Návrh komplexního bezpečnostního systému výrobní společnosti

Jiří Ševela

Bakalářská práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jiří Ševela**
Osobní číslo:	**A12543**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Návrh komplexního bezpečnostního systému výrobní společnosti**
Téma anglicky:	**A Proposal for a Complex Security System in a Production Company**

Zásady pro vypracování:

1. **Nastudujte normy vztahující se k zaměření práce.**
2. **Proveďte bezpečnostní audit ve vybrané společnosti.**
3. **Analyzujte možná rizika a hrozby.**
4. **Na základě získaných výsledků a požadavků klienta navrhněte optimální bezpečnostní systém/y.**
5. **Vytvořený návrh vhodně prezentujte.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LÁTAL, Ivo a ŠTANTEJSKÝ, Michal. Bezpečnostní zásady ochrany podniku. Prevence a řešení krizových situací. Praha: Prospektrum, 2001. ISBN 80-7175-091-3.**
2. **BRABEC, František a kolektiv. Bezpečnost pro firmu, úřad, občana. Praha: Public History, 2001. ISBN 80-86455-04-06.**
3. **RODRYČOVÁ, Danuše a STAŠA, Pavel. Bezpečnost informací jako podmínka prosperity firmy. Praha: Grada Publishing, 2000. ISBN 80-7169-144-5.**
4. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 80-7226-632-2.**
5. **LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management III. Zlín: VeRBuM, 2013. ISBN 978-80-87500-35-4.**

Vedoucí bakalářské práce: **Ing. et Ing. Kateřina Sulovská**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **6. února 2015**

Termín odevzdání bakalářské práce: **3. června 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že 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 samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně .....

podpis diplomanta

ABSTRAKT

Cílem bakalářské práce bylo navrhnout bezpečnostní systém pro výrobní společnost. Tento systém by měl splňovat nejen technické požadavky ale i požadavky zadavatele, v tomto případě vedení sledované společnosti. V první části této práce je popsána ochrana bezpečnosti podniku, co to je bezpečnostní politika podniku, rozebraná bezpečnostní analýza a typy analýz. Dále jsou rozebrány prvky a normy, které se týkají zabezpečení podniku. Druhá část je zaměřena na vytvoření návrhu komponentů k zajištění bezpečnosti. Jsou provedeny dva návrhy, ze kterých si bude moct vedení firmy vybrat, který pro společnost bude přívětivější.

Klíčová slova: Bezpečnostní systém, technická ochrana, bezpečnostní analýza, bezpečnostní politika podniku, poplachový zabezpečovací systém

ABSTRACT

The aim of the bachelor work was to design a security system for a manufacturing company. This system should comply not only technical requirements but also the requirements of the submitter, in this case leadership of the company. In the first part of this work is to describe the protection of plant safety, what is the security policy of the company, disassembled safety analysis and types of analysis. There are also analyzed the elements and standards relating to enterprise security. The second part is focused on creating the design of components to ensure safety. They are made two possibilities, from which the leadership of the company will be able to choose more appropriate choice.

Keywords: Security systems, technical protection, security analysis, security policy of the enterprise, alarm security system

Tímto bych těch poděkovat vedoucí mé bakalářské práce Ing. et Ing. Kateřině Sulovské za pomoc při zpracování, odborné rady a vedení mé bakalářské práce. Dále bych chtěl poděkovat hlavně svým rodičům, kteří mě během studia a psaní této práce podporovali. V neposlední řadě chci poděkovat vedení ENTEC-KOVO s.r.o., že mi umožnili využít jejich společnost ke zpracování této práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Tématem této bakalářské práce bude navrhnout bezpečnostní systém pro výrobní společnost. Vzhledem k současnému stavu zločinnosti a majetkové kriminalitě je obava o majetek a zájmy společnosti oprávněný. Již nestačí spoléhat jen na mechanické prvky zabezpečení jako ploty, mříže, atd., ale je potřeba tyto prvky doplnit o systém elektronický. Dohromady pak svojí kooperací dokáží vytvořit adekvátní systém zabezpečení, který odradí pachatele od případného útoku na zájmy společnosti. Vzhledem k vývoji těchto elektronických zabezpečovacích systémů je možnost velkého výběru na trhu a záleží pouze na odběrateli, od jaké společnosti si komponenty vybere.

Důvod výběru tohoto tématu je fakt, že bych se chtěl dále věnovat této problematice zabezpečování. Díky psaní této bakalářské práce a navrhnutí bezpečnostního systému pro vybranou společnost získám také potřebné zkušenosti z tohoto hlediska. Jelikož se zmíněná firma spoléhá pouze na mechanické zábranné systémy, budu se snažit implementovat k těmto prvkům i prvky elektronického zabezpečení.

V první části práce bude zaměřena na bezpečnost podniku, na bezpečnostní politiku a její vliv na fungování celé společnosti. Bezpečnostní politika vychází z faktu, že každé vedení má snahu chránit svá aktiva a zájmy, proto je třeba vypracovat bezpečnostní politiku. Dále bude v první části zmíněna fyzická a technická ochrana objektu, jejich rozdělení a zmíněny budou také krizové situace, které mohou ovlivnit chod společnosti. V této práci bude také popsána bezpečnostní analýza, uvedení základních pojmů této analýzy, zhodnocení rizik a zmínění různých typů bezpečnostních analýz. V neposlední řadě budou uvedeny prvky k zabezpečení objektu, které jsou rozděleny na mechanické zábranné systémy a elektrické a elektronické systémy.

V druhé části práce jsou vypracované dva návrhy bezpečnostních systémů. Po dohodě s vedením společnosti nebudou zveřejněny soukromé informace a nebudou zveřejněny fotografie z vnitřních prostor objektů. Návrhy jsou vytvořeny k možné pozdější realizaci. Výše rozpočtu na realizaci bezpečnostního systému nebyla přesně stanovena.

I. TEORETICKÁ ČÁST

1 OCHRANA BEZPEČNOSTI PODNIKU

1.1 Bezpečnostní politika podniku

Mezi nejvyšší priority každé společnosti patří zájem chránit svá aktiva a své zájmy. Proto by měla každá firma dbát na svoji bezpečnostní politiku. Jde o dokument, nejčastěji v písemné podobě, který pomáhá vedení řídit společnost podle daných pravidel, norem a ujednání. Mají za úkol snížení případných rizik a zvýšení bezpečnosti pomocí technologií a bezpečnostních prvků. Jedná se tedy o komplexní zabezpečení objektu firmy a jeho aktiv. [1]

Bezpečnostní politiku podniku můžeme označit jako souhrnná opatření vrcholového managementu na základní otázky, které se týkají zabezpečení, a to:

- co by měla společnost vzhledem k oblasti bezpečnosti dělat a proč,
- jakých cílů v tomto ohledu chce dosáhnout,
- jak budou řízeny činnosti podniku a jaké opatření budou provedeny, aby bylo dosaženo stanovených cílů.

Bezpečnostní politika musí být podřízena strategickému plánu organizace, protože se jedná pouze o jednu z oblastí činností podniku a nejedná se tedy o primární aktivitu firmy. Avšak bezpečnostní politiku nelze vnímat pouze jako vizi. Vize společnosti je většinou vnímána jako velmi obecná podoba. Vzhledem k tomu že bezpečnostní politika je úzce spjata se strategií podniku, může nastat ten problém, že dojde ke střetu zájmů obecné politiky podniku s bezpečnostní politikou. V případě tohoto střetu by měly být bezpečnostní cíle podřadné cílům obecné politiku podniku.

Krom výše uvedených otázek ohledně bezpečnosti podniku existují i další a to:

- kdo je odpovědný za plnění bezpečnostní politiky,
- jak bude zavedena bezpečnostní politika v praxi,
- jaké požadavky jsou kladeny na efektivitu,
- jaké budou sankce za porušení zásad a cílů bezpečnostní politiky,
- jak dlouho bude trvat naplnění cílů bezpečnostní politiky.

1.1.1 Zaměření bezpečnostní politiky

Vzhledem k tomu, že i obecná politika firmy se zaměřuje na 3 základní oblasti – zaměstnance, majetek a informace, je i bezpečnostní politika nucena řešit problémy z těchto oblastí. Jedná se o:

- personální oblast,
- organizační a administrativní oblast,
- oblast ochrany majetku,
    - politika objektové bezpečnosti – ochrana nemovitého majetku
    - politika ochrany majetku – ochrana movitého majetku
    - politika ochrany nehmotného majetku – ochrana technologických postupů a know-how, obchodních tajemství
- oblast informačních systémů. [2]

Dalším faktorem ovlivňujícím bezpečnostní politiku podniku jsou vlivy vnitřní a vnější.

Vnitřními vlivy můžeme chápat jako překážky, které vychází ze samotného podniku a ovlivňují i chod společnosti. Většinou se jedná o vlivy z hlediska ekonomického, organizačního uspořádání, personální a technickou úroveň. [2]

Vnější vlivy představují okolnosti mimo organizaci. Tyto vlivy nemůže podnik nijak ovlivnit. Jedná se o legislativní činnost státu, konkurenční prostředí, mezinárodní smlouvy atd. [2]

Bezpečnostní politika odkazuje na obecný bezpečnostní plán organizace a poukazuje na výsledný stav zabezpečení. Jedná se tedy o vytvoření plánu na dosažení určitého stavu za daný čas. Avšak v moment, kdy je splněn hlavní cíl, nepřestává bezpečnostní politika platit. Jedná se o dosažení určitého stavu a je v zájmu organizace, aby byl tento stav dodržen i v budoucnosti a bude trvalou součástí obecné politiky podniku. Lze tedy bezpečnostní politiku brát i jako dlouhodobý a nekonečný proces, který chrání zájmy a aktiva firmy. [2]

Úkolem bezpečnostní politiky je dosažení předem daných vytyčených cílů, které chce společnost splnit. Jedním z důležitých faktorů je seznámení všech zaměstnanců s touto vizí pro zvýšení jejich efektivity během práce. Zaměstnanci by také měli dodržet veškeré závazky, které mají vůči podniku.

1.1.2 Typy bezpečnostní politiky

- **Promiskuitní**

Neomezující, pracovníci vykonávají činnosti, aniž by měli dostatečnou kvalifikaci

- **Liberální**

Přístup volnější, umožňuje pracovníkům vykonávat vše až na věci explicitně zakázané

- **Racionální**

Zakazuje dělat vše, co není explicitně povoleno.

- **Paranoidní**

Zakazuje dělat vše, co by mohlo být potenciálně nebezpečné [3]

1.2 Ochrana majetku a osob

Ochrana bezpečnosti firem a podniků v současné době často řešené téma. Zabezpečení podniku by se mělo řešit jako komplexní ochrana movitého, nemovitého majetku a z hlediska bezpečnosti informací. Jako ochranu bezpečnosti objektu by se tedy nemělo vnímat pouze jako zajištění obvodové ochrany ale jako systém tvořen subsystémy.

Předmětem zájmu bezpečnosti je vnímáno jako:

- Ochrana osob
- Ochrana hmotného majetku
- Ochrana nehmotného majetku

Osobami jsou myšleni stálí zaměstnanci podniku, externí zaměstnanci a osoby, které se v danou chvíli na pozemku podniku vyskytují.

Pod hmotným majetkem si můžeme představit veškeré prvky movité i nemovité. Ochrana těchto prvků jsou základem dobré prosperity firmy, protože na nich záleží finanční struktura společnosti. Škody na movitých i nemovitých prvcích majetku jsou škody, které uškodí firmě nejen z finančního hlediska, ale může mít i dopad na efektivitu práce a vykonávání jiných činností. Můžeme tedy říct, že na ochraně hmotného majetku je firma přímo závislá.

Nehmotným majetkem ve firmě je soubor veškerých informací a dat. V dnešní době, kdy je většina dat zpracovávána v elektronické podobě a ukládána na datová úložiště, musí společnosti dbát na ochranu těchto prvků. Existuje možnost útoků na tyto citlivá data, ať už se jedná o technologické postupy, know-how nebo i obchodní tajemství. Útočníci již nemusí získávat data fyzicky, ale díky neoprávněnému přístupu po síti se mohou dostat k citlivým informacím na datovém úložišti. Lze tedy tvrdit, že ochrana informací patří k nejsložitějším procesům komplexního zabezpečení společnosti. [2]

V konečném důsledku každý útok nebo jakákoliv ztráta hmotného či nehmotného majetku je pro firmu vždy ztráta, která je vyčíslitelná penězi.

Jelikož útoky směřují na majetek a činnost podniku je třeba, aby vedení společnosti bylo obeznámeno s možnými typy útoků a znali potenciální hrozby a rizika. Druhy, které mohou ohrozit podnik, lze označit jako potenciální krizové situace.

- Živelné pohromy (povodeň, požár, zemětřesení),
- selhání lidského faktoru
    - úmyslné (špionáž, sabotáž, útok na síť)
    - neúmyslné
    - zaviněné (nedodržení pracovních norem a postupů)
    - nezaviněné (vina poruchy stroje, vada materiálu, atd.) [2]

1.3 Režimová ochrana

Jedná se o soubor pravidel, opatření, norem, zákazů a předpisů, které stanovuje vlastník firmy nebo objektu. Podstatou těchto pravidel je stanovit určitý řád způsobu použití bezpečnostních opatření a zajistit součinnost těchto opatření s uživateli objektu, technickou a fyzickou ochranou. Povinnost zavedení režimových opatření není pro každý podnik nutná. Záleží na odvětví podnikání, ve kterém se daná společnost pracuje (jaderná energetika, apod.). Režimová ochrana vychází z bezpečnostní politiky podniku a také z analýzy bezpečnostních hrozeb a rizik. [4]

Režimová opatření se týkají:

- vlastních zaměstnanců podniku a jejich činnosti,

- pohyb a chování osob, které nejsou zaměstnanci podniku, ale nachází se v danou chvíli na pozemku podniku,
- zpracování interních informací, dat a dokumentů společnosti [2]

1.4 Fyzická a technická ochrana objektu

Mezi hlavní úkoly podniku, z hlediska zabezpečení objektu, patří obvodová ochrana. Základem je fyzická ochrana, která je doplněna o technické prostředky k ochraně (mechanické, elektronické). Primárním úkolem těchto prvků ochrany není v odhalování protiprávních jednání, nýbrž slouží jako preventivní opatření proti tomuto jednání. Cílem implementace těchto bezpečnostních prvků je zcela eliminovat možnost odcizeni, poškození či zneužití majetku firmy a také riziko napadení zaměstnanců a dalších osob, které se v danou chvíli nachází na pozemku firmy. Ochranu podniku a zájmů dále dělíme na vnější a vnitřní. Ochrana vnější je zaměřena na bezpečnost majetku a osob v objektech podniku pomocí fyzické ochrany nebo implementací systému technické ochrany. [5]

Vnější ochranu dělíme na:

- **Plášťovou –** Plášťová ochrana je realizována pomocí prvků poplachových zabezpečovacích a tísňových systémů (PZTS).
- **Obvodovou** – Obvod celého objektu podniku charakterizuje administrativní hranice. Základem obvodové ochrany je oplocení objektu, což ukazuje na ohraničení pozemku firmy. Tento prvek však pachatele nezastaví, pouze zpomalí. Je třeba přidat další prvky fyzické ochrany nebo prvky PZTS. Důležitým aspektem obvodové ochrany je i dobré osvětlení.
- **Prostorovou –** Ochrana prostorová je specifická pro celý prostor objektu. Je realizována fyzickou ochranou a technickými prostředky, zejména CCTV (Closed Circuit Television, uzavřený televizní okruh),

- **Předmětovou** – Touto ochranou je myšleno především ochranou samostatných předmětů v objektu podniku. Většinou se jedná o skrytý způsob ochrany a cílem je detekovat narušení a manipulaci se střeženým předmětem. [5]

1.5 Druhy krizových situací

Z výše uvedených příkladů rizik a hrozeb, které mohou dopadat na společnost, vznikají krizové situace. Tyto situace můžeme rozdělit podle vzniklých příčin.

