Návrh optimalizace poplachového systému průmyslového podniku

A Design of the alarm system of optimization of an industrial company

Bc. Radek Světinský

Diplomová práce 2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

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

Jméno a příjmení:	**Bc. Radek SVĚTINSKÝ**
Osobní číslo:	**A10488**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Návrh optimalizace poplachového systému průmyslového podniku**

Zásady pro vypracování:

1. **Na modelovém objektu průmyslového podniku analyzujte stávající stav vybraných prvků poplachového systému.**
2. **Vymezte oblasti pro optimalizaci a doplnění poplachových aplikací a vyhodnoťte potenciální přínos.**
3. **Vymezte možnosti integrace poplachových a nepoplachových aplikací.**
4. **Navrhněte technické řešení optimalizace a rozšíření poplachového systému.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management. 1. vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.**
2. **KINDL, Jiří. Projektování bezpečnostních systémů I. [skriptum]. Zlín: UTB, 2007. ISBN 978-80-7318-554-1.**
3. **UHLÁŘ, Jan. Technická ochrana objektů: II. díl. Elektrické zabezpečovací systémy. 1. vyd. Praha: Policejní akademie České republiky, 2005. 230 s. ISBN 80-7251-189-0.**
4. **KŘEČEK Stanislav. Příručka zabezpečovací techniky. Vydání 3. Blatná: Cricetus, 2006. 315 s. ISBN 80-902938-2-4.**
5. **LOVEČEK, T., NAGY, P. Bezpečnostné systémy: kamerové bezpečnostné systémy. Žilina: Žilinská univerzita v Žilině, 2008. 272 s. ISBN 978-80-8070-893-1.**
6. **ČSN CLC/TS 50398. Poplachové systémy– Kombinované a integrované systémy– všeobecné požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. 20 s. Třídící znak 334597.**
7. **ČSN CLC/TS 50131-7. Poplachové systémy– Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. 44 s. Třídící znak 334591.**

Vedoucí diplomové práce: **Ing. Jan Valouch, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Úvodní část diplomové práce představuje analýzu stavu stávajících vybraných poplachových prvků v průmyslovém podniku. V další části práce je provedeno bezpečnostní posouzení. Vybrané vymezené oblasti jsou doplněny o poplachové aplikace, a to zejména o poplachové zabezpečovací a tísňové systémy, přístupové a kamerové systémy. Dále jsou vymezeny možnosti integrace poplachových a nepoplachových aplikací. Stěžejní výstup práce představuje návrh technického řešení v souladu s možnostmi integrace jednotlivých poplachových systémů.

Klíčová slova: Poplachové systémy, poplachové zabezpečovací a tísňové systémy, kamerové systémy, přístupové systémy, integrace, analýza, průmyslový podnik, návrh systému.

ABSTRACT

The introductory part of the dissertation presents an analysis of the current state of selected elements of alarm in an industrial company. In another section is an safety assessment undertaken. The selected determined areas are complemented by alarm applications, especially alarm systems, intrusion and hold-up alarm systems, access control systems and CCTV systems. Further are defined possibility of integration of alarm and no-alarm applications. The key output of the work contains the technical solution in accordance with the possibilities of integration of the various alarm systems.

Keywords: Alarm systems, intrusion and hold-up alarm systems, CCTV systems, access kontrol systems, integration, analysis, industrial company, system design.

Rád bych poděkoval Ing. Janovi Valouchovi, Ph.D. za odborné vedení, také za jeho cenné rady a připomínky při zpracování diplomové práce.

Dále bych chtěl poděkovat Pavlovi Rejdovi a Pavlovi Poláškovi za rady a náměty.

Děkuji také své přítelkyni Simoně Švecové za její trpělivost a podporu při studiu a poskytnutí potřebného zázemí.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/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 – diplomovou/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);
- beru na vědomí, že pokud bylo k vypracování diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

