 dní v týdnu.

Aby bylo možné adekvátně reagovat na všechna rizika a eliminovat jejich stav, musel by se počet bezpečnostních pracovníků navýšit minimálně o 2 BP na směnu. Tedy by muselo být v celém areálu 5 BP, z toho 3 BP na objektu T a 2 BP na objektu D.

Pokud vezmeme v potaz průměrnou fakturační cenu 240,- za hodinu a režim 24/7, pak by byl počet odsloužených hodin za 1 měsíc 3600 hodin. S průměrnou cenou 240,- za hodinu by pak majitel platil měsíčně 864.000,-. Z tohoto důvodu je pouze navýšení fyzické ostrahy neekonomické a bylo by vhodnější najít rovnovážný vztah s využitím technologií.

Samotné navýšení fyzické ostrahy ovšem nezajistí, že se nám minimalizují veškerá rizika, jelikož s fyzickou ostrahou mohou být komplikace lidského faktoru. Bezpečnostní pracovník se nemusí dostavit na směnu, může onemocnět, zranit se během výkonu služby, usnout, vynechat obchůzku nebo nereagovat na poplachový stav. Zároveň i přesto, že bude více lidí sledovat kamery, může nastat, že zrovna bude sledovat jiný náhled a dojde tak k přehlédnutí zloděje nebo úrazu v areálu.

7.2 Zabezpečení pouze technologiemi

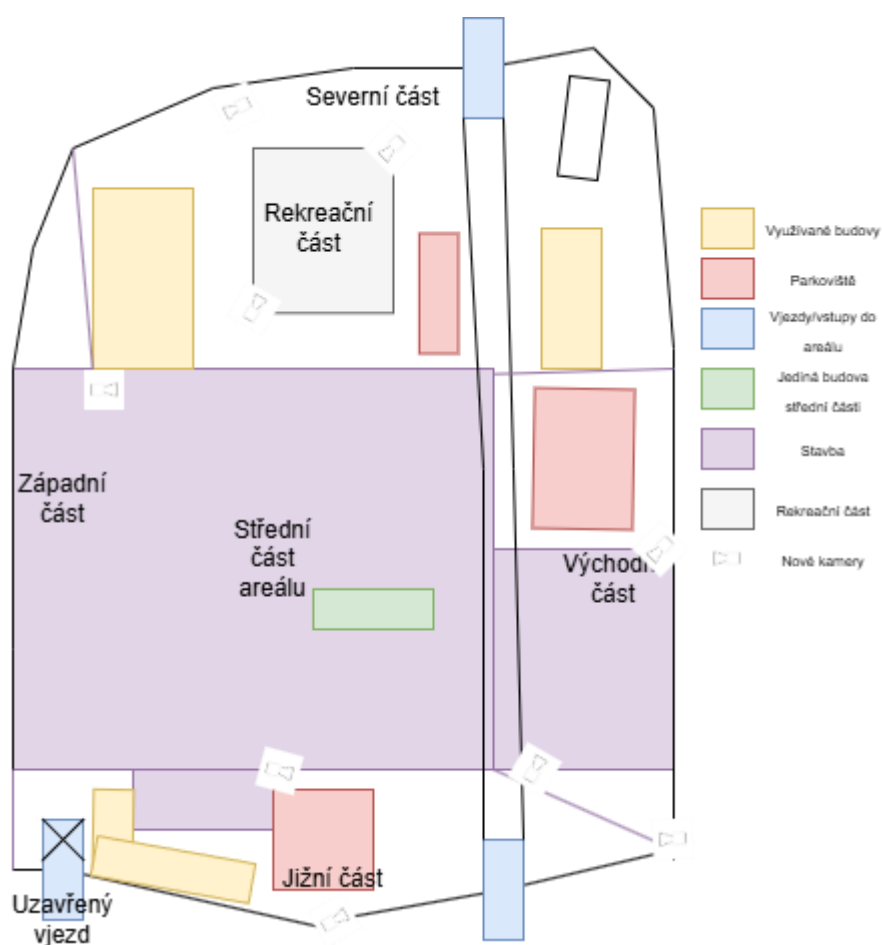
Jelikož se na objektu již vyskytují kamery, EPS, PZTS, přístupové systémy, automatické závory, pak by se toto řešení mohlo jevit jako nejvýhodnější, pokud vezmeme v potaz vyšší prvotní investice do nových technologií a rozšíření již stávajících.