Působení vyšší moci – do této skupiny patří jevy jako přírodní katastrofy, povodně, zemětřesení

Havárie techniky – tyto skutečnosti, jejichž příčina se může lišit, mají pokaždé vliv na celý podnik. Můžeme sem zařadit:

- *„Kontaminace území objektu toxickými látkami,*
- *Dopravní havárie a katastrofy, které ovlivnili technologický proces podniku*
- *Zničení objektů kvůli porušení stability*
- *Poškození komunikací, strojů, výrobního zařízení a inženýrských sítí*
- *Poruchy způsobené přerušením dodávek energie, působením magnetických si polí, vibrací“ [2]*

Sociální krize – Tato situace nastává v nedodržování či neznalosti právních a organizačních norem, nevhodnému vedení a chování se k zaměstnancům. Tyto faktory následně vedou k situacím nespokojenosti zaměstnanců, stávkám, porušováním pracovních povinností, ztráty dobré pověsti vzhledem k dodavatelům i odběratelům a celkovému snížení kreditu firmy. Všechny tyto vlivy a situace vedou k ovlivnění činnosti firmy. [2]

Zdravotní krizové jevy – Vznik epidemie a šíření různých virů, který má dopad na zaměstnance, anebo jiné vnější subjekty důležité pro chod podniku.

Válečné události – Zde se jedná o krizi způsobenou ozbrojenými konflikty. [2]

Všechny tyto krizové situace, které mohou dopadat na podnik, ovlivňují celkový chod firmy. Tyto aspekty by měly být zhodnoceny a řešeny v bezpečnostní politice podniku. Proto by měla mít firma zpracovaný krizový plán pro různé případy mimořádných událostí. Základem je však prevence, jak by se měla společnost takových situacím vyhnout. Důležité je si stanovit skutečnost realizace ochrany s ohledem na možnost vyskytnutí dané situace. Lze zohlednit například dopravní infrastrukturu, geografické umístění podniku a jeho okolí, atd.

2 BEZPEČNOSTNÍ ANALÝZA

Je to proces, který slouží managementu společnosti k hledání nedostatků v bezpečnosti. Jde o postupné rozdělení firmy jako celku na dílčí části a následnému zkoumání těchto částí a zkoumání jednotlivých vztahů mezi nimi. Je důležité dbát při analýze na tyto jednotlivé části a hlavně vztahy mezi nimi. Při bezpečnostní analýze jednotlivých části lze přehlédnout problémy, které na první pohled nejsou znatelné. Jde o mechanismy a zákonitosti, které jsou vzájemně propojeny a pro chod firmy důležité. Pro odhalení těchto vazeb je používána syntéza. Analýza a syntéza jsou úzce spjaty. Syntéza je proces, který je opačný analýze a slouží nám ke zpětnému dosazení jednotlivých části do celku kvůli zmiňovanému pochopení vazeb mezi dílčími částmi. [2]

Bezpečnostní analýza tedy zkoumá veškeré předměty, jevy a informace a další podněty, které se jakkoli dotýkají bezpečnosti podniku. Cílem bezpečnostní analýzy je identifikovat co největší počet nedostatků a zranitelných míst v objektu, odhaleni hrozeb a rizik. Dále určit stávající efektivitu současných bezpečnostních zařízení a vytvořit návrh změn, případně nových prvků zabezpečení. To vše pro snížení rizik na minimum.

Při vykonávání bezpečnostní analýzy by měl být management podniku obeznámen těmito otázkami:

- Proč je analýza vykonávána?
- Kdy by měla být vykonána?
- Co je předmětem analýzy?

Analýza je vykonávána k minimalizaci a zamezení ztrát, které mají dopad na podnik. Je vykonávána v době, kdy je možnost, že se nebezpečí mění v hrozbu. Předmětem analýzy jsou lidské zdroje, procesy, stav současného stavu bezpečnosti a majetek. [1]

2.1 Základní pojmy

Před tím než se začne cokoli analyzovat, je třeba definovat základní pojmy, které obsahuje téměř každá analýza. Každá z analýz nám pomáhá zhodnotit dva cíle:

- čím je v analyzovaném případě specifikováno riziko,
- jak riziko kvantifikovat

- **Aktivum** - každá entita, která pro firmu má nějakou hodnotu. Tyto aktiva lze rozdělit na hmotná a nehmotná. Avšak jakákoliv hrozba na aktiva nám jejich hodnotu snižují. Za hmotná aktiva považujeme např. cenné papíry, elektroniku, materiál potřebný k výrobě, atd. Za nehmotná aktiva pak považujeme know-how výrobních procesů a také morálku zaměstnanců. Za aktivum lze považovat firmu jako celek. Velká hodnota aktiva se může stát terčem případných útočníků, které tato velká hodnota motivuje. [6]
- **Riziko –** jedná se o pravděpodobnost vzniku negativních situací dopadající na firmu. Rozlišujeme na kvantitativní a kvalitativní, což vyjadřuje stupeň nebo míru ohrožení. [6]
- **Hrozba –** představuje událost, aktivitu nebo osobu, která má přímý vliv na vznik škody. Jako příklad lze uvést přírodní katastrofy, požáry, povodně nebo krádež majetku či získání přístupu k citlivým informacím. [6]
- **Zranitelnost –** Určuje míru nedokonalosti aktiva. Čím vyšší je tato hodnota, tím vyšší pravděpodobnost, že se aktivum stane předmětem poškození nebo odcizení. Zranitelnost tedy parametr aktiva, na které působí hrozba. Hodnota zranitelnosti se hodnotí citlivostí a kritičností. Citlivost vyjadřuje možnost poškození aktiva danou hrozbou a kritičnost vyjadřuje, jak je pro podnik dané aktivum důležité. [6]
- **Protiopatření** - Vyjadřuje nám postupy, procesy nebo prostředky, které vedou ke snížení zranitelnosti nebo k naprosté eliminaci hrozby. Cílem je vytvořit preventivní opatření, které zabrání vzniku případných škod na majetku podniku. To je potom charakterizováno parametry, jak je toto opatření efektivní a jak bude nákladné. [6]

2.2 Obsah bezpečnostní analýzy

Bezpečnostní analýza by měla obsahovat následující body.

- **Cíl bezpečnostní analýzy a způsob provedení:**
  - z jakého důvodu je bezpečnostní analýza prováděna,
  - jakým způsobem bude provedena. Jestli bude provedena vlastníky podniku, nebo zda bude vykonána nezávislým expertem mimo firmu,
  - zda bude zpracována jako dílčí nebo jako komplexní analýza.

- **Vypracování postupů a zásad:**
  - na bezpečnost majetku a osob,
  - bezpečnost obecných zájmů podniku,
  - bezpečnost konkrétních zájmů podniku.
- **Sběr informací:**
  - od managementu firmy,
  - od zaměstnanců firmy,
  - zvenčí firmy
  - posouzením experta, který vykonává analýzu.
- **Třídění získaných informací**

  Vychází z:

  - Vypracovaných postupů a zásad
  - Sběru informací
- **Analýza a rozbor vytříděných informací:**
  - z hlediska kritérií na ochranu bezpečnostních zájmů podniku
  - rizik, které je třeba považovat za hrozící nebezpečí pro podnik
  - současného stavu [5]

2.3 Zhodnocení rizik

„Pro zhodnocení rizik se jeví vhodné zpracovat tzv. matrici nebezpečí útoků, a to jak zevně, tak zevnitř objektu. V matrici je vhodné ve svislé posloupnosti vymezit:

- *Objekty*
- *Prostory*
- *Zařízení*
- *Jiné možné objekty (např. know how) možného ohrožení či napadení, přičemž je třeba zvlášť zvýraznit nebezpečné provozy apod.*

Dále ve vodorovné posloupnosti je vhodné v matrici rizik uvést možná rizika, jako např:

- *všeobecné krádeže,*
- *krádeže vloupáním,*
- *napadení osob,*
- *vandalismus,*
- *žhářství,*

- *možná samovznícení,*
- *teroristické útoky,*
- *provozní havárie,*
- *možnosti výbuchu,*
- *možností sabotáže vyvolané konkurencí či nespokojeným pracovníkem,*
- *možnosti živelných pohrom,*
- *ohrožení provozního, výrobního či obchodního tajemství,*
- *ohrožení databází počítačů,*
- *Jiná ohrožení a útoky.“[5]*

2.4 Typy analýz

Pro vytvoření postupů a technik nebyla nijak dána žádná definice či platné normy. Proto lze využít metody a techniky z jiných oblastí, zejména z ekonomiky a financí. Jelikož vrcholový management podniku využívá techniky v tomto oboru, lze je využít i v oblasti bezpečnosti. Mezi tyto techniky se pro provedení bezpečnostní analýzy se řadí:

- analýza SWOT,
- analýza PEST,
- What If
- PHA
- FTA
- HAZOP
- HRA

2.4.1 Analýza SWOT

Tento typ analýzy je využíván řadou organizací pro zjištění silných a slabých stránek firmy a pro zjištění příležitostí a hrozeb. Jak už vypovídá z názvu analýzy, zkratka SWOT je tvořena prvními písmeny anglických slov Strengths (silné stránky), weaknesses (slabé stránky), Opportunities (příležitosti), Threats (hrozby). Obsah těchto skupin nám říka, co je předmětem analýzy. SWOT analýza vychází z toho, že firma dosáhne strategického úspěchu rozvíjením silných stránek a minimalizací slabých stránek a hrozeb. V případě, že je tento typ analýzy uplatněn ve smyslu bezpečnosti podniku, nebude jejím předmětem firma jako celek, ale stav její bezpečnosti. [7]

Z pohledu této analytické metody lze považovat za silné stránky podniku vnitřní podmínky, které představuje např. dobře propracovaná organizační struktura organizace, přesné rozdělení kompetencí a pravomocí mezi řídící pracovníky, odborná kvalifikace zaměstnanců v oblasti bezpečnosti, dobré finanční zázemí podniku.

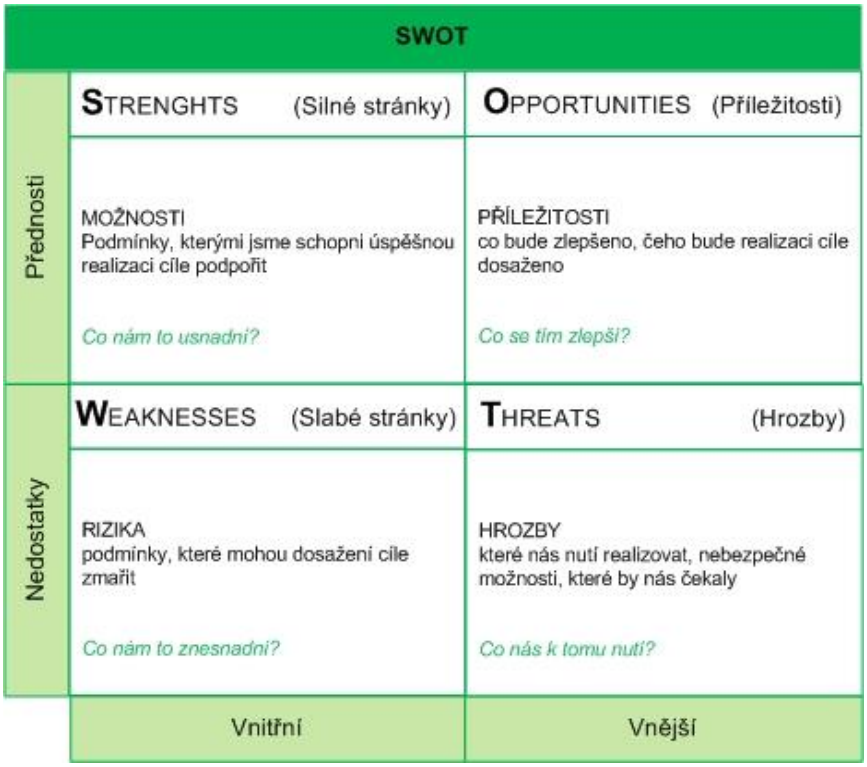
Za nedostatky v organizaci můžeme považovat nepříznivé vnitřní podmínky v podniku, které mají negativní dopad na bezpečnost celé firmy. Mezi nedostatky lze zařadit nedostatečně rozvinutou a definovanou organizační strukturu, špatnou ekonomickou a finanční situaci, nedostatek nebo úplná absence kvalifikovaných zaměstnanců v oblasti zabezpečení, špatná nebo žádná technika pro zabezpečení podniku. [2]

Příležitosti jsou definovány jako vnitřní podmínky, které mají příznivý dopad na postavení společnosti jak v současnosti, tak i v budoucnu. Pokud tyto příležitosti zasahují, nebo v budoucnu budou zasahovat, negativně, ovlivní to i stav bezpečnostního systému podniku. Především se bude jednat o příležitosti, které v první řadě příznivě ovlivní budoucnost firmy jako celku, teprve poté ovlivní i její bezpečnostní systém. Mezi takové příležitosti lze zahrnout i dlouhodobé snížení cen v oblasti zabezpečovací techniky a služeb. [2]

Hrozby představují současné i budoucí negativní vlivy ve vnějším prostředí, které mají negativní dopad na stav zabezpečení podniku. Může se jednat o hrozby, které mají dopad na společnost jako celek a dopad na zabezpečení by byl až druhořadý, ale může to být i přímý dopad na stav zabezpečení. Jako obecnou hrozbu, která má přímý dopad na společnost jako celek, lze považovat ztráty zakázek. Tyto ztráty budou mít negativní dopad na finanční stránku podniku. Jako negativní vliv lze považovat i kvalitativní a kvantitativní zaostání za zabezpečením konkurence. [2]

Mezi všemi těmito aspekty, tedy přednostmi, nedostatky, příležitostmi a hrozbami, lze najít takové podmínky, které ovlivňují stav a úroveň zabezpečení podniku. Některé z těchto aspektů vyžadují rychlou změnu v zabezpečení společnosti, avšak jiné změny jsou spíše směřovány do budoucnosti.