……
podpis diplomanta

OBSAH

ÚVOD

V současné době jsou poplachové systémy nezbytnou součástí základního zabezpečení průmyslových podniků. Poplachové systémy sice přímo narušiteli nebo lupiči nezabrání v narušení objektu, ale umožní vzniklou situaci okamžitě signalizovat a předat zprávu správci objektu, bezpečnostní agentuře či přímo policii. Poplachové systémy aktivně přispívají ke snížení či úplné eliminaci vzniku materiálních škod či ohrožení lidských životů. Moderní systémy lze přizpůsobit konkrétním požadavkům uživatele. Poplachové systémy nemusí být aktivní pouze v nočních hodinách, ale mohou výrazným způsobem zvýšit bezpečnost objektu i za denního provozu. Pomocí přenosových zařízení lze informace z poplachových zabezpečovacích systémů okamžitě přenášet na specializovaná místa jako jsou centrální monitorovací pracoviště nebo poplachové přijímací centra bezpečnostních agentur. V dnešní moderní době se možnosti přístupu k sofistikovaným technologiím stále rozšiřují, zároveň však i sílý aktivity osob s protispolečenskými úmysly, počínaje vandalismem až po terorismus. Ve své diplomové práci jsem se rozhodl věnovat problematice zabezpečení konkrétního průmyslového podniku.

V úvodu své diplomové práce objasňuji základní pojmy zabezpečení objektů a poplachových systémů, což by mělo vést ke snadnějšímu a rychlejšímu pochopení dané problematiky. V další části práce analyzuji stávající stav vybraných prvků poplachového systému modelového objektu průmyslového podniku a vymezeji rizikové oblasti pro doplnění poplachových aplikací. Pomocí analýzy a bezpečnostního posouzení jsem zjistil nedostatky v ochraně areálu daného podniku. Protože se jedná o velký areál s řadou objektů, volných ploch, vstupů a vjezdových bran, s relativně volným pohybem velkého množství osob, ve kterém se vyskytuje široká škála výrobních a skladovacích prostorů, bude pro zabezpečení prioritou důkladná perimetrická ochrana. V předposlední části práce se zabývám integrací poplachových a nepoplachových aplikací ve vybraných oblastech analyzovaného podniku. Poslední část diplomové práce představuje návrh poplachového systému perimetrické ochrany, který je vhodný pro bezpečnost osob, budov a má zabránit škodám na hmotném i nehmotném majetku.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST PRŮMYSLOVÝCH PODNIKŮ

Ochrana bezpečnosti podnikatelských subjektů (průmyslových podniků) v současné době nesporně vyžaduje komplexní a systémový přístup. Ochranu bezpečnosti podniku nelze spatřovat pouze v zajištění vnější (plášťové) ochrany objektů patřících příslušnému podnikatelskému subjektu, ale je ji třeba chápat jako složitý systém tvořený subsystémy. [1]

Objektem podniku je třeba rozumět nejen celkovou plochu areálu, ale také všechny výrobní haly a sklady, administrativní a jiné budovy. Všechny tyto objekty mohou být předmětem samostatné ochrany, ať už uvnitř areálu, nebo mimo něj, nebo ochrany celkové.

1.1 Bezpečnost objektu

Předmětem zájmu bezpečnosti každého průmyslového podniku je ochrana:

- osob,
- hmotného majetku,
- nehmotného majetku.

Osobami jsou myšleni vlastní kmenoví zaměstnanci, externí smluvně vázaní pracovníci, ale i jiné osoby, které se nacházejí v objektech firmy.

Hmotným majetkem je soubor movitých i nemovitých prvků, které jsou ve vlastnictví podniku nebo jsou podle zákona předmětem zájmu ochrany podniku.

Nehmotným majetkem v rámci podniku jsou informace (data, know-how), které podnik vytváří, přijímá nebo doplňuje podle smluvní dohody, ujednání, zákona, podnikové normy nebo jiné závazné normy v rámci své činnosti. [2]

Soudobý systém fyzické bezpečnosti objektu (ochrany majetku) zpravidla zahrnujeme:

- režimová opatření,
- fyzickou ochranu (činnost fyzické ostrahy),
- technickou ochranu (technické prostředky systému fyzické bezpečnosti).

1.1.1 Režimová opatření

Režimová opatření v průmyslovém podniku představují procesní naplnění bezpečnostní politiky organizace. Cílem režimových opatření je stanovit zásady, pravidla, oprávnění při pohybu zaměstnanců a dalších osob v prostorách organizace, způsob nakládání s bezpečnostně důležitými prvky, pravidla provádění bezpečnostních kontrol vnášeného a vynášeného materiálu apod. Režimová opatření by měla být navržena tak, aby příliš neomezovala pohyb osob v objektu organizace a současně zajistila požadovaný stupeň bezpečnosti. Významnou roli v této oblasti sehrává systém kontroly vstupu (ACS). [3]

1.1.1.1 Vnější režimová opatření

Vnější režimová opatření týkají se především vstupních a výstupních podmínek z chráněného objektu, tj. prostorů, kudy se vozidla i osoby dostávají do objektu a kudy jej opouštějí. Jedná se především o různé vchody, vjezdy apod.