Jednou z možností, jak zajistit zlepšení pomocí technologií by byla investice do softwaru AI v kamerách. Tímto by došlo k eliminaci lidského faktoru. Jelikož by však samotné AI nemohlo více reagovat na vyvolávající podnět alarmu, bylo by třeba zajistit napojení kamerového systému včetně poplašného, zabezpečovacího systému a EPS na DPPC, kde by byla následná reakce ze strany operátora dle zásahového plánu.

AI v kamerách by mohla zajistit vyvolání poplachu v případě zjištění zablokování nouzových východů například dodaným zbožím, při zjištění vandalismu na objektu, kolapsu zaměstnance nebo i dopravní nehody.

Dále by bylo vhodné umístit další kamery na inkriminovaná místa, kde může dojít například k vandalismu, užívání návykových látek nebo založení požáru. Celkově by bylo vhodné přidat ještě 9 kamer a to tak, aby došlo k zamezení možnosti vzniku slepého místa.

Tímto způsobem dojde k eliminaci slepých míst a k rozšíření kontroly kamerovým systémem nad objektem.



Obrázek 21 Plánek návrhu navýšení počtu kamer

(zdroj: vlastní)

Pro eliminaci problémů s SHZ by bylo možné využít automatický dohledový systém SHZ, který by pomocí čidel kontroloval otevřenost/zavřenost ventilů, tlak a průtok v potrubí a napájení čerpadel a motorů.

Pro povodně by bylo možné využít automatizované protipovodňové bariéry. K tomu by byly využity čidla v blízkosti vody a pokud by došlo k zatopení těchto čidel, pak by se spustil systém s automatickými bariérami. Tyto bariéry by pak mohly zabránit vylití vody až do areálu a eliminovat tak poškození majetku.

Jednou z velmi zajímavých technologií, která by mohla zcela nahradit fyzickou ostrahu na obchůzkách by byl automatický dron, který by byl naprogramován na různé časy a vykonával by tak dohled nad celým areálem. Jednou z nevýhod je, že dron by nemusel vzlétnout kvůli nepříznivému počasí nebo příliš vysokému větru. Značnou výhodou ovšem je možnosti upgradu dronu termokamerou, přídavným světlem nebo reproduktorem. Jelikož je dron zcela autonomní, pak není potřeba žádného operátora, jelikož dron se nastaví na přesný čas ve který má vzlétnout a provést kontrolu objektu. Pokud by nebylo možné z důvodu nepříznivého počasí vzlétnout, pak by bylo možné využít napojení na DPPC, který by vyslal na místo mobilní patrolu, která by potřebnou kontrolu provedla za dron.

Hlavní nevýhodou by mohla být vyšší pořizovací cena včetně možného rušení signálů z okolních budov.

Pro budovy do ulice mimo areál by bylo vhodné využít detektory tříštění skla, která by následně byla připojena na PZTS. S tím je i spojené ošetření loupeže, kde by bylo možné napojit systém PZTS na PČR. Díky tomu bychom mohli zkrátit reakční dobu a dobu příjezdu PČR.

7.3 Zabezpečení kombinací FO a technologiemi

Jelikož je tato možnost využívána i aktuálně, doporučil bych i její zachování s případným rozšířením o jednoho BP na denní směnu a modernizací kamerového systému včetně využívání AI v kamerách a doplnění o automatizovaný dron.

Využitím AI v kamerách by mohlo docházet k rychlému odhalení hrozeb, neoprávněných vstupů nebo ničení majetku na objektu, přičemž operátor CCTV by si mohl kontrolovat pouze kamery, které nutně potřebuje a mohlo by tak docházet k rychlé reakci na hrozby. Vzhledem k rychlé detekci by nemuselo ani dojít ke zbytečně velkému navyšování fyzické ostrahy (stačil by tedy nárůst o 1 BP), přičemž by stále byla zachována kvalita služby s lepšími výsledky při detekci hrozeb.

Dále by bylo vhodné umístit další kamery na inkriminovaná místa viz. Obrázek 21, kde může dojít například k vandalizmu, užívání návykových látek nebo založení požáru.