I když hovoříme pouze o jedné analýze, provádíme čtyři analýzy. Pro přehlednost je výsledek analýzy rozdělen do grafické podoby na 4 kvadranty.



Obrázek 1 – Analýza SWOT [8]

Výhoda analýzy SWOT spočívá ve schopnosti ohodnotit stávající i budoucí stav, což napomáhá managementu v rozhodování o nejvhodnějších a nejúčinnějších opatřeních. Velkou měrou zlepšuje fungování systému organizace, jelikož zaměstnanci jsou schopni správně poznat a pochopit význam vnitřních nedostatků a vnějších hrozeb. Analýza by měla být prováděna pravidelně, a to kvůli aktualizaci dat. Lze díky tomu předcházet změnám ve vnitřních a vnějších podmínek, zejména změnám zabezpečení podniku. [2]

2.4.2 Analýza PEST

Název analýzy PEST je tvořen začátečními písmeny odvětví, které charakterizují předměty této analýzy. Jedná se o politiku, ekonomiku, sociální oblast a technologii. Při provedení analýzy těchto oblastí se do rukou managementu dostávají informace o okolním prostředí a informace ohledně budoucích trendů. Při použití tohoto typu analýzy je třeba dbát na výběr informací z těchto čtyř odvětví, které se budou dotýkat oblasti zabezpečení společnosti. V oblasti politiky management sleduje vývoj mezinárodních smluv, jestli kvůli nim nedojde ke změně právních předpisů a norem, které by měli za následek změnu opatření v zabezpečení podniku. [2]

Jelikož je společnost ekonomický subjekt, je jedním z odvětví, kterým se zabývá analýza PEST, i ekonomika. Na ekonomice a finanční jistotě je postavena celá firma, tím pádem každá negativní ekonomická situace ovlivní podnik značným způsobem. Avšak může se jednat i o negativní vliv na zabezpečení přímo, ne na firmu jak celek. Jedná se např. o zvýšení cen zabezpečovacích služeb, což má za vliv na ekonomiku provozu bezpečnostního systému celé společnosti. [2]

Další z oblastí je tzv. sociální oblast. Jedná se o problém např. s nezaměstnaností. Z toho vyplývá růst nezaměstnanosti a možnost zvýšení kriminality a možným škodám na majetku společnosti. Naopak zvýšení nezaměstnanosti může mít pozitivní dopad na podnik a to takový, že bude mít větší možnost přijmout další zaměstnance a zvýšit produktivitu. Z pohledu bezpečnosti je první možnost úzce spjata s druhou. Podnik může najmout kvalifikované pracovníky jako fyzickou ostrahu a zvýšit tím ochranu firmy. [2]

V technologické oblasti vedení podniku hlavně zajímá technologický vývoj, který může zlepšit produktivitu práce, a také, z hlediska bezpečnosti, zajistit vyšší ochranu podniku. V oblasti IT (informační technologie) má zdokonalování a vývoj nových technologií zásadní význam pro zabezpečení počítačových sítí v organizaci. Organizace musí řešit náhradu staré techniky novou, což ji nutí i požadavky na bezpečnost v IT. Dále se jedná i o technologický vývoj zabezpečovacích technologií jako je třeba kamerový systém, apod. [2]

2.4.3 What If

Tato metoda je založena na brainstormingu, kdy se posuzují havarijní situace, které vyplynou z otázek typu: „Co se stane když?“. Na těchto poradách celý tým probírá případné situace a hledá správné řešení. Výhodou této metody je malá časová náročnost. Nevýhodou je však, že tato metoda analýzy je přímo závislá na zkušenosti týmu a postrádá určitou uspořádanost. [6]

2.4.4 Předběžná analýza ohrožení (PHA)

Tato metoda analýzy je využívána při návrhu projektu zařízení, ale lze ji využít na již současné zařízení. Slouží k zjištění ohrožení před samotnou realizací projektu a tím snížit případné pozdější náklady na změny. Výhodou je včasné příprava na možné druhy nebezpečí a zvládnutí bezpečnosti. [6]

2.4.5 Analýza stromem poruch (FTA)

Jedná se o metodu, která vyhodnocuje jednotlivé příčiny havárií a zkoumá jejich příčiny. Jde o grafický model poruch zařízení a lidských chyb, ze kterých se může stát vrcholová událost. Tato metoda je založena na Booleovské algebry. Konečným výstupem analýzy jsou typy poruch a pravděpodobnost poruch systémů, pokud je známa pravděpodobnost příčiny. [6]

2.4.6 HAZOP

Metoda HAZOP (Hazard and Operability Study) je analýzou, která slouží k identifikaci ohrožení a provozuschopnosti. Je založena na posouzení pravděpodobnosti ohrožení a následných rizik. Je využívána v průběhu realizace projektu avšak i po dokončení. Během analýzy se odhalují kritická místa v projektu, odchylky a nedostatky, které vedou k nežádoucím následkům. [6]

2.4.7 Analýza lidské spolehlivosti (HRA)

Metoda HRA (Human Reliability Analysis) slouží k hodnocení různých faktorů pracovní činnosti, které mají dopad na všechny zaměstnance podniku. Cíl této metody je zjistit veškeré potenciální chyby, z čeho tyto chyby vyplívají a následky. Metoda je spojována a využívána i s výše zmíněnou metodou FTA a výsledky jsou v podobě stromu chyb. Většinou ji provádí jeden nebo dva analytici ve formě rozhovorů. Avšak tato technika je časově náročná a vyžaduje zkušené analytiky. [6]

3 PRVKY K ZABEZPEČENÍ OBJEKTU

Jak již bylo v práci řečeno, prioritou každého managementu je snaha chránit veškerý svůj majetek a zájmy společnosti. Je tím myšleno jak aktivum firmy, jako jsou výrobní stroje, materiál potřebný k provozu a výrobě, tak i bezpečnost zaměstnanců, informace, firemní know how, atd. V této kapitole bude naznačeno, které technické prostředky mohou být použity.

Jako nejjednodušší dělení technických prostředků k zabezpečení je třídění podle technického postupu výroby. Podle toho rozeznáváme 2 skupiny a to:

- Mechanické zábranné systémy
- elektrické a elektronické systémy. [2]

3.1 Mechanické zábranné systémy

Mechanické zábranné systémy (dále jen MZS) jsou základním prvkem v oblasti zabezpečení objektů. Úkolem MZS je co nejvíce ztížit útočníkovi přístup do chráněných prostor, případně zabránění manipulace s citlivými materiály a dokumenty. MZS tedy poskytují ochranou svojí mechanickou pevností. Na každý prvek MZS, který je překonáván, je třeba vynaložit určité úsilí a čas pro jeho zdolání. Tím mohou odradit pachatele od případného činu úplně. [9]

3.1.1 Mříže

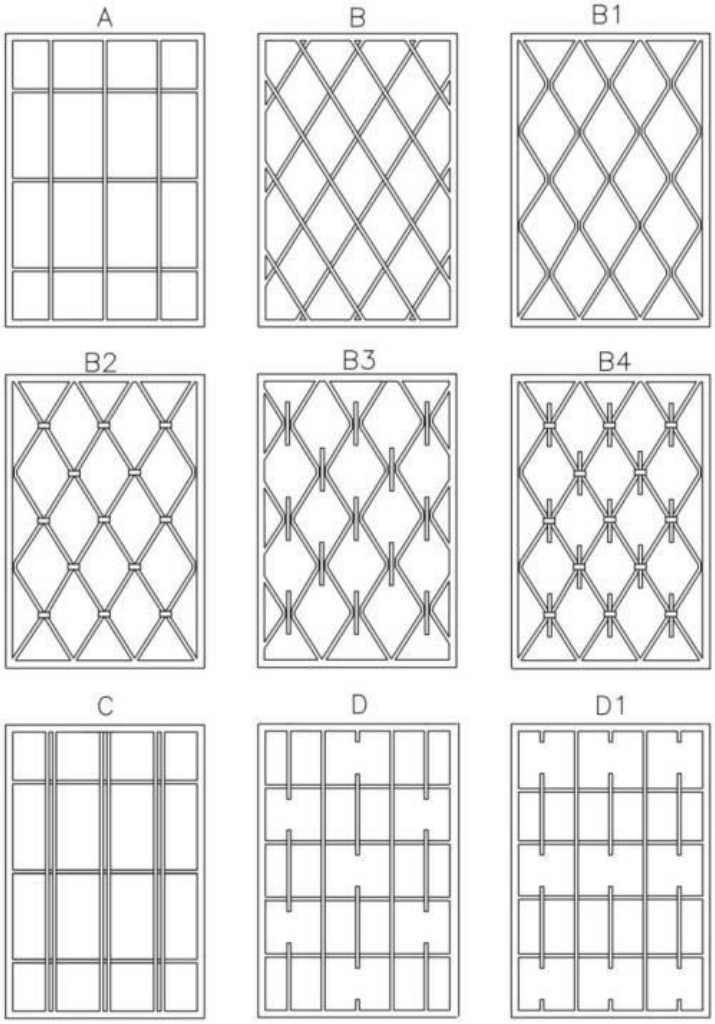
Jedná se o jeden z nejstarších a nejúčinnějších bezpečnostních prvku z pohledu ochrany prosklených výplní. Jde o prvek plášťové ochrany, jehož hlavními přednostmi jsou odolnost, ukotvení ok a nerozebratelná konstrukce. Pevnost a jistotu ochrany mříží zajištují tyto faktory. Konstrukce však nesmí být narušitelná a musí být stabilní. Mříže se nesmí dát roztáhnout, vzdálenost tyčí zaručuje, že se pachatel nedostane skrz. Přestože jsou skleněné výplně nejčastějším překonávaným místem při vloupání, jsou mříže nejúčinnějším prvkem ochrany těchto míst. Při pojištění objektu jsou přesně dány požadavky pojišťoven, které musí mříže splňovat. [9]

Znění všeobecných smluvních podmínek České Pojišťovny a.s. k lednu 2015 je:

„Funkční mříží se rozumí mříž, která splňuje požadavky příslušné normy minimálně v bezpečnostní třídě 2, nebo taková mříž, jejíž ocelové prvky (pruty) jsou z plného materiálu o průřezu minimálně 1 cm2. Velikost ok musí být maximálně 250 x 150 mm.

Mříž musí být dostatečně tuhá (např. svařenec) a musí být z vnější strany pevně, nerozebíratelným způsobem, ukotvena (zazděna, zabetonována, připevněna apod.) nebo uzamčena bezpečnostními visacími zámky v závislosti na velikosti mříže, minimálně však ve čtyřech bodech (kotveních). Za funkční mříž se též považuje mříž vyrobená z jiné- ho materiálu a jinou technologií, která však vykazuje minimálně stejnou mechanickou odolnost proti krádeži vloupáním jako mříž výše definovaná v tomto bodě. Mříž lze z venkovní (vnější) strany demontovat nebo odstranit pouze hrubým násilím (kladivem, sekáčem, pilkou na železo apod.).“[10]

Dle konstrukce rozdělujeme mříže na uchycené, odnímatelné, navíjecí a otevírací. Další dělení je podle způsobu montáže, tedy vnitřní a vnější. Materiálem, ze kterého jsou zhotoveny, bývá zpravidla ocel, ale je využíván i tvrzený a šlechtěný hliník. Mříže jsou vyráběny dle požadavků zákazníka, ozdobné, aby nenarušovali esteticky objekt, na kterém budou instalovány. [2]



Obrázek 2 – Příklad typů mříží [11]

3.1.2 Zámky a bezpečnostní uzamykací systémy

Zámky a uzamykací systémy jsou jedním z nejstarších technických prvků. I když se v podstatě jedná o mechanické zařízení, vývoj zámků v poslední době velkou měrou ovlivnila elektronika. Revoluční zlom přinesl zámek s cylindrickou vložkou, který byl svou konstrukcí velmi jednoduchý. Z počátku byla cylindrická vložka tvořena drážkou na klíč a pět kolmých otvorů na stavítka. Postupem času se tento prvek zámkového systému vyvíjel a cylindrická vložka obsahuje různé boční otvory na boční stavítka, prvky proti odvrtání zámku a další bezpečnostní prvky. Je samozřejmostí, že pro použití prvků MZS je třeba používat výrobky, které mají prohlášení o shodě, tedy prošly testováním a certifikací. K zabezpečení objektů jsou využívány i visací zámky, které se dle klíče rozdělují na zámky s otočným klíčem, zásuvným klíčem, se svorníkem a s třmenem. Další dělení zámků dle typu jsou dozické, motýlkové a kódované. [2]

3.1.3 Závory

Mechanický zabraný prostředek, sloužící k zajištění vjezdu do objektu. Konstrukce závory je tvořena různými materiály, ale většinou bývá kovová. Cílem je zabránit nepovoleným vozidlům vjezd do areálu objektu, či zabránění výjezdu z něj. Závory mohou být ovládány dálkovým ovládáním, samostatnou obsluhou či jinými technickými a elektronickými systémy. [2]

3.1.4 Rolety

Prvek MZS, který stejně jako mříže, sloužící k ochraně skleněných výplní, avšak není tak účinný jako zmiňované mříže. K navíjení rolet je využíván buď pohon ruční, nebo elektrický. Dále dělíme rolety dle jejich umístění na vnitřní, vnější a garážové. Materiálem, ze kterého jsou rolety tvořeny, je nejčastěji hliník, ocel nebo plast. Vzhledem k použitému materiálu je nutno podotknout, že plastové provedení rolet nemá takový bezpečnostní účinek jako předešlé dva materiály. Pokud lze roleta uzamknout, musí splňovat i tento uzamykací systém jisté bezpečnostní požadavky. [9]

3.1.5 Úschovné objekty

Úschovnými objekty rozumíme trezory, komorové trezory, trezorové skříně a depozitní systémy. Podle způsobu jejich umístění je rozdělujeme na trezory, které jsou pevně spojeny s objektem, nebo jsou přenosné. S postupem času roste vývoj úschovných objektů a zdokonaluje se jejich odolnost proti průniku. Důležitým parametrem

úschovných objektů je jejich bezpečnostní třída. Tato třída udává, jak je trezor bezpečný a jak dlouho by měl vydržet útok případného útočníka. Všechny tyto bezpečnostní třídy nám určuje evropská norma ČSN EN 1143-1. Trezory jsou testovány a výsledky těchto zkoušek jsou rozhodujícím faktorem pro klasifikaci do dané bezpečnostní třídy. [12]

3.1.6 Ploty

Ploty se rozumí mechanický zábranný prvek obvodové ochrany areálu podniku, jehož cílem je zastavení pachatele proniknout na pozemek. Tento systém ochrany je nepřetržitě vystavován venkovním vlivům a musí tedy splňovat určité parametry odolnosti, např. odolnost proti povětrnostním podmínkám. Z hlediska umístění plotového systému je třeba dbát na určité parametry. Jedná se o objekty, které se nacházejí blízko plotu, jako třeba stromy, které svojí výškou přesahují výšku plotu, a které mohou být určitým nástrojem pro překonání, atd. Ploty rozdělujeme dle použitého materiálu a bezpečnostních požadavků:

- živé ploty,
- umělé ploty

Živé ploty se vysazují zejména trnité a nepropustné, aby odradily případné pachatele. Umělé ploty se liší od použitého materiálu k realizaci a máme jako zděné, dřevěné, kovové a z umělé hmoty. V současnosti je však nejrozšířenější použití drátěného oplocení. [2,9]

3.2 Elektrické a elektronické systémy

Technologický vývoj způsobil velkou měrou přínos elektrických a elektronických systému do oblasti zabezpečení objektů. Již se není třeba spoléhat pouze na MZS, ale tyto prvky jsou doplněny elektronickými systémy, které jsou mnohem častěji podniky využívány. I přes neustálý vývoj těchto systémů je zastavovací účinek pachatelů minimální. Tyto zabezpečovací systémy plní roli spíše signalizační. Jde o např. zvukový, obrazový nebo světelný signál, či přenos informace na dohledové poplachové přijímací centrum (dále jen DPPC). Lze tedy říct, že poplachové systémy zvyšují efektivitu celkové ochrany v kombinaci s prvky MZS.