1.1.1.2 Vnitřní režimová opatření

Vnitřní režimová opatření týkají se především omezení pohybu osob a vozidel v objektu jen na určité oblasti, prostory nebo okruhy (např. omezení vstupu do určitých prostor pouze pro určité pracovníky či vozidla). [4]

1.1.2 Fyzická ochrana (činnost fyzické ostrahy)

Fyzická ostraha zajišťuje ochranu objektu, plní v této oblasti významnou roli. Fyzická ochrana bývá prováděna strážnými, hlídači, hlídací službou či policisty. Většina organizací zajišťuje svoji fyzickou ochranu jako službu poskytovanou jiným právním subjektem, zpravidla soukromou bezpečnostní službou. [3]

1.1.3 Technická ochrana (technické prostředky fyzické bezpečnosti)

Současně s fyzickou ostrahou přestavují technické prostředky fyzické bezpečnosti základní bezpečnostní opatření fyzické bezpečnosti objektu. Cílem technických prostředků je podpořit realizaci režimových opatření, zkvalitnit činnost fyzické ostrahy a odradit narušitele od jeho činu, případně významně ztížit činnost a prodloužit dobu jeho přístupu k chráněným aktivům. Mezi základní technické prostředky fyzické bezpečnosti se řadí mechanické zábranné systémy a elektronické bezpečnostní systémy. Mechanické zábranné

systémy zahrnují dveře, zámky, ploty, mříže apod., které svými vlastnostmi brání fyzickému pohybu narušitele. Cílem elektronických bezpečnostních systémů je řízení přístupu k aktivům organizace a odhalení neoprávněného přístupu k nim. Mezi základní elektronické bezpečnostní systémy řadíme poplachové zabezpečovací a tísňové systémy (PZTS), kamerové systémy (CCTV), přístupové systémy (ACS) a elektronickou požární signalizaci (EPS). [3]

1.2 Poplachový zabezpečovací systém

Poplachový zabezpečovací systém je ve své podstatě digitální elektronický systém, který ve střeženém prostoru trvale monitoruje specifické fyzikální projevy a při jejich výskytu vyhlašuje poplach. Specifickými fyzikálními projevy jsou demaskující projevy přítomnosti narušitele ve střeženém prostoru, spojené zejména s jeho pohybem. Jedná se například o změnu kmitočtu akustických vln odražených od povrchu těla narušitele, vyzařování infračerveného záření tělem lupiče, přerušení paprsku infračerveného záření tělem nebo sepnutí spínače pohybem apod.

Poplachové zabezpečovací systémy jsou zpravidla složeny z ústředny, optických a akustických výstražných prvků, detektorů narušení a přímých spojů, zajišťujících připojení detektorů do ústředny. Ústředna zajišťuje příjem poplachů z jednotlivých detektorů narušení, jejich zaznamenání, vyhodnocení a vyhlášení poplachu. Ústředna poplachového zabezpečovacího systému může být připojena prostřednictvím poplachového přenosového systému na poplachové přijímací centrum (dříve pult centrální ochrany). Detektory narušení tvoří senzorickou část poplachového zabezpečovacího systému. [3]

1.2.1 Základní stupně ochrany

Mezi výsledky optimalizace bezpečnostního systému v průmyslovém podniku patří vymezení principů, uplatněných při jeho návrhu a realizaci. Jedním z těchto principů je princip vícestupňovosti ochrany. Podstata tohoto principu spočívá ve vymezení základních stupňů při zajištění fyzické bezpečnosti, které představují určité hranice, které musí pachatel překonat při postupu v objektu k předmětu jeho zájmu. Základními stupni ochrany jsou:

- perimetrická ochrana,
- plášťová ochrana,

- prostorová ochrana,
- předmětová ochrana.