Vzhledem k rozsahu objektu by bylo dobré i uvažovat nad využitím automatizovaného dronu. Jelikož je dron plně automatizovaný, je možno jej nastavit na určité časy, kdy bude provádět kontrolu na předem nastavených trasách. Zároveň lze udělit ostraze přístup k manuálnímu startu dronu. Ostraha by mohla dron zastavit na místě a využít ke sledování například vandala při inkriminující činnosti z dálky pomocí kamer umístěných na dronu. Z důvodů plné automatizace dronu, není třeba mít na objektu pracovníka, který by dron pilotoval a musel by tak mít ze zákona splněny pilotní zkoušky. Tento dron by mohl vypomáhat při nočních obhlídkách například termokamerou, která by mohla napomáhat při detekci neoprávněných osob v areálu, případně při vandalismu. Jednou z mnoha dalších výhod by mohla být i vizuální kontrola vysokých budov, případně střech, například po živelných pohromách. Z hlediska finančních úspor vychází i tyto kombinace nejlépe z dlouhodobého hlediska. Pokud by dron například z důvodu nepříznivého počasí nemohl vzlétnout, byla by provedena potřebná kontrola přítomnou fyzickou ostrahou.

Nákup licencovaného dronu je dle vybavení zhruba investicí od 200.000,- do 500.000,-, zde by postačil menší dron s možností termokamery a dobou letu do zhruba 40 minut. Doba dobíjení je pak zhruba 1,5 hodinu, záleží na typu dronu a kapacitě baterie.

Pro eliminaci problémů s SHZ by bylo možné využít automatický dohledový systém SHZ, který by pomocí čidel kontroloval otevřenost/zavřenost ventilů, tlak a průtok v potrubí a napájení čerpadel a motorů. Dále by bylo možné napojit tyto systémy na EPS, kde by v případě selhání došlo k vyhlášení poplachu, který by si následně odbavil bezpečnostní pracovník.

Aplikace AI do již aktuálních kamer na objektu by byla z prvotních nákladů dražší, ale úspora by se objevila již po několika měsících. Pokud vezmeme v potaz, že je na objektu zhruba 100 kamer, které mohou fungovat s AI, pak by licence, na každou kameru stála jednorázově 1500,-. Pokud by majitel chtěl servery u sebe na objektu, pak se cena za pronájem těchto serverů pohybuje v ceně od 60.000,- do 400.000,-. Cena za licence by tedy byla jednorázově 150.000,-, následně server včetně úložiště s předplaceným servisem za 500.000,-. Celková cena by se tedy mohla pohybovat do 650.000,-. Pak je nutné řešit výběru dodavatele, kde by mohla být sleva případně lehce se odlišující ceny, výměna kamery a případné instalační úpravy. I přes možné odchylky ceny se jeví celá aplikace AI jako nejvýhodnější. Vezmeme-li v potaz rezervu +20%, pak by se celková konečná cena mohla pohybovat okolo 870.000,-, tedy jsem na skoro stejné ceně jako za navýšení fyzické ostrahy s tím rozdílem, že tato částka se nebude opakovat každý měsíc, ale bude jednorázová.

Abychom zajistili i fungování kamer při výpadku elektrického proudu, pak by bylo vhodné zajistit jeden náhradní generátor pouze pro kamery, tak aby bylo možné zajistit funkcionalitu po dobu alespoň 2 hodin. Cena takového agregátu se pohybuje od 50.000,-.

7.4 Komparace efektivností

Efektivnost u všech možností může být sporná, ale jednoznačně nejlepší volbou z hlediska efektivnosti je kombinace fyzické ostrahy a technologií.

Areál s mnoha návštěvníky není možné nechat pouze pod dohledem technologií, jelikož by nám tímto vznikla nová rizika, která by mohla mít katastrofální následky. Případné řešení bezpečnostního návrhu na nová rizika by se mohlo prodražit. Zároveň při vzniku nestandardní situace jako je prasknutí vodovodního potrubí nebo spuštění SHZ je potřeba rychlé reakce. K tomu by mohl sloužit detektor tlaku vody, který by následně vyhlásil poplach a přivolal techniky nebo mobilní patrolu, zásahovou jednotku. Ale v takovém případě se bavíme o dojezdu v řádech minut až desítek minut.