3.2.1 Dohledové poplachové příjímací centrum

DPPC, dříve označováno jako pulty centralizované ochrany (PCO), je důležitou součástí celého systému PZTS i CCTV. DPPC jsou technická zařízení, která slouží k příjmu, vyhodnocení, signalizaci informace o narušeném prostoru, který je střežen. Podstatou DPPC je možnost střežit vzdálený objekt tak, že při vzniku poplachové situace je vyslán právě na DPPC signál o narušení. Obsluha DPPC poté vyšle výjezdovou skupinu, která zajistí střežený objekt. DPPC pracuje nepřetržitě a zpracovává signály z CCTV, EPS, PZTS a přístupových systémů. [13]

Pro přenos zpráv mezi prvky zabezpečení v objektu a DPPC jsou využívány různé typy komunikace. Jde o telefonní síť, rádiovou síť nebo síť GSM (Globální Systém pro Mobilní komunikaci). Z ústředen v objektu se na DPPC dostávají informace o:

- narušení zóny,
- opětovná aktivace zóny do střežení,
- výpadek napájení systému nebo subsystému,
- porucha baterie
- narušení ochranných smyček
- porucha sirény
- test komunikace. [14]

3.2.2 Poplachové zabezpečovací a tísňové systémy

Funkcí PZTS je detekce a signalizace pokusu o narušení nebo již přítomnost pachatele v chráněné zóně. Dříve byly tyto systémy označovány jako elektronický zabezpečovací signalizace (EZS). Jedná se o skupinu detektorů, ústředen, tísňových hlásičů, poplachové signalizace a dalších zařízení díky nim je signalizováno narušení střeženého objektu. Všechny tyto prvky mají daná funkce a dohromady tvoří ucelený soubor zabezpečení. Každé PZTS je musí mít stanoven:

- stupeň zabezpečení,
- třídu prostředí [15]

Jsou dány čtyři stupně zabezpečení a jsou dány normou ČSN EN 50131-1.

- *„Stupeň 1. – Nízké riziko (NR) – Předpokládá se, že narušitelé mají malou znalost EZS a že mají k dispozici omezený sortiment snadno dostupných nástrojů.*
- *Stupeň 2. – Nízké až střední riziko (NR/SR) – Předpokládá se, že narušitelé mají určité znalosti o EZS a že použijí základní sortiment nástrojů a přenosných elektronických přístrojů.*
- *Stupeň 3. – Střední až vysoké riziko (SR/VR) – Předpokládá se, že narušitelé jsou obeznámeni s EZS a že mají úplný sortiment nástrojů a přenosných elektronických přístrojů.*
- *Stupeň 4. – Vysoké riziko (VR) – Předpokládá se, že narušitelé mají podrobné informace pro zpracování podrobného plánu vniknutí a dále že mají kompletní zařízení a prostředky umožňující nahradit rozhodující prvky EZS“ [13]*

Stejně jako stupně zabezpečení jsou je i klasifikace prostředí rozdělena do čtyř tříd dle normy ČSN en 50131-1:

- *„Třída I: Prostředí vnitřní – Komponenty EZS musí správně pracovat při působení vlivů prostředí, které se vyskytuje ve vytápěných místnostech. Předpokládají se změny teplot v rozmezí +5°C až + 40°C při střední relativní vlhkosti okolo 75% bez kondenzace.*
- *Třída II: Prostředí vnitřní všeobecné – Komponenty EZS musí správně pracovat při působení vlivů prostředí, kde není udržována stálá teplota. Předpokládají se změny teplot v rozmezí -10°C až + 40°C při střední relativní vlhkosti okolo 75% bez kondenzace.*
- *Třída III: Prostředí venkovní chráněné - Komponenty EZS musí správně pracovat při působení vlivů prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty EZS nejsou vystaveny plně vlivům počasí. Předpokládají se změny teplot v rozmezí -25°C až + 50°C při střední relativní vlhkosti okolo 75% bez kondenzace.*
- *Třída IV: Prostředí venkovní všeobecné - Komponenty EZS musí správně pracovat při působení vlivů prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty EZS jsou vystaveny plně vlivům počasí. Předpokládají se změny teplot v rozmezí -25°C až + 60°C při střední relativní vlhkosti okolo 75% bez kondenzace. „[15]*

Pro prostorovou ochranu jsou používány zařízení zvané detektory. Toto zařízení reaguje na podněty v jeho snímaném prostoru a předává informaci o narušení dalšímu komponentu PZTS, kterým je ústředna. Základní dělení detektoru spočívá v tom, jestli ke své činnosti potřebují, či nepotřebují, elektrickou energii. Podle toho jsou děleny na detektory:

- aktivní – potřebují ke své činnosti elektrickou energii,
- pasivní – napájení elektrickou energií nepotřebují.

Aktivní detektory jsou rozlišovány dle toho, kde jsou instalovány, tedy jestli jsou uvnitř nebo vně objektů. Detektory, instalované uvnitř objektu, se dále člení na klasické a detektory duální. Mezi klasické detektory řadíme pasivní infra, aktivní infra, mikrovlnný, ultrazvukový, mikrovlnnou a ultrazvukovou závoru, vibrační detektor, nárazová detektor. Mezi duální detektory řadíme pasivní infra, mikrovlnné, pasivní infra ultrazvukové a akustické vibrační. [2]

Aktivní detektory, které jsou použiti vně střeženého objektu, jsou od vnitřních detektorů odlišné v konstrukčním provedení. Tyto detektory musí mít zvýšenou odolnost proti venkovním dlouhodobým vlivům. Mezi aktivní detektory pro venkovní použití řadíme detektory pasivní infra, infrazávory, mikrovlnné závory, kapacitní detektory, tenzometrické, štěrbinové kabely, vibrační, akustické, atd. [2]

Pasivní detektory dělíme dále na tísňové hlásiče a pasivní detektory ostatní. Rozdělení tísňových hlásičů je závislé na místě, kde jsou tyto detektory umístěné. Rozlišujeme na venkovní, vnitřní a skryté. Ostatní pasivní detektory jsou magnetické kontakty, destrukční detektory a zajišťovací kontaktní prvky. Princip magnetických kontaktů je založen na jazýčkových kontaktech, které jsou ovládány magnetickým polem. Destrukční detektory jsou využívány k detekci narušení mechanického prvku zabezpečení. Nevýhodou je však pouze možnost jediného použití, protože při splnění své funkce jsou zničeny. [2]

Ústředny, neboli programovatelné a diagnostické zařízení, které zpracovává informace od detektorů a podle toho vyhodnocuje stav. Tyto ústředny lze manuálně ovládat pomocí ovládacího panelu. V denním režimu zpracovává data o pohybu osob v objektu a v nočním režimu vyhlašuje poplach pomocí vyslání signálu na optickou či akustickou signalizaci nebo na dohledové poplachové a přijímací centrum (dále jen

DPPC). Napájení ústředen je řešeno buď odběrem energie ze sítě, nebo využitím baterií. [5]

3.2.3 Elektronická požární signalizace

Elektronická požární signalizace (dále jen EPS) je skupina detektorů požáru, ústředen a doplňujících zařízení. Spolu vytváří systém, který opticky nebo akusticky vyhlásí poplach, pokud detekuje požár a slouží jako včasná signalizace vzniklého požáru. Při detekci požáru může aktivovat prvky, které provedou protipožární zásah např. samohasící systémy. [5]

Hlásič požáru rozdělujeme podle způsobu vyhodnocení stavu na samočinný a tlačítkový. Samočinné hlásiče reagují na změny okolí bez obsluhy, tlačítkové jsou uvedeny do chodu pomocí osob. Celkově lze rozlišit hlásiče požáru na:

- optické hlásiče kouře,
- plamenné hlásiče kouře,
- ionizační hlásiče kouře,
- lineární hlásiče kouře,
- kombinované hlásiče. [5]

Ústředny EPS jsou nedílnou součástí celého systému EPS. Tyto ústředny vyhodnocují získané informace a signály od detektorů. Dokážou ovládat zařízení, které dokáže, přímo či nepřímo, které zabrání šíření požáru. Požadavkem na ústředny je schopnost jejich určení přesné polohy místa vzniku požáru. Musí na informace z hlásičů reagovat akusticky a opticky. Stejně tak i signalizaci poruchy nebo vzniku požáru alespoň tří požárních smyček, což jsou veškeré spojující detektory a hlásiče s ústřednou. [2]

Dalším z prvků EPS jsou **doplňující zařízení**. Mezi ně řadíme např. signalizační zařízení, signalizační panel, orientační tablo, signalizační prvky, ovládací jednotku, zařízení pro dálkový přenos a řídící jednotku. Signalizační panel signalizuje opticky a akusticky vzniklý požár nebo poruchu díky signálu z ústředny. Orientační tablo, na příchozí signál z ústředny, opticky signalizuje místo požáru. Signalizační prvky jsou např. sirény, zvonky, světelné prvky, které signalizují požár. Ovládací jednotka, která zajišťuje ovládání zařízení a přístrojů, které dokáží zabránit požáru nebo usnadňují jeho likvidaci. Zařízení na dálkový přenos je samočinné zařízení, které zajišťuje přenos informace z ústředny do určeného místa pomocí vedení nebo bezdrátově. Řídící jednotka

je zařízení, které samočinně a podle nastaveného programu zapíná či vypíná jednotlivá zařízení EPS. [2]

3.2.4 Kamerové systémy

Systémy průmyslové televize (CCTV – Closed Circuit Television) je jedním z nejpoužívanějších a nejrozšířenějších prostředků k zabezpečení objektů. Největší výhodou tohoto způsobu ochrany je, že je možno sledovat v stejný okamžik více střežených oblastí objektu. Kamerové systémy jsou využívány pro střežení velkých prostor a objektů, výrobních komplexů, v bankách, velkoprodejnách ale také u menších objektů a firem. Díky technickému pokroku a poklesu cen se nasazování kamerových systému dostává i do domácností a střežení rodinných domů.

Kamerové systémy jsou využívány samostatně, nebo jako systém, který doplňuje akustickou a vizuální kontrolu objektu. Tento systém je tvořen částmi pro:

- snímání obrazu,
- přenos signálu,
- zobrazení signálu,
- ovládací část
- další pomocné a doplňkové části. [2]

Pro snímání obrazu jsou použity barevné nebo černobílé kamery. Použití kamer se liší od toho, jak budou využívány. Nejdůležitějšími prvky kamer je rozlišovací schopnost a citlivost. Na kamerové systémy jsou kladeny určité požadavky. Jedná se o možnost detekce pohybu, ukládání poplachových snímků pro pozdější využití, atd. Pokud jsou kamery umístěny vně budovy, musí splňovat určité požadavky na odolnost. Jde o odolnost proti dlouhodobým vnějším vlivům, vlivům počasí nebo proti vandalismu. Ochrana proti vandalismu lze zajistit kryty kamer, ale nejvhodnější volbou je správné umístění kamer, tzn. mimo dosah případných útočníků nebo vandalů.

Kamerové systémy nejsou schopny přímo zamezit případným útokům, přesto však dokáží pachatele od tohoto činu odradit. Slouží také jako určitý psychologický faktor, díky kterému si útočník vnik do chráněného prostoru rozmyslí.

4 NORMY

V této kapitole bude uveden přehled norem, které se týkají prvků, které mohou být použity při instalaci PZTS.