Každý z výše uvedených stupňů ochrany má svá specifika, která vycházejí z určení z klasifikace prostředí (třídy I až IV) a prostorových dispozic dané ochrany. [3]

1.2.2 Perimetrická ochrana

Perimetrická ochrana přestavuje souhrn bezpečnostních opatření fyzické bezpečnosti, uplatněných na obvodu pozemku průmyslového podniku a v prostoru mezi jeho hranicí a chráněným objektem. Perimetrická ochrana by měla signalizovat narušení odvodu objektu průmyslového podniku. Detektory narušení, použité v rámci perimetrické ochrany, mají obvykle delší dosah a užší detekční charakteristiku, musí splňovat požadavky vyšší klimatické odolnosti a být odolné vůči planým poplachům. [3]

1.2.3 Plášťová ochrana

Plášťová ochrana je souhrnem bezpečnostních opatření fyzické bezpečnosti realizovaných na plášti chráněného objektu (budovy) v průmyslovém podniku. Cílem plášťové ochrany je odstrašení, znemožnění průchodu, zpoždění a odhalení narušitele. Plášťová ochrana signalizuje narušení pláště budovy. Plášťovou ochranu tvoří stěny, okna, dveře, zámky, a zámkové systémy, mříže, kamerové systémy, systémy kontroly vstupu, u PZTS (magnetické kontakty,detektory tříštění skla atd.). [3]

1.2.4 Prostorová ochrana

Cílem prostorové ochrany je zpoždění a odhalení pohybu narušitele uvnitř střežené budovy. Opatření prostorové ochrany jsou realizována ve vnitřních prostorách budovy, zpravidla na chodbách, schodištích a v místnostech. Prostorovou ochranu tvoří dveře, mříže, zámky a zámkové systémy, kamerové systémy, systémy kontroly vstupu a poplachové zabezpečovací systémy s detektory narušení. Detektory narušení by měly v rámci prostorové ochrany signalizovat vniknutí do vnitřních prostor budovy. [3]

1.2.5 Předmětová ochrana

Předmětovou ochranu tvoří opatření vedoucí k zamezení zcizení a neoprávněné manipulaci s chráněnými aktivy. Chráněnými aktivy jsou obvykle cenné umělecké předměty atd., z jakéhokoliv důvodu cenné, fyzické předměty. Detektory narušení by měly identifikovat bezprostřední přítomnost narušitele u chráněného předmětu nebo jakoukoliv manipulaci s ním. [3]

1.2.6 Stupeň zabezepčení

Stupeň zabezpeční je stanoven na kvalitativní schopnosti činnosti narušitele a jeho znalosti, dovednosti a technické vybavení, jimiž disponuje při překonání systému fyzické bezpečnosti. Stupně zabezpečení jsou rozděleny na čtyři stupně , nízké riziko, nízké a střední riziko, střední a vysoké riziko a na vysoké riziko.

Stupeň zabezpečení určuje provedení systému fyzické bezpečnosti, včetně poplachového zabezpečovacího systemu a detektorů narušení. Stupeň zabezpečení celého poplachového zabezpečovacího systemu je dán nejnižším stupněm zabezpečení kteréhokoliv z použitých komponentů, včetně detektorů narušení. [3]

1.3 Poplachové systémy

Poplachové systémy rozdělujeme na poplachové zabezpečovací a tísňové systémy, kamerové a přístupové systémy, systémy přivolání pomoci, poplachové přenosové systémy a zařízení a systémy kombinované nebo integrované. Dále jsou uvedeny poplachové systémy, které jsou použity v návrhu technického řešení poplachového systému.

1.3.1 Poplachové zabezpečovací a tísňové sytémy

Poplachové zabezpečovací a tísňové systémy (dale PZTS), z angličtiny Intruder and Hold-up Alarm System (I&HAS), slouží k signalizaci nebezpečí ve střeženém objektu. Zejména informují o nežádoucím vniknutí (vloupání) do objektu. Mouhou však být kombinovány i s indikací jiných nebezpečí (např. tísňové hlášení při přepadení či zdravotních obtížích, požární nebezpečí, únik plynu apod. Podrobné údaje uvadí normy ČSN EN 50131-1 ed. 2 a ČSN CLC/TS 50131-7. [3]

Zařízení poplachového zabezpečovacího a tísňového systému je soubor detektorů, tísňových hlásičů, ústředen, prostředků polachové signalizace, přenosových zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno na určeném místě narušení střeženého objektu nebo prostoru. [2]

1.3.2 Kamerové systémy

Kamerové systémy (dale CCTV) jsou vysoce účinným prvkem zabezpečení průmyslových podniků. Výrazným způsobem znásobují možnosti fyzické ostrahy objektu tím, že jsou schopny monitorovat současně množství střežených prostor, umožňují obsluze doslovat vidět, co se ve střeženém prostoru děje, a v případě jakéhokoliv narušení je trvale dokumentovat. CCTV jsou používány při ochraně velkých průmyslových komplexů.