U mnoha nestandardních situací je potřeba rychlé reakce, proto by měla být fyzická ostraha zachována a mělo by dojít k podpoření jejich reakcí, tak aby docházelo, co k nejmenším prodlevám mezi vznikem a reakcí.

Zajištění pouze navýšením fyzickou ostrahou nebude řešit příliš mnoho, protože zde hraje hlavní roli lidský faktor popsáný již v kapitole 7.1. Teoretické zvýšení efektivnosti zde je, ale bude velmi proměnlivé i podle bezpečnostního pracovníka, který zrovna bude ve službě.

Z hlediska efektivnosti nejlépe vychází doplnění AI do kamer, jelikož tímto zabezpečením můžeme dosáhnout snížení středního rizika loupeže, přijatelného rizika kolapsu zaměstnance, dále pak i bezvýznamná rizika jako vandalismu, krádeže, užívání návykových látek, úmyslné nebo neúmyslné založení požáru nebo zablokování nouzových východů.

Využití dronu snižují střední riziko loupeže a bezvýznamná rizika jako vandalismu, krádeže a vzniku úmyslných i neúmyslných požárů.

Pro řešení středního rizika, problémů s SHZ je možné využít automatický dohled pro SHZ, který pomocí čidel může kontrolovat stav tlaku vody, polohu ventilů nebo napájení čerpadel a motorů.

7.5 Závěr kapitoly

V této kapitole byla vzata v potaz rizika na objektu a jejich možnosti řešení. Návrh bezpečnostního opatření byl brán z hlediska navýšení fyzické ostrahy, zabezpečení objektu pouze technologiemi a kombinací fyzické ostrahy a technologií, která se i nyní na objektu nachází. Ze zvážení všech možností vychází nejlépe rozšíření aktuální ostrahy s využitím dalších možností nových technologií, které zvýší bezpečnost v objektu.

ZÁVĚR

Tato bakalářská práce se zaměřila na problematiku bezpečnosti v jednom bývalém průmyslovém areálu, s důrazem na analýzu rizik a návrhu vhodného a efektivního bezpečnostního opatření. Na vybraném bývalém průmyslovém areálu byl popsán postup a význam řízení rizik, který je nezbytný pro následné zachování a zajištění bezpečného prostředí pro zaměstnance, návštěvníky i majetek.

V teoretické části bakalářské práce byly definovány základní termíny řízení rizik, jako je aktivum, hrozba, zranitelnost, bezpečnostní opatření, riziko, zbytkové riziko a narušení, které jsou klíčové při vypracování analýzy rizik. V této části byly představeny některé metody analýzy rizik, a to kvalitativní metody, tak i kvantitativní metody, které následně umožňují systematický přístup k identifikaci rizik na vybraném areálu.

Praktická část bakalářské práce uvedla konkrétní popis bývalého průmyslového areálu včetně aktuálního zabezpečení, které je dostačující vzhledem k aktuálnímu stavu, ale do budoucna, jak se bude celý areál měnit nebude stačit a budou se stále více objevovat slabá místa v zabezpečení, která by mohla být v budoucnu zneužita hrozbou a vést tak ke zhoršení bezpečnosti areálu. K tomu byla použita metoda FMEA (Failure Mode and Effect Analysis), která tak umožnila detailní posouzení rizik a identifikaci slabých míst, na která je potřeba se zaměřit.

Na základě vypracování analýzy rizik byla identifikována rizika jako jsou loupež, problémy s SHZ, krádež, vandalismus nebo nehoda v areálu, a to na základě výsledků analýzy rizik byla navržena konkrétní bezpečnostní opatření, která zahrnují 3 různé přístupy podle typu zabezpečení včetně cenového určení. První návrh bezpečnostního opatření byl navrhnout pouze zvýšení počtu bezpečnostních pracovníků, který by ovšem cenově nebyl výhodný a není ani zaručeno zvýšení bezpečnosti na objektu. Druhý návrh pracoval pouze s verzí technologií, ale jelikož se areál bude v průběhu let měnit, není příliš vhodné se spoléhat na technologie, které by se navíc musely navrhnout již s budoucí vizualizací celého areálu a nejspíše by muselo docházet k častým změnám, které jsou nákladné a pro majitele objektu ne příliš výhodné. Třetí návrh již zahrnuje fyzickou ostrahu i technologie, což odpovídá i aktuálnímu způsobu zabezpečení. V poslední kapitole byla popsána komparace efektivnosti jednotlivých typů návrhů zabezpečení.