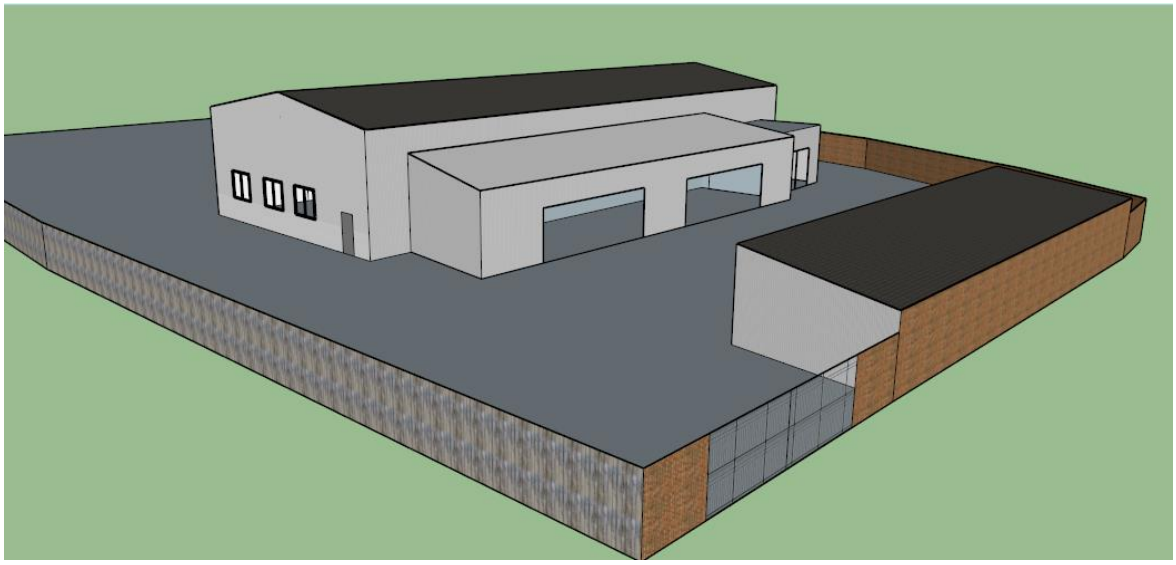
ČSN EN 50131-1 ed. 2	PZTS Systémové požadavky
ČSN CLC/TS 50131-7	PZTS Pokyny pro aplikace
TNI 33 4591-1	PZTS Návrh systému PZTS
TNI 33 4591-3	PZTS Uvedení PZTS do provozu a jeho následný provoz, údržba a servis
ČSN EN 50131-6 ed. 2	PZTS: Napájecí zdroje
ČSN EN 50131-3	PZTS: Ústředny
ČSN EN 50132-1	CCTV: Systémové požadavky
ČSN EN 50132-7 ed. 2	CCTV: Pokyny pro aplikace
ČSN EN 50132-5-1	CCTV: Video přenosy - obecné provozní požadavky
ČSN EN 50132-5-2	CCTV: IP video přenosové protokoly
ČSN EN 50132-5-3	CCTV: Video přenosy - Analogový a digitální video přenos
ČSN EN 60839-11-1	ACCESS: Požadavky na systém a komponenty
ČSN EN 50133-1	ACCESS: Systémové požadavky
ČSN EN 50133-2-1	ACCESS: Všeobecné požadavky na komponenty
ČSN EN 54-1	EPS: Úvod
ČSN EN 54-2	EPS: Ústředny
ČSN EN 54-3	EPS: Sirény
ČSN EN 54-4	EPS: Napájecí zdroj

ČSN EN 54-5	EPS: Bodové hlásiče
ČSN EN 54-7	EPS: Hlásiče bodové využívající rozptýleného světla, vysílaného světla a ionizace
ČSN EN 54-10	EPS: Hlásiče plamene - Bodové hlásiče
ČSN EN 54-11	EPS: Tlačítkové hlásiče
ČSN EN 54-12	EPS: Hlásiče lineární využívající optického světelného paprsku
ČSN EN 54-13	EPS: Posouzení kompatibility komponentů systému
ČSN EN 54-16	EPS: Ústředny pro hlasová výstražná zařízení
ČSN EN 54-17	EPS: Izolátory
ČSN EN 54-18	EPS: Vstupní/výstupní zařízení
ČSN EN 54-20	EPS: Nasávací hlásiče

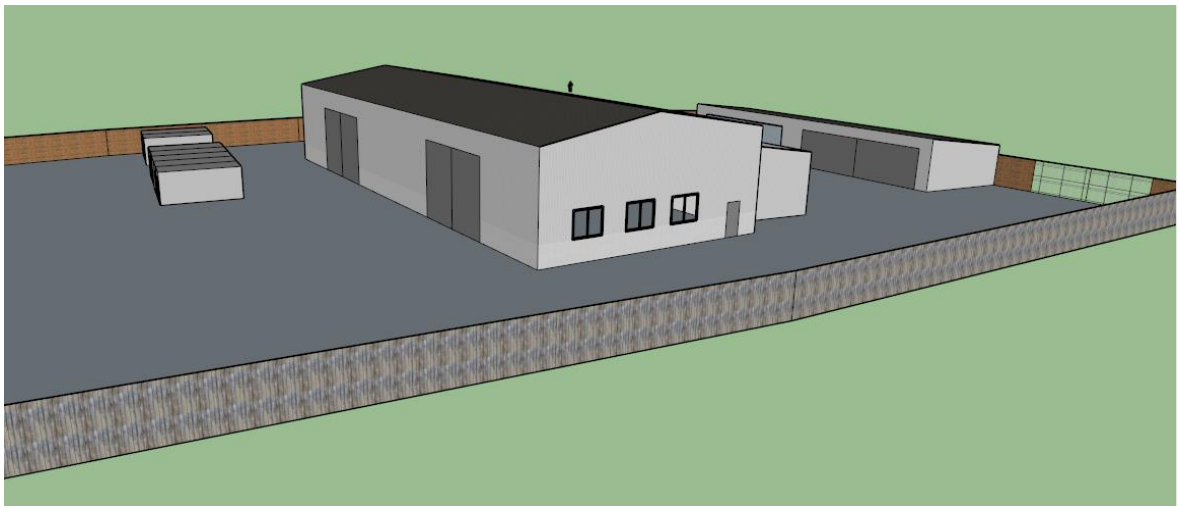
II. PRAKTICKÁ ČÁST

5 ZABEZPEČENÍ OBJEKTU FIRMY ENTEC-KOVO S.R.O.

Praktická část této bakalářské práce se bude věnovat navrhnutí bezpečnostního systému a celkové zabezpečení výrobního komplexu firmy ENTEC-KOVO s.r.o. Se spoluprací vedení této společnosti bude provedena bezpečnostní analýza k posouzení veškerých rizik a hrozeb. Dále budou uvedeny 2 typy návrhů, ze kterých bude moct management firmy vybírat. Společnost ENTEC-KOVO s.r.o. působí od roku 2012, jejíž sídlo a výroba se nachází v průmyslové oblasti ve Starém městě u Uherského Hradiště. Podnik se zbývá výrobou ocelových konstrukcí, palet a kontejnerů pro automobilový průmysl, nádrží, jednoduchých strojů a zařízení, pásových dopravníku, lisovacích a ohýbacích přípravků a odpadových kontejnerů.



Obrázek 3 – pohled na objekt – západní strana [autor]



Obrázek 4 – pohled na objekt – severní strana [autor]

5.1 Obhlídka objektu

V celém areálu, kde se nachází i zabezpečovaná firma, je i další podnik na zpracování skla, který je v tuto dobu ve fázi výstavby. Dále se v areálu nachází nevyužívaný objekt, dříve užívaný jako lakovna. Výrobní komplex naší zabezpečované firmy se skládá z hlavní haly, lakovny, skladovacích prostor hotových výrobků a v poslední řadě obytné kontejnery. Jediným prvkem zabezpečení, který je již instalován v podniku, jsou kamerové systémy.

5.1.1 Analýza objektu – výrobní hala

Výrobní hala je největším objektem, který bude zabezpečován. Ocelovo betonová konstrukce o rozměrech 40×16 se rozkládá na 630m^2. V tomto výrobník objektu jsou aktiva tvořena výrobky, materiálem, vybavením a stroji potřebným k výrobě. Mezi tyto aktiva a stroje patří zejména ohraňovací lis, zařízení k řezání plazmou a vodním paprskem, pásové pily, hydraulické nůžky, svářecí poloautomaty a výbava ke svařování. Do objektu vedou čtyři vchody. Na severní straně jsou dvoje dvoukřídlá vrata, dostatečně velká k manipulaci s výrobky a průjezdu s vysokozdvižným vozíkem. Na jižní straně je vchod do zadní části objektu. Poslední vchod je ze západní strany, kde se nachází pásové pily. U tohoto vchodu se nachází jediné prosklené plochy. Dále se uvnitř nachází i biometrický docházkový systém.

Obrázek 5 – Biometrický docházkový systém [autor]

Obrázek 6 – čelní strana výrobní haly [autor]

5.1.2 Analýza objektu – lakovna, skladovací prostory

Dalšími zkoumanými objekty jsou lakovna a skladovací prostory. Oba tyto objekty se nachází na jižní straně areálu, tedy za výrobní halou. Do tohoto prostoru vedou dvě cesty, které jsou vedeny z obou stran objektu. Do lakovny vedou 2 vstupy. Ty jsou realizovány posuvnými vraty, uzpůsobeny tak, aby se dalo manipulovat s výrobky a také pro vjezd a výjezd vysokozdvižného vozíku. V lakovně se nachází i benzínové čističe, ředidla a další hořlaviny. Skladovací prostory plechové konstrukce jsou vystavěny pro potřebu úschovy hotových výrobků před expedicí.

Obrázek 7 – Lakovna [autor]

Obrázek 8 – Skladovací prostory [autor]

5.1.3 Analýza objektu – obytné kontejnery

Obytné kontejnery se nacházejí na severní straně areálu, přímo před výrobní halou. Tři kontejnery slouží jako kanceláře vedení firmy, techniků a účetní. V dalších dvou buňkách jsou umístěny toalety, sprchy a šatny.

Obrázek 9 – Obytné kontejnery [autor]

5.1.4 Analýza přilehlého okolí

Jak již bylo řečeno, objekt se nachází v průmyslové oblasti ve Starém městě u Uherského Hradiště. V jeho blízkém okolí se nachází centrální distribuční sklad společnosti Hamé s.r.o., KOVOSTEEL recycling s.r.o. a OTR recycling s.r.o. Během dne se tedy kolem areálu pohybuje velký počet osob. Vzhledem k tomu, že je společnost koncipována jako kovovýroba, nachází se v blízkosti výrobní haly velký počet materiálu, který by mohl být předmětem krádeže. Během letních měsíců jsou v blízkosti pořádány různé akce pro veřejnost, takže v tuto dobu je výskyt osob v okolí areálu nejvyšší. Za plotem ze severní strany se nachází parkoviště kamionů, které zde parkují i přes noc, což může být dalším předmětem hrozby. Velkou nevýhodou je propojení areálu s areálem společnosti OTR recycling s.r.o., které odděluje brána na jižní straně.

5.2 Posouzení stávajícího zabezpečení

Zřízení bezpečnostní politiky podniku nebyl prvořadý cíl společnosti. Avšak v průběhu let docházelo ke ztrátám materiálu a různého vybavení. Prvním krokem společnosti bylo pořízení kamerového systému. Jedná se o IP kamery, které snímají jak vnější oblast, tak i vnitřní prostory výrobní haly. Jde však o jediný prvek, který zajišťuje

bezpečnost. Celý objekt je ohraničen plotem. Ze severní a západní strany je dřevěný plot do výšky 2,5m , z jižní a východní strany je areál ohraničen cihlovým plotem do výšky 3m. Ploty jsou zajištěny proti přelezení ostnatým drátem.

Obrázek 10 – Cihlový plot s ostnatým drátem [autor]

Obrázek 11 – Dřevěný plot s ostnatým drátem [autor]

Obrázek 12 – Rozmístění kamer [autor]

Obrázek 13 – Prostory snímané kamerami [autor]

Kamerový systém je řešen IP kamerami Ubiquiti airCam. Tyto kamery jsou napájeny po Ethernetu, tedy po lokální počítačové síti. K obsluze byl dodán i softwarový program, kterým lze ovládat všechny kamery snímající areál. Celkem 9 kamer snímá jak venkovní, tak i vnitřní prostor objektu. Dvě kamery jsou instalovány uvnitř výrobní haly, zbývající kamery jsou instalovány venku. Jediná možná slabá místa, která nejsou pokryty kamerami, se nachází u brány a plotu na jižní straně. Brána bude zajištěna v následujícím návrhu zabezpečení. Ochranu proti přelezení plotu zajišťuje dostatečná výška plotu a ostnatý drát.

5.3 Analýza SWOT

Jak již bylo řečeno výše, SWOT analýza využíván pro zjištění silných a slabých stránek firmy a pro zjištění příležitostí a hrozeb. V této podkapitole provedu příslušnou analýzu ke zjištění těchto faktorů, které budou nápomocny při návrhu celkového zabezpečení podniku. Cílem této analýzy je zjištění rizik a eliminace případných nežádoucích situací ve sledovaném podniku.

Tabulka 1 – Analýza SWOT

Silné stránky	Příležitosti
Kamerový systém Průmyslová oblast	Snížení nákladů Zvýšení produkce
Slabé stránky	**Hrozby**
Chybějící EPS Chybějící PZTS Chybějící SBS	Akce pro veřejnost v blízkém okolí Úmyslné poškození majetku

Mezi silné stránky lze zařadit již nainstalovaný kamerový systém, který dokáže pokrýt zájmové prostory vně i uvnitř objektu. Za silnou stránku lze považovat i skutečnost, že se objekt nachází v průmyslové oblasti, což znamená, že v okolí není takový výskyt cizích osob a tím eliminuje množství možných útoků na majetek firmy.

Ve výrobní hale se nachází různé přístroje, které emitují teplo. Ať už jde o zařízení k řezání plazmou, svářecí poloautomaty nebo brusky, všechny tyto nástroje mohou způsobit svou činností vznik požáru. Jako první slabou stránku lze tedy uvést chybějící EPS. Dále, jak již bylo uvedeno výše, chybí PZTS, což je další slabou stránkou. Jako další faktor lze hodnotit fakt, že objekt se nachází v průmyslové zóně, který leží na okraji města. V blízkém okolí se totiž nenachází žádná z bezpečnostních služeb.

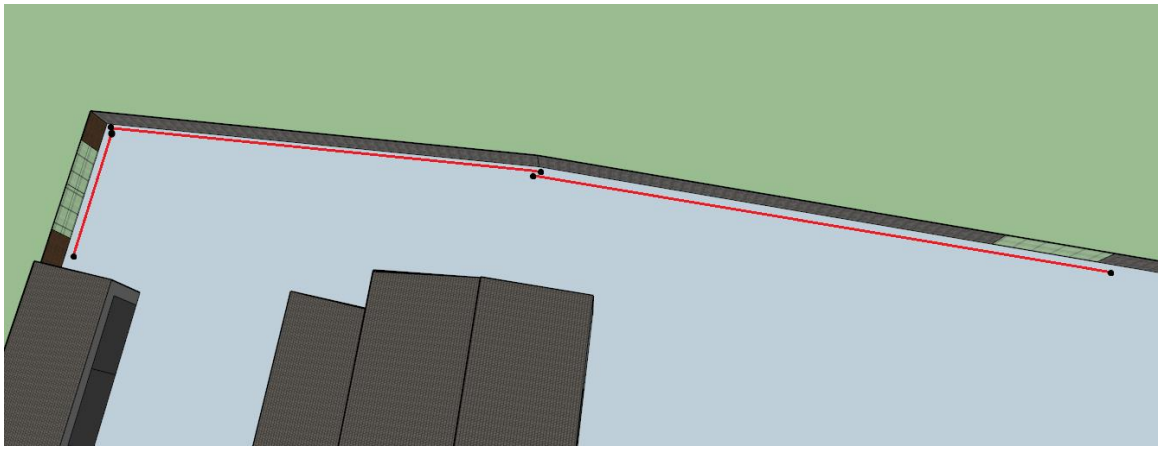
Jako příležitosti, které vyplynou z realizace zabezpečení podniku, lze v první řadě označit snížení nákladů spojených s nežádoucími situacemi, jako jsou krádeže, vandalismus, apod. Dále lze jako příležitost označit zvýšení produkce, z důvodu bezpečnějšího uložení a skladování hotových výrobku či výrobního materiálu.