Velkým a důležitým přínosem této práce je poskytnutí praktického doporučení, která mohou být aplikována i na jiné areály či komplexy budov. Vede k zefektivnění řízení rizik a

implementaci bezpečnostních opatření, které tak mohou významně přispět ke zvýšení bezpečnosti a snížení potencionálních škod.

Na závěr lze říct, že zajištění bezpečnosti v takto rozsáhlých průmyslových areálech je velmi složitý proces, který vyžaduje systematický a ucelený přístup s neustálým zlepšováním a hledáním hrozeb, které mohou narušit bezpečnost. Tato bakalářská práce dále přispívá k lepšímu porozumění problematice analýzy rizik s přispěním konkrétních nástrojů a metod pro efektivní řízení rizik, které by měly vést k bezpečnějšímu a příjemnějšímu prostředí nejen v tomto vybraném průmyslovém areálu.

SEZNAM POUŽITÉ LITERATURY

- [1] *Řízení rizik*. Online. Businessinfo. 2006. Dostupné z: <https://www.businessinfo.cz/navody/rizeni-rizik/>. [cit. 2024-12-31].
- [2] *Základy řízení rizik ve firmě*. Online. Aptien. C2023. Dostupné z: <https://aptien.com/cs/kb/articles/risk-management>. [cit. 2024-12-31].
- [3] MAREŠ, Miroslav; REKTOŘÍK, Jaroslav a ŠELEŠOVSKÝ, Jan . *Krizový management: Případové bezpečnostní studie*. Ekopress, 2013. ISBN 978-80-86929-92-7.
- [4] *Bezpečnostní posouzení – revize současného stavu Vaší bezpečnosti*. Online. Bezpečnostní konzultant. C2022. Dostupné z: <https://www.bezpecnostnikonzultant.cz/bezpecnostni-analyza/>. [cit. 2024-12-31].
- [5] *Analýza rizik: Jemný úvod do analýzy rizik*. Online. Mchblog. 23. dubna 2012. Dostupné z: <http://mch2blog.blogspot.com/2012/04/analyza-rizik.html>. [cit. 2024-12-31].
- [6] *Co jsou aktiva z pohledu rizik*. Online. Aptien. C2023. Dostupné z: <https://aptien.com/cs/kb/articles/what-are-assets-in-risk-management>. [cit. 2024-12-31].
- [7] *Hrozby*. Online. Kybez. C2021. Dostupné z: <https://kybez.cz/hrozby/>. [cit. 2024-12-31].
- [8] *Co je to zranitelnost*. Online. Aptien. C2023, 2024. Dostupné z: <https://aptien.com/cs/kb/articles/what-is-vulnerability>. [cit. 2024-12-31].
- [9] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II. 2*. VeRBuM, 2012. ISBN 978-80-8750-019-4.
- [10] *Zranitelnost (Vulnerability)*. Online. Managementmania. C2011-2016. Dostupné z: <https://managementmania.com/cs/zranitelnost-vulnerability>. [cit. 2024-12-31].
- [11] *Protiopatření (Countermeasures)*. Online. Managementmania. C2011-2016. Dostupné z: <https://managementmania.com/cs/protiopatreni-countermeasures>. [cit. 2024-12-31].

- [12] *Riziko*. Online. Ministerstvo Vnitra České republiky. 2003. Dostupné z: <https://mv.gov.cz/clanek/riziko.aspx>. [cit. 2024-12-31].
- [13] *Rizika (Risks)*. Online. Managementmania. C2011-2016. Dostupné z: <https://managementmania.com/cs/rizika>. [cit. 2024-12-31].
- [14] *Inherent vs. residual risk*. Online. Cleverandsmart. 2013. Dostupné z: <https://www.cleverandsmart.cz/inherent-vs-residual-risk/>. [cit. 2024-12-31].
- [15] KOVAŘÍK, Karel. *Technické prostředky ochrany majetku a osob*. Praha: Grada, 2020. ISBN 978-80-271-1262-6.
- [16] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Komora podniků komerční bezpečnosti ČR, 2014. ISBN 978-80-260-7115-0.
- [17] *Mechanické zábranné systémy*. Online. Alsyko. C2025. Dostupné z: <https://alsyko.cz/sluzby/mechanicke-zabranne-systemy/>. [cit. 2025-05-18].
- [18] ĎURICA, Jakub, Martin BOROŠ a Vlastimil MACH. *Bezpečnostné systémy – Mechanické zábranné systémy*. EDIS, 2022. ISBN 9788055418858.
- [19] *MZS – mechanické zábranné systémy*. Online. Eluc. 2014. Dostupné z: <https://eluc.ikap.cz/lekce/mechanicke-zabezpeceni>. [cit. 2025-05-18].
- [20] LUCKI, Michal. *Moderní zabezpečovací systémy*. Online. Praha: České vysoké učení technické v Praze, 2015. Dostupné z: <https://publi.cz/books/255/Cover.html>. [cit. 2025-05-18].
- [21] *Elektromechanické a elektromotorické zámky*. Online. C2015-2025. Dostupné z: <https://www.klicovecentrum.cz/elektromechanicke-a-elektromotoricke-zamky/>. [cit. 2025-05-18].
- [22] HLADÍK, Drahošlav. *Elektronické zabezpečovací systémy a elektrická požární signalizace*. Online. 2011. Dostupné z: <https://www.souepl.cz/wp-content/uploads/2020/09/elektronick%C3%A9-zabezpe%C4%8Dovac%C3%AD-syst%C3%A9my-a-elektronick%C3%A1-po%C5%BE%C3%A1rn%C3%AD-signalizace.pdf>. [cit. 2025-05-18].
- [23] *Elektronická kontrola vstupu (EKV)*. Online. C2019. Dostupné z: <http://www.daltech.cz/elektronicka-kontrola-vstupu.html>. [cit. 2025-05-18].

- [24] *FYZICKÁ OSTRAHA*. Online. C2022. Dostupné z: <https://www.diol.cz/ostraha-majetku/fyzicka-ostraha/>. [cit. 2025-05-18].
- [25] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management V. 5*. VerBuM, 2015. ISBN 978-80-8750-067-5.
- [26] *Formy fyzické ostrahy*. Online. C2025. Dostupné z: <https://www.fyzicka-ostraha.cz/fyzicka-ostraha-formy/>. [cit. 2025-05-18].
- [27] *Analýza rizik: kvantitativní vs. kvalitativní*. Online. 2010. Dostupné z: <https://www.cleverandsmart.cz/analyza-rizik-quantitativni-vs-kvalitativni/>. [cit. 2025-05-18].
- [28] *Analýza rizik*. Online. 2022. Dostupné z: <https://www.guard7.cz/analyza-rizik/>. [cit. 2025-05-18].
- [29] *Co je matice rizik*. Online. 2025. Dostupné z: <https://aptien.com/cs/kb/articles/what-is-risk-matrix>. [cit. 2025-05-18].
- [30] *Analýza pomocí kontrolního seznamu - CLA (Checklist analysis)*. Online. 2017. Dostupné z: <https://managementmania.com/cs/analyza-kontrolni-seznam-cla-checklist-analysis>. [cit. 2025-05-18].
- [31] HRUŠKA, Jiří. *METODY ANALÝZY RIZIK*. PDF. 2014. Dostupné také z: <https://www.jh.cz/cs/mestsky-urad/krizove-rizeni/rizika-a-hrozby/>.
- [32] *Co - když analýza (What-if Analysis)*. Online. 2015. Dostupné z: <https://managementmania.com/cs/co-kdyz-analyza-what-if-analysis>. [cit. 2025-05-18].
- [33] *Metoda „What – If“ (Co se stane, když..)*. Online. 2022. Dostupné z: <https://www.guard7.cz/metoda-what-if-co-se-stane-kdyz/>. [cit. 2025-05-18].
- [34] *SWOT analýza jako základ každého projektu*. Online. C2025. Dostupné z: <https://lamael.cz/swot-analyza-jako-zaklad-kazdeho-projektu/>. [cit. 2025-05-18].
- [35] *FMEA – Vyhodnocení rizik*. Online. C2025. Dostupné z: <https://lean6sigma.cz/fmea/>. [cit. 2025-05-25].