Jako hrozby, které vedou vedení společnosti k instalaci bezpečnostních zařízení, lze brát např. pořádání akcí pro veřejnost okolních firem, což vede k většímu výskytu osob v okolí zabezpečovaného podniku Další hrozbou je možnost vandalismu, krádeží nebo žhářství.

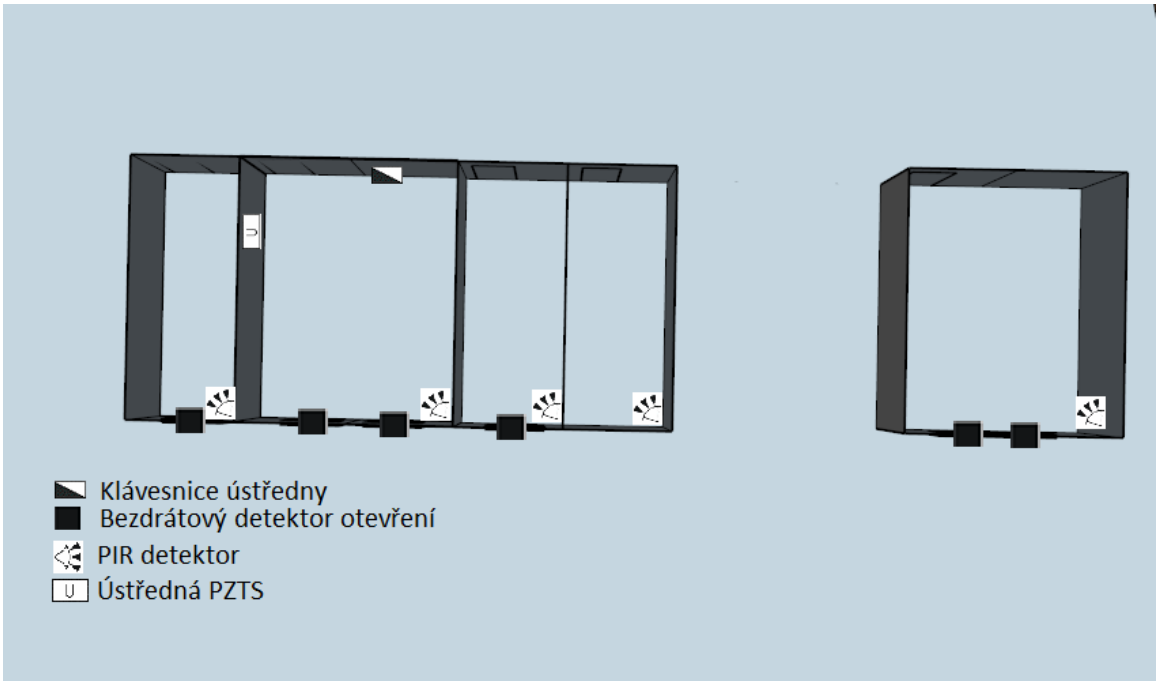
6 I. NÁVRH ZABEZPEČOVACÍHO SYSTÉMU

Poté, co byla provedena bezpečnostní analýza je jasné, že vnější riziko je vyšší než vnitřní. Zařízení a stroje potřebné k výrobě se nachází uvnitř výrobní haly. Většina těchto strojů se díky své konstrukci nedá odcizit. Proto bude hlavní prioritou zabezpečit perimetr objektu a plášť. Ve sborníku technické harmonizace úřadu pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ), který určuje úroveň stupně zabezpečení, je pro zámečnictví a kovovýrobu určen stupeň I. Vzhledem k provedené analýze a dalším faktorům je, ve sledovaném podniku, zvolen stupeň zabezpečení č. II. Dle příslušného stupně, jak již bylo zmíněno výše, se předpokládá, že pachatelé mají určitou znalost o PZTS a užívají jen základní vybavení. Pro tento návrh zabezpečení bude použit systém OASiS společnosti Jablotron. Veškeré prvky budou komunikovat bezdrátově. Výhodou bude snadná instalace a odpadá nutnost tahání kabeláže.

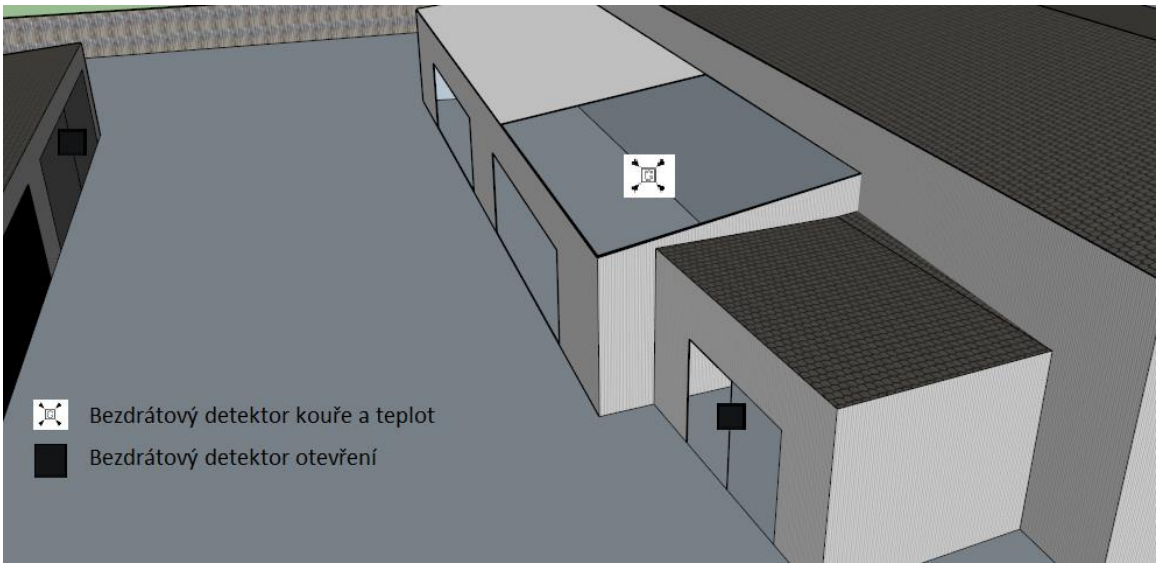
6.1 Aplikace zabezpečení



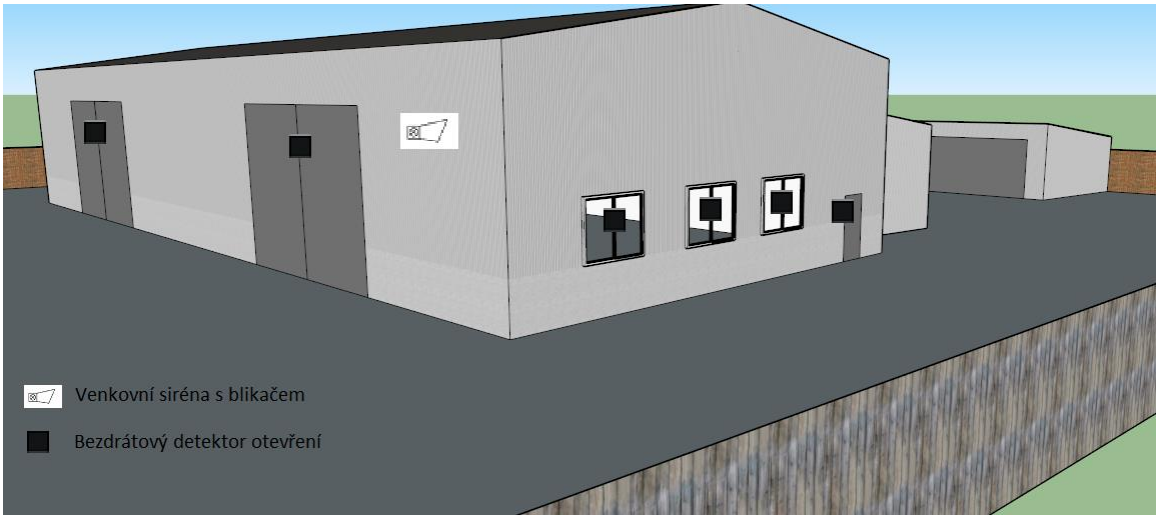
Obrázek 14 – Rozmístění bezdrátových infra závor, západní strana [autor]



Obrázek 15 – Zabezpečení buněk [autor]



Obrázek 16 – Zabezpečení zadní části objektu – Lakovna [autor]



Obrázek 17 – Umístění venkovní sirény – Čelní strana výrobní haly [autor]

6.2 Použitá technika

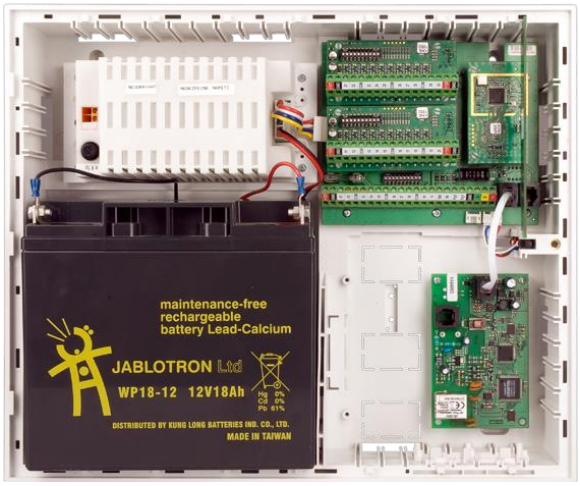
Ústředna JA-83K OASIS

Jedná se o hybridní ústřednu, lze tedy využívat bezdrátovou komunikaci či komunikaci po sběrnici. Je ideální pro zabezpečení rodinných domů i malých a středních firem. Ústředna splňuje stupeň bezpečnosti č. 2. Dále lze rozdělit na 2 subsystémy, paměť pro 50 uživatelů, využívající kódy nebo RFID čipy.

Tabulka 2 – Technické parametry - JA-83K [16]

Napájení	230 V / 50 Hz, max. 0,1 A
Stupeň zabezpečení	2 dle ČSN EN50131-1,ČSN CLC/TS 50131-3, ČSN EN 50131-6, ČSN EN 50131-5-3
EMC	ČSN EN 50130-4, ČSN EN 55022
Třída prostředí	II. vnitřní všeobecné - ČSN EN 50131-1
Zálohovací akumulátor	12V, 7 až 18 Ah
Počet adres pro bezdrátové periferie	až 50 s rozšiřujícím modulem
Počet drátových vstupů	10 (až 30 s rozšiřujícím modulem, dvojitě vyvážené vstupy rozlišující aktivaci a sabotáž
Paměť událostí	255 posledních událostí včetně data a času
Napájecí zdroj	typ A (ČSN EN 50131-6)

Maximální doba na dobití akumulátoru	72 h
Životnost kvalitního akumulátoru	max. 5 let



Obrázek 18 – Ústředna JA-83K [16]

JA-82Y GSM komunikátor

Jde o rozšiřující modul ústředny. Je to GSM komunikátor, díky kterému lze umožnit vzdálený přístup do systému. Pří narušení komunikuje s DPPC a odesílá SMS na mobilní telefon a to až pro 8 telefonních čísel. Díky tomuto komunikátoru lze ovládat systém pomocí mobilního telefonu přes hlasové menu a SMS.

Tabulka 3 - Technické parametry - JA-82Y [17]

Napájení	12V DC (z ústředny)
Zabezpečení	stupeň 2
EMC	ČSN ETSI EN 301489-1, ČSN ETSI EN 301489-7, ČSN EN 55022, ČSN EN 50130-4
Třída prostředí	II. vnitřní všeobecné - ČSN EN 50131-1
Proudový odběr	cca 35 mA (závisí na síle GSM)
Pracovní pásmo	QUAD-BAND, 850/900/1800/1900MHz

Obrázek 19 – JA-82Y GSM komunikátor [17]

JA-81F Bezdrátová klávesnice

Tato bezdrátová klávesnice komunikuje se systémem OASiS. Slouží k ovládání a programování ústředny a celého systému. Výhodou této klávesnice je čtečka přístupových karet. Je napájena pomocí baterií.

Tabulka 4 – Technické parametry – JA-81F [18]

Napájení	2x lithiová baterie
Komunikační pásmo	868 MHz, protokol OASiS
Zabezpečení	ČSN EN 50131-1, ČSN EN 50131-3, ČSN EN 50131-6, ČSN EN 50131-5-3 - stupeň 2
Komunikační dosah	cca 100m (přímá viditelnost)
Životnost baterie	Max 2 roky
Třída prostředí	II. vnitřní všeobecné - ČSN EN 50131-1

Obrázek 20 - JA-81F
Bezdrátová klávesnice [18]

Bezdrátový detektor kouře a teplot JA-85ST

Jedná se o kombinovaný detektor, který obsahuje teplotní detektor a detektor kouře. První jmenovaný pracuje na principu rozptýleného světla a je citlivý na částice, které jsou obsaženy v hustém dýmu. Méně citlivý je však při hoření kapalin, např. alkoholu. Proto je kombinovaný s teplotním detektorem, který na požár s malým množstvím kouře reaguje podstatně lépe. Je napájen pomocí baterií.

Tabulka 5 – Technické parametry – JA-85ST [19]

Napájení	3x lithiová baterie
Komunikační pásmo	868,5 MHz, protokol OASiS
Zabezpečení	ČSN EN 50131-1, ČSN EN 50131-3, ČSN EN 50131-6, ČSN EN 50131-5-3 - stupeň 2
Poplachová teplota	+60 °C až +65 °C
Detekce kouře	optický rozptyl světla
Třída prostředí	II. vnitřní všeobecné - ČSN EN 50131-1
Detekce teplot	třída A1 dle ČSN EN 54-5
Rozsah pracovních teplot	-10 °C až +70 °C

Obrázek 21 – Bezdrátový detektor kouře a teplot JA-85ST [19]

JA-80P Bezdrátový PIR detektor pohybu

Tento typ detektoru slouží k ochraně vnitřních prostor budovy. Plocha, kterou dokáže pokrýt, činí přes 100m^2. Díky digitální analýze dosahuje vysoké odolnosti vůči falešným poplachům. Citlivost odolnosti lze nastavit do dvou úrovní. Detektor komunikuje s protokolem OASiS a je napájen pomocí baterie.

Tabulka 6 – Technické parametry – JA-80P [20]

Napájení	1x lithiová baterie
Komunikační pásmo	868 MHz, protokol Oasis
Komunikační dosah	cca 300m (přímá viditelnost)
Prostředí dle ČSN EN 50131-1	II. vnitřní všeobecné -10 až +40 °C
Doporučená instalační výška	2,5 m nad úrovní podlahy
Úhel detekce / délka záběru	120° / 12 m (se základní čočkou)
Klasifikace	Dle ČSN EN 50131-1, ČSN EN 50131-2-2, ČSN EN 50131-5-3 - stupeň 2
Životnost baterie	Max. 3 roky

Obrázek 22 - PIR detektor [20]

JA-81M Bezdrátový detektor otevření

Jedná se o zabezpečovací zařízení, které detekuje otevření dveří, oken či jiných otvorů. Detektor se montuje na pevný rám, aktivační magnet na pohyblivý rám. Detektor reaguje na oddálení magnetu při otevření okna. Detektor bezdrátově komunikuje s protokolem OASiS a je napájen baterií.

Tabulka 7 – Technické parametry – JA-81M [21]

Napájení	1x Lithiová baterie typ LS(T)14500
Komunikační pásmo	868 MHz, protokol Oasis
Komunikační dosah	cca 300m (přímá viditelnost)
Životnost baterie	Max 3 roky
Prostředí dle ČSN EN 50131-1	II. vnitřní všeobecné -10 až +40 °C
Klasifikace	ČSN EN 50131-1, ČSN EN 50131-2-6, ČSN EN 50131-5-3 stupeň 2
Rozměry	Detektor:110 x 31 x 26 mm, 90g magnet: 56 x 16 x 15 mm

Obrázek 23 - JA-81M Bezdrátový detektor otevření [21]

RC-86K Bezdrátový ovladač

Zařízení komunikující s protokolem OASiS, které dálkově umožňuje ovládat bezpečnostní systém a vyvolat tísňový poplach. Ovladač lze používat nejen na ústřednu, ale i na jiné výrobky firmy Jablotron, které komunikují s protokolem OASiS. Lze nastavit ovládání výrobků v pásmu 868 MHz i 433MHz.

Tabulka 8 – Technické parametry – RC-86K [22]

Napájení	alkalická baterie typ L1016
Komunikační pásmo	868 MHz / 433 MHz
Komunikační dosah	cca 30 m (přímá viditelnost)
Životnost baterie	cca 4 roky
Rozsah pracovních teplot	-10 až +40 °C
Prostředí	II. vnitřní všeobecné dle ČSN EN 50131-1
Klasifikace dle ČSN EN 50131-1	stupeň 2

Obrázek 24 - RC-86K Bezdrátový ovladač [22]

JA-80IR Bezdrátová venkovní infra závora

Celé zařízení je tvořeno vysílačem a přijímačem. Jeho princip spočívá v odeslání signálu na ústřednu v případě, pokud narušitel objektu protne optickou spojnici mezi vysílačem a přijímačem. Obě části mohou indikovat ústředně případnou sabotáž. Jedná se

o prvek perimetrické ochrany. Umístění a montáž této infra závory je 1m nad zemí. Vysílače provádí automatický test a informace posílají ústředně.

Tabulka 9 – Technické parametry – JA-80IR[23]

Napájení	4x Lithiová baterie
Rozsah pracovních teplot	-20°C až +60°C
Životnosti baterie	3 roky
Třída prostředí	IV dle ČSN EN 50131-1
Pracovní kmitočet	868 MHz
Komunikační dosah	až 300 m na přímou viditelnost
Montážní výška detektoru	0,7 – 1,0 m
Vzdálenost (max.) jednotek závory	60m

Obrázek 25 - JA-80IR Bezdrátová venkovní infra závora [23]

JA-80A Bezdrátová vnější siréna

Siréna, komunikující s ústřednou bezdrátově, která slouží k signalizaci narušení objektu. Toto zařízení je doplněno také o optickou signalizaci narušení. Doba trvání akustické signalizace dosahuje 3 minut, ale optická signalizace trvá 30 minut po narušení. Siréna komunikuje s protokolem OASiS a je napájena pomocí baterií.

Tabulka 10 – Technické parametry – JA80A [24]

Napájení	lithiová baterie BAT-80 Jablotron 6 V
Komunikační pásmo	868 MHz, protokol Oasis
Rozměry	230 x 158 x 75 mm, 850 g
Komunikační dosah	cca 300 m (přímá viditelnost)
Životnost baterie	cca 3 roky
Třída prostředí	venkovní všeobecné -25 až +60 °C
Doba houkání sirény	3 minuty
Doba blikání blikače	30 min. po poplachu

Obrázek 26 - JA-80A Bezdrátová vnější siréna [24]

6.3 Cenová kalkulace

Tabulka 11 – Cenová kalkulace – Jablotron

Název	Počet kusů	Cena bez DPH	Celková cena bez DPH	Celková cena s DPH
JA-83K Ústředna	1	2 171,00 Kč	2 171,00 Kč	2 627,00 Kč
JA-82Y GSM Komunikátor	1	5 480,00 Kč	5 480,00 Kč	6 631,00 Kč
JA-81F Bezdrátová klávesnice	1	2 389,00 Kč	2 389,00 Kč	2 891,00 Kč
JA-85ST Kombinovaný detektor kouře a teplot bezdrátový	1	1 316,00 Kč	1 316,00 Kč	1 592,00 Kč
JA-80P Bezdrátový PIR detektor pohybu osob	5	1 239,00 Kč	6 195,00 Kč	7 495,00 Kč
JA-81M bezdrátový detektor otevření a univerzální vysílač	14	921,00 Kč	12 894,00 Kč	15 596,00 Kč
RC-86K Bezdrátový ovladač	3	418,00 Kč	1 254,00 Kč	1 518,00 Kč
JA-80A bezdrátová vnější siréna	1	2 053,00 Kč	2 053,00 Kč	2 484,00 Kč
JA-80IR Bezdrátová venkovní infra závora	3	12 338,00 Kč	37 014,00 Kč	44 787,00 Kč
CELKEM			70 766,00 Kč	85 621,00 Kč

7 II. NÁVRH ZABEZPEČOVACÍHO SYSTÉMU

Pro první návrh byla použita technika od společnosti Jablotron a byl zvolen stupeň zabezpečení číslo II. Pro druhý návrh bude použita technika od společnosti SATEL, rovněž minimální stupeň zabezpečení číslo II. Rozmístění všech bezpečnostních prvků zůstává stejné, jako tomu bylo v případě prvního návrhu.

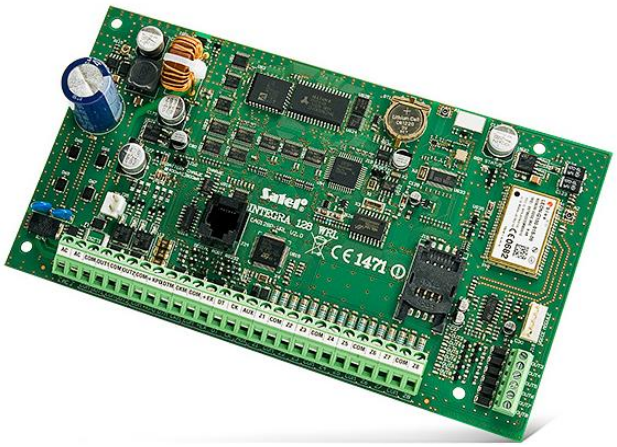
7.1 Použitá technika

Ústředna INTEGRA 128 WRL

Ústředny INTAGRA jsou jedny z nejvýkonnějších a nejrozšířenějších ústředen od společnosti SATEL. Možnost rozšiřování ústředny a možnost výběru z široké nabídky komponentů umožňuje tuto ústřednu použít nejen jako zabezpečovací systém, ale i jako přístupový systém nebo pro automatizaci budov. Tati ústředna obsahuje již zabudovaný GSM komunikátor pro přenos na DPPC, hlasových zpráv nebo SMS. Ovládání je zajištěno klávesnicí, avšak lze ji ovládat i vzdáleně pomocí mobilního telefonu nebo PC.

Tabulka 12 – Technické parametry – INTEGRA 128 WRL [25]

Stupeň zabezpečení	II. dle ČSN EN 50131
Třída prostředí	II.
Rozsah pracovních teplot	-10 °C…+55 °C
Max. počet zón	128
Max. počet bezdrátových zón	120
Rozměry základní desky	192 x 106 mm
GSM komunikátor	ANO (vestavěný)
Ovládání přes WWW prohlížeč	Ano (ETHM-1)
Vzdálené ovládání pomocí mobilního telefonu	Ano



Obrázek 27 - Ústředna INTEGRA 128 WRL [25]

LCD klávesnice INT-KLFR-BSB

Klávesnice je navržena pro každodenní užívání ústředen Integra pomocí klasického uživatelského rozhraní. Komunikace mezi klávesnicí a ústřednou je zajištěna bezdrátovým přenosem. Obsahuje čtečku karet, díky které je možnost ovládat systém pomocí bezkontaktních karet nebo přívěsků. Na klávesnici je možnost vyvolat poplachy tíseň, požár a pomoc.

Tabulka 13 – Technické parametry – INT-KLFR-BSB [26]

Napájecí napětí	12 V DC
Rozměr krytu	145 x 143 x 25 mm
Rozsah pracovních teplot	-10…+55 °C
Třída prostředí	II. dle EN50131-5
Proudová spotřeba v klidu	60 mA
Max. proudová spotřeba	110 mA
Hmotnost	350g

Obrázek 28 - Klávesnice
INT-KLFR-BSB [26]

Detektor kouře a teplot ASD-110

Jedná se o kombinovaný bezdrátový detektor kouře a teploty. Optickou detekcí při zjištění přítomnosti kouře vyhlásí poplach. Stejně tak i teplotní detekcí při dosažení kritické hodnoty teploty ve snímaném prostoru. Informace o poplachu jsou zasílány na ústřednu, dokud přetrvávají podmínky pro jeho vyhlášení. Detektor je vybaven akustickou signalizací a optickou signalizací poplachu v podobě LED diod. Napájení je realizováno pomocí baterie.

Tabulka 14 – Technické parametry – ASD-110 [27]

Frekvence	868.0 MHz – 868.6 Mhz
Dosah	až 500 m ve volném prostoru
Napájení	3V lithiová baterie
Spotřeba	0,085 mA
Životnost baterie	2 roky
Pracovní teplota	0°C až +55°C
Rozměry/Hmotnost	108 x 61 mm / 170g

Obrázek 29 - Detektor
kouře a teplot ASD-110 [27]

PIR Detektor APD-100

Jde o bezdrátový pasivní infračervený detektor pohybu. Pomocí softwarových programů lze dálkově nastavit citlivost detektoru. Další výhodou tohoto typu detektor je možnost nastavení imunity vůči domácím zvířatům. Obsahuje ochranu proti vytržení ze zdi a proti otevření krytu v podobě 2 tamperů. PIR element má zvýšenou odolnost vůči interferencím.

Tabulka 15 – Technické parametry – APD-100 [28]

Pásmo pracovní frekvence	868.0MHz ÷ 868.6MHz
Dosah bezdrátového signálu	až 150 m (v otevřeném prostoru)
Napájení	3V lithiová baterie
Životnost baterie detektoru	3 roky
Třída prostředí/ Rozsah pracovních teplot	II. / -10°C...+55°C
Detekovatelná rychlost pohybu	0,3 až 3 m/s
Rozměry krytu/Hmotnost	63x96x49mm / 110g
Doporučená montážní výška	2,2 až 2,4 m

Obrázek 30 – PIR detektor

APD-100 [28]

Magnetický kontakt AMD-103

Jedná se o bezdrátový magnetický detektor otevření dveří, oken apod. Ochrana je zajištěna tamperem proti odtržení od povrchu, kde je kontakt namontován, a také proti otevření krytu. Mezi hlavní výhody tohoto detektoru patří jeho malé rozměry.

Tabulka 16 – Technické parametry AMD-103 [29]

Pásmo pracovní frekvence	868,0MHz ÷ 868,6MHz
Dosah radiového signálu	350m (v otevřeném prostoru)
Baterie	CR2477N 3V
Životnost baterie	2 roky
Proudová spotřeba v klidu	60μA
Proudová spotřeba maximální	14mA
Třída prostřed	II. dle EN50130-5
Rozsah pracovních teplot	-10°C...+55°C
Rozměry krytu detektoru	32 x 45 x 20mm
Rozměry krytu magnetu	11 x 45 x 10mm
Hmotnost	40g

Obrázek 31 – Magnetický kontakt
AMD-103 [29]

Tlačítkový ovladač APT-100

Víceúčelový ovladač sloužící k ovládání systému zabezpečení. Využívá obousměrné komunikace, což slouží k potvrzení každé zadané operace a indikují je pomocí tří LED diod. Ovladač má 5 tlačítek, které slouží k funkcím jako vypnutí či zapnutí střežení, aktivace poplachu, ovládání zařízení automatizace. Je napájen baterií.

Tabulka 17 – Technické parametry – APT-100 [30]

Pracovní frekvence	868.0 MHz ÷ 868.6 MHz
Dosah rádiového signálu	Až 150m (ve volném prostoru)
Napájení	3V lithiová baterie
Třída prostředí	II. dle EN50130-5
Pracovní teploty	-10…+55 °C
Rozměry	78 x 38 x 16 mm
Hmotnost	30 g

Obrázek 32 – Tlačítkový ovladač
APT-100 [30]

Venkovní siréna ASP-105R

Bezdrátová venkovní siréna, která obsahuje optickou i akustickou signalizaci, která je spouštěna bezdrátovým přenosem. Optickou signalizaci zajišťují výkonné LED diody, akustickou signalizace pak piezoelektrický měnič. Ochrana proti stržení ze stěny a proti otevření je zajištěna tamperem. Lze si vybrat ze čtyř signálových signálů.

Tabulka 18 – Technické parametry – ASP-105R [31]

Pásmo pracovní frekvence	868.0MHz ÷ 868.6MHz
Nominální napájecí napětí	12V DC ±15%
Proudová spotřeba v klidu	30mA
V klidu + nabíjení akumulátoru	150mA
Optická signalizace	165mA
Akustická signalizace	450mA
Vnitřní akumulátor	6V/1.2Ah
Vnitřní ochrana akumulátoru	pojistka T 3.15A
Rozsah pracovních teplot	-20°C...+55°C
Rozměry krytu	148x254x64mm

Obrázek 33 – Venkovní siréna ASP-105R [31]

Optická infrazávora AX-100TFR

Venkovní bezdrátová infrazávora s funkcí úspory energie. Díky těmto funkcím vydrží baterie v detektoru až 5 let. Detektor je chráněn třemi tampery. Lze nastavit čtyři frekvence paprsků kvůli případné instalaci dalších detektorů na jeden sloup. Hlavními výhodami je např. snadná instalace nebo kompatibilita s mnoha bezdrátovými vysílači. Jelikož je detekční rozsah 30m, bude tento detektor využit pro střežení vjezdu.