- [36] *FTA (Fault Tree Analysis) - Analýza stromu poruchových stavů*. Online. 2015. Dostupné z: <https://managementmania.com/cs/fault-tree-analysis>. [cit. 2025-05-25].
- [37] *Jak se vyhnout chybám při provádění analýzy stromu poruchových stavů*. Online. 2022. Dostupné z: <https://www.vseoprurnyslu.cz/udrzba-a-diagnostika/asset-management/jak-se-vyhnout-chybam-pri-provadeni-analyzy-stromu-poruchovych-stavu.html>. [cit. 2025-05-25].
- [38] *ETA (Event tree analysis) - analýza stromu událostí*. Online. 2015. Dostupné z: https://managementmania.com/cs/eta-event-tree-analysis-analyza-stromu-udalosti#google_vignette. [cit. 2025-05-25].
- [39] *Analýza a hodnocení rizik s ohledem na lidský faktor: materiály z 50. semináře odborné skupiny pro spolehlivost, Praha, únor 2013 : [sborník přednášek]*. Praha: Česká společnost pro jakost, 2013. ISBN 978-80-02-02434-7.
- [40] *HAZOP (Hazard and Operability Study)*. Online. 2021. Dostupné z: <https://managementmania.com/cs/hazop-hazard-and-operability-study-analyza-ohrozeni-a-provozuschopnosti>. [cit. 2025-05-25].

SEZNAM OBRÁZKŮ

Obrázek 1 Obecné schéma analýzy rizik	16
Obrázek 2 Plánek rozložení objektu	43
Obrázek 3 Jižní komplex budov včetně provizorního parkoviště.....	44
Obrázek 4 Opravená hlavní budova v severní části	45
Obrázek 5 Automatické závory v severní části.....	46
Obrázek 6 Uzavřená střední část z důvodů probíhajících staveb.....	47
Obrázek 7 Narušení MZS z důvodů stavby v západní části areálu.....	48
Obrázek 8 Ovládací tablo ústředny EPS	50
Obrázek 9 Perimetr areálu ukončen budovami	51
Obrázek 10 KTPO umístěné v plášti objektu.....	52
Obrázek 11 OPPO včetně central a total stopu	52
Obrázek 12 Aktuálně demontovaná automatická brána z důvodu probíhajících prací.....	53
Obrázek 13 Rozšířený hlavní vjezd do areálu pro MHD a nákladní dopravu	54
Obrázek 14 Ruiny v západní části před opravou	55
Obrázek 15 Poslední budova ve střední části areálu (před rekonstrukcí)	56
Obrázek 16 Špatný stav MZS v severozápadní části	57
Obrázek 17 Betonový svah oddělující východní část a přilehlé nádraží	58
Obrázek 18 Řeka podél západní části areálu	59
Obrázek 19 Přístupový systém pro ovládání výtahů.....	61
Obrázek 20 Vypracovaná tabulka metodou FMEA	75
Obrázek 21 Plánek návrhu navýšení počtu kamer	83

SEZNAM TABULEK

Tabulka 1 Odhad hodnoty aktiv.....	65
Tabulka 2 Tabulka výskytu hrozeb.....	72
Tabulka 3 Tabulka významu hrozeb s dopadem na areál.	73
Tabulka 4 Pravděpodobnost odhalení hrozby.....	74
Tabulka 5 Přijatelnost hodnot RPN	74

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BP Bezpečnostní pracovník

KTPO Klíčový trezor požární ochrany

EPS Elektrická požární signalizace

BOZP Bezpečnost a ochrana zdraví při práci

SHZ Samostatné hasící zařízení

OPPO Obslužné pole požární ochrany

ESKV Elektronický systém kontroly vstupu

CCTV Komerové systémy

ČR Česká republika

STO Systémy technické ochrany

PČR Policie České republiky

MZS Mechanické zábranné systémy

ACCESS Přístupové systémy