Tabulka 19 – Technické parametry – AX-100TFR [32]

Detekční rozsah	30m
Metoda detekce	infračervený paprsek narušení
Napájení	LSH20 lithiová baterie: 3,6V; 13Ah; vysílač – 2 kusy; přijímač – 2 kusy
Proudový odběr	5 let
Životnost baterie – vysílač/přijímač	5 let
Perioda poplachu	2 sekundy
Pracovní teplota	-20°C až + 60°C
Přizpůsobení úhlu	+/- 90° horizontálně; +/- 5° vertikálně
Hmotnost	1600g
Rozměry	88x217x163mm

Obrázek 34 – Optická infrazávora AX-100TFR [32]

Optická infrazávora SL-350QNR

Jde o 4 paprskovou závoru, využívající aktivní infračervený sensor, který zajišťuje dosah až 100m. Stěna, přední a zadní kryt detektoru jsou zajištěny proti otevření tamperem. Použitím 4 paprsků je snížen počet falešných poplachů způsobeny padajícím listím nebo ptactvem. Jelikož dosah tohoto detektoru činí 100m, bude přijímač a vysílač použit podél plotu a k zajištění vjezdu od areálu.

Tabulka 20 – Technické parametry – SL-350QNR [33]

Maximální detekční dosah	100m
Detekční metoda	přerušení 4 detekčních paprsků
Zdroj napájení	doporučeno 3,6V, 13Ah
Životnost baterie	vysílač -4 roky, přijímač – 3 roky
Proudový odběr	745uA (vysílač 420uA + přijímač 325uA)
Rozměry	452 x 83 x 138mm (V x Š x H)
Hmotnost	3,3kg (vysílač + přijímač bez příslušenství)
Pracovní teplota	-20°C až +60°C
Čas narušení	nastavitelný 50/100/250/500ms

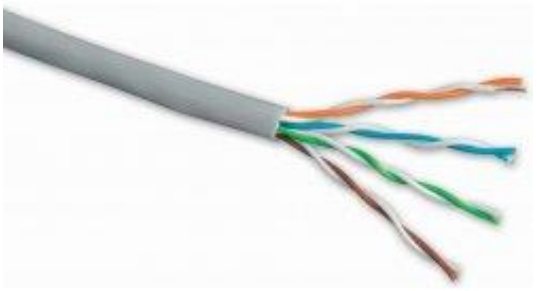
Obrázek 35 - Optická infrazávora SL-350QNR [33]

Instalační kabel SXKD-5E-UTP-PVC

Tento instalační kabel vychází z produktové řady Solarix CAT5E. Je specifický dlouhou životností a maximálním výkonem. Jedná se o měděný vodič o průměru 0,50 mm, průměr kabelu pak 5mm. Všechny tyto kabely splňují požadavky a standardy ANSI/TIA/EIA 568, ISO/IEC 11801 a EN 50173 pro kategorii 5E. Kabeláž je označena po celé své délce metráží po jednom metru.

Tabulka 21 – Technické parametry - SXKD-5E-UTP-PVC [34]

Kategorie	CAT5E
Šířka pásma	100 MHz
Vodič	měděný drát 0, 50 mm AWG 24
Izolace	polyethylen 0, 88 mm
Průměr kabelu	5, 0 mm
Hmotnost	30 kg/km
Skladovací teplota	-20°C až 60°C
Provozní teplota	-20°C až 60°C
Teplota při instalaci	0°C až 50°C



Obrázek 36- Instalační kabel

SXKD-5E-UTP-PVC [34]

7.2 Cenová kalkulace

Tabulka 22 Cenová kalkulace - Satel

Název	Počet kusů ks/m	Cena bez DPH	Celková cena bez DPH	Celková cena s DPH
INTEGRA 128 WRL Ústředna	1	12 058,00 Kč	14 590,00 Kč	14 590,00 Kč
INT-KLFR-BSB Klávesnice	1	3 203,00 Kč	3 876,00 Kč	3 876,00 Kč
ASD-110 Kombinovaný detektor kouře a teplot bezdrátový	1	1 844,00 Kč	2 231,00 Kč	2 231,00 Kč
APD-100 Bezdrátový PIR detektor pohybu osob	5	1 786,00 Kč	8 930,00 Kč	10 805,00 Kč
AMD-103 bezdrátový magnetický kontakt	14	1 270,00 Kč	17 780,00 Kč	21 518,00 Kč
APT-100 Bezdrátový ovladač	3	1 410,00 Kč	4 230,00 Kč	6 824,00 Kč
ASP-105R bezdrátová vnější siréna	1	2 654,00 Kč	2 654,00 Kč	3 211,00 Kč
AX100-TFR Bezdrátová venkovní infra závora	1	11 519,00 Kč	11 519,00 Kč	13 938,00 Kč
SL-350QNR Bezdrátová venkovní infra závora	1	18 502,00 Kč	18 502,00 Kč	22 387,00 Kč
Instalační kabel CAT5e	5m	7,00 Kč	35,00 Kč	40,00 Kč
CELKEM			84 347,00 Kč	99 420,00 Kč

ZÁVĚR

Cílem bakalářské práce bylo navrhnout bezpečnostní systém pro výrobní společnost. Práce je rozdělena na teoretickou a praktickou část. Teoretická část je zaměřena na ochranu bezpečnosti objektu. Je zmíněna bezpečnostní politika, její zaměření a její typy. Pro vytvoření návrhu bezpečnostního systému bylo třeba provést bezpečnostní analýzu. V teoretické části jsou rozebrány bezpečnostní analýzy, základní pojmy, hodnocení rizik spojených s analýzou a jsou rozebrány různé typy analýz, které jsou využívány. V další kapitole jsou shrnuty prvky k zabezpečení objektu, které jsou rozděleny na mechanické zábranné systémy, jakou jsou mříže, závory, rolety, atd. a elektrické a elektronické systémy, což jsou dohledové poplachové a přijímací centra, poplachové zabezpečovací tísňové systémy atd. Ve sledovaném objektu jsou využity jen prvky mechanických zábranných systému. V poslední řadě jsou v teoretické části zmíněny normy, které jsou úzce spjaty s řešenou problematikou.

V podniku je využíván již nainstalovaný kamerový systém. V praktické části jsou vytvořeny dva návrhy bezpečnostního systému, které tento kamerový systém doplní. Oba návrhy byly řešeny na základě vypracované bezpečnostní analýzy pomocí metody SWOT, která definuje silné a slabé stránky podniku, příležitosti a hrozby. Vedení společnosti neurčilo výši rozpočtu na realizaci bezpečnostního systému, proto je rozmístění jednotlivých komponentů u obou návrhů totožné. Pro realizaci těchto návrhů jsou použity prvky od společností Jablotron a Satel. Pro grafické zpracování a vizualizaci objektu byl použit softwarový program SketchUp. Pro přehled jsou oba návrhy dodány i s cenovou kalkulací jednotlivých komponentů. Vedení podniku má tedy možnost vybrat ze dvou cenových variant. Rozmístění detektorů je pro obě varianty stejné. Liší se pouze použití infračervených závor. Tyto zařízení jsou v návrhu určena k zabezpečení části obvodu plotu. V první variantě jsou použity tři infračervené závory, jelikož detekční dosah zařízení činí 60m. V druhé variantě jsou použity dvě různé infračervené závory s dosahem 60m a 100m, což zaručí pokrytí obou vjezdů i zmíněné části obvodu. I z tohoto důvodu, i přes vyšší cenu, bych volil druhou variantu zabezpečení.

SEZNAM POUŽITÉ LITERATURY

[1] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9.

[2] BRABEC, František. *Bezpečnost pro firmu, úřad, občana*. Praha: Public History, 2001, 400 s.

[3] Výstavba bezpečnostní politiky. Výstavba BP [online]. 2010 [cit. 2015-06-01]. Dostupné z: https://akela.mendelu.cz/~lidak/bis/2vystavba.htm

[4] Úvod do režimové ochrany. F.S.C. BEZPEČNOSTNÍ PORADENSTVÍ [online]. 2008 [cit. 2015-06-01]. Dostupné z: http://www.securitye-shop.cz/seznam-e-kurzua-a-dokumentaci/fyzicka-ochrana/uvod-do-rezimove-ochrany

[5] BRABEC, František. *Ochrana bezpečnosti podniku*. 1. vyd. Praha: Eurounion, 1996. ISBN 9788085858297.

[6] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II*. 1. vyd. Zlín: VeRBuM, 2012, 386 s. ISBN 978-80-87500-19-4.

[7] SWOT analýza firmy. FINANČNÍ ANALÝZA FIRMY [online]. 2015 [cit. 2015-06-01]. Dostupné z: http://www.faf.cz/Analyza-ostatni/SWOT-ANALYZA-FIRMY.htm

[8] Metodika zpracování analýzy SWOT pro orgány veřejné správy [online]. 2009 [cit. 2015-06-01]. Dostupné z: http://www.vlastnicesta.cz/clanky/metodika-zpracovani-analyzy-swot-pro-organy-ver/

[9] IVANKA, Ján. *Mechanické zábranné systémy*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 151 s. ISBN 978-80-7318-910-5.

[10] *Pojištění majetku a osob: Všeobecné a doplňkové pojistné podmínky. Česká spořitelna [online]. 2015 [cit. 2015-06-01]. Dostupné z: http://www.ceskapojistovna.cz/documents/10262/50012/Vseobecne-a-doplnkove-pojistne-podminky.pdf*

[11] Bezpečnostní mříže. *Zámečnický servis Mahdal* [online]. 2008 [cit. 2015-06-01]. Dostupné z: http://www.mahdal.cz/mrize_pevne0.html

[12] EN 1143. *Trezory a vše okoli nich* [online]. 2015 [cit. 2015-06-01]. Dostupné z: http://www.jinova.cz/norma-csn-en-1143-1

[13] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-80-7318-889-4.

[14] Elektronická ostraha objektů. *STRÁŽNÍ A BEZPEČNOSTNÍ SLUŽBA* [online]. 2014 [cit. 2015-06-01]. Dostupné z: http://www.sabs.cz/sluzby-3/ostraha-pultem-centralizovane-ochrany

[15] KINDL, Jiří. *Projektování bezpečnostních systémů*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.

[16] JA-83K Ústředna zabezpečovacího systému OASiS Jablotron. *Jabloshop.cz* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.jabloshop.cz/ja-83k-ustredna-zabezpecovaciho-systemu-oasis [17] http://www.jabloshop.cz/ja-82y-gsm-komunikator

[17] JA-82Y GSM Komunikátor Jablotron. Jabloshop.cz [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.jabloshop.cz/ja-81f-bezdratova-klavesnice

[18] JA-81F Bezdrátová klávesnice Jablotron. *Jabloshop.cz* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.jabloshop.cz/ja-81f-bezdratova-klavesnice20 http://www.jabloshop.cz/ja-80p-bezdratovy-pir-detektor-pohybu-osob

[19] JA-85ST Kombinovaný detektor kouře a teplot bezdrátový - Jablotron. *Jabloshop.cz* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.jabloshop.cz/ja-85st-kombinovany-detektor-koure-a-teplot-bezdratovy

[20] JA-80P Bezdrátový PIR detektor pohybu osob - Jablotron. *Jabloshop.cz* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.jabloshop.cz/ja-80p-bezdratovy-pir-detektor-pohybu-osob

[21] JA-81M bezdrátový detektor otevření a univerzální vysílač - Jablotron. *Jabloshop.cz* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.jabloshop.cz/ja-81m-bezdratovy-detektor-otevreni-a-univerzalni-vysilac

[22] RC-86K Bezdrátový ovladač - černé provedení - Jablotron. *Jabloshop.cz* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.jabloshop.cz/rc-86k-bezdratovy-ovladac-cerne-provedeni

[23] JA-80IR Bezdrátová venkovní infra závora Jablotron. *Jabloshop.cz* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.jabloshop.cz/ja-80ir-bezdratova-venkovni-infra-zavora

[24] JA-80A bezdrátová vnější siréna Jablotron. *Jabloshop.cz* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.jabloshop.cz/ja-80a-bezdratova-vnejsi-sirena-1

[25] INTEGRA 128 WRL. *Euroalarm* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.euroalarm.cz/zabezpecovaci-technika/zabezpeceni/komunikace/gsm-gprs/integra-128-wrl

[26] INT-KLFR-BSB. *Euroalarm* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.euroalarm.cz/zabezpecovaci-technika/zabezpeceni/ustredny-a-moduly/klavesnice/lcd/int-klfr-bsb0

[27] ASD-110. *Euroalarm* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.euroalarm.cz/zabezpecovaci-technika/zabezpeceni/bezdratove-prvky/detektory/asd-110

[28] APD-100. *Euroalarm* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.euroalarm.cz/zabezpecovaci-technika/zabezpeceni/bezdratove-prvky/detektory/apd-100

[29] AMD-103. *Euroalarm* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.euroalarm.cz/zabezpecovaci-technika/zabezpeceni/bezdratove-prvky/detektory/amd-103

[30] APT-100. *Euroalarm* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.euroalarm.cz/zabezpecovaci-technika/zabezpeceni/bezdratove-prvky/ovladace/apt-100

[31] ASP-105 R. *Euroalarm* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.euroalarm.cz/zabezpecovaci-technika/zabezpeceni/bezdratove-prvky/sireny/asp-105-r

[32] AX-100TFR. *Euroalarm* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.euroalarm.cz/zabezpecovaci-technika/zabezpeceni/bezdratove-prvky/detektory/ax-100tfr

[33] SL-350QNR. *Euroalarm* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.euroalarm.cz/zabezpecovaci-technika/zabezpeceni/bezdratove-prvky/detektory/sl-350qnr

[34] SXKD-5E-UTP-PVC. *Euroalarm* [online]. 2007 [cit. 2015-06-02]. Dostupné z: http://www.euroalarm.cz/zabezpecovaci-technika/kabelaz/strukturovana-kabelaz/cat-5e/kabely/sxkd-5e-utp-pvc

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CCTV Closed Circuit Television, uzavřený televizní okruh

DPPC Dohledové poplachové a příjímací centrum

EPS Elektronická požární signalizace

EZS Elektronická zabezpečovací signalizace

IT Informační technologie

MZS Mechanické zábranné systémy

PCO Pult centralizované ochrany

PZTS Poplachové zabezpečovací a tísňové systémy

SEZNAM OBRÁZKŮ

SEZNAM TABULEK