Kamerový systém je složen z několika částí:

- část, která zajišťuje snímání obrazu,
- část, která zajišťuje přenos obrazu,
- část, která uchovává záznam obrazu (digitální videorekordér),
- část, která přenesený signal zobrazuje,
- část ovládací,
- příslušenství.

CCTV mají určitý psychologický vliv na potenciálního vetřelce a samotnou svou existencí v místě, které mají spoluochraňovat, mohou případného narušitele od nežádoucího jednání odradit. CCTV přenáší obsluze nezkreslenou informaci v reálném čase v podobě, která je naprosto srozumitelná (obraz) a kterou je možné nezkresleně zadokumentovat. CCTV system slouží na identifikaci, rekognostiku a detekci osob. [2]

Podrobné údaje uvadí norma ČSN EN 50132-1, nebo ČSN EN 50132-7. CCTV se používají buď jako samostatné, autonomní systémy nebo v kombinaci převážně se systémy PZTS a ACS. Celý kamerový systém se skládá z několika dílčích částí z jednotlivých kamerových sestav zajišťujících snímání obrazu, z prvků pro zajištění přenosu videosignálu (obrazu), z prvků zajišťujících zpracování a vyhodnocení přijatých videosignálů a z jiných doplňkových zařízení a příslušenství.

1.3.3 Přístupový systém

Přístupový systém (dále jen ACS) neboli systém kontroly vstupů (SKV) můžeme chápat jako soubor opatření k zajištění řízení a evidence přístupu do zabezepčeného objektu nebo prostor na základě jednoznačně přidělených přístupových práv. Tato opatření mohou být systémová, fyzická (ostraha), mechanická (zámky, mříže, závory) nebo elektronická, nejúčinnější je jejich kombinace. Přístupová práva jsou každému uživateli přidělena na základě personální politiky, stupně oprávnění, časového harmonogramu apod. Na základě jednoznačné identifikace uživatele je po ověření přístupových práv povolen nebo zamítnut přístup. Sofistikovanější systémy umožnují např. sledovat pohyb a přítomnost osob v jednotlivých úsecích, definovat návaznost průchodů nebo "za běhu" měnit přístupová práva. [3]

Podrobné údaje uvádí norma ČSN EN 50133-1 a ČSN EN 50133-7. Hlavní technické požadavky kladené na zařízení přístupových system, které jsou obsaženy v harmonizovaných evropských normách ČSN EN řady 50 133-2-1, případně v zákonu č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti a take ve vyhlášce NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Je nutné rozlišovat pojmy „přístupové" a „docházkové" systémy. U docházkových systémů je prokázání identity uživatele také nezbytné, ale prvotním cílem není pouze řízení přístupu do objektu, ale především monitorování času a důvodu průchodu daným místem (zákonná povinnost zaměstnavatele monitorovat pracovní dobu zaměstnanců, povinné přestávky apod.). [3]

1.3.3.1 Integrace ACS s jinými systémy

Přístupové systémy mohou být provozovány s jinými slaboproudými systémy, jejich funkce jsou integrovány nebo rozšířeny. V praxi existují převážně kombinace s těmito systémy:

- docházkový systém – v jednom systému jsou použity docházkové i přístupové funkce,
- stravovací systém – využívá se především shodných identifikačních médií, jinak samotný systém,
- poplachový zabezpečovací a tísňový systém (PZTS) – sofistikovanější sběrnicové systémy PZTS často podporují základní funkce přístupových systémů, výhodou je zde

možnost ovládat systém PZTS prostřednictvím přístupových identifikátorů, monitorovat stav PZTS za dveřmi na čtečce apod. (např. otevření dveří a zároveň odjištění PZTS subsystém / delší podržení zajistí PZTS subsystém apod.,

- kamerový systém (CCTV) – CCTV systém může při časové synchronizaci s ACS poskytnout doplňkové obrazové informace ke každé prostupové události,
- elektrická požární signalizace (EPS),
- IT systémy – samostatnými čtečkami identifikačních médií, připojených k PC se může řídit přístup k PC, k síti apod.,
- měření a regulace – přítomnost osob může např. automaticky přizpůsobit osvětlení, vytápění apod. [3]

Dílčí závěr

První část diplomové práce se skládá z teoretické části popisující základní pojmy k zabezpečení průmyslových podniků. Cílem teoretické části je vysvětlení základních stupňů ochrany a rozdělení a definování poplachových systemů jako jsou poplachové zabezpečovací a tísňové systémy, kamerové a přístupové systémy, které jsou dále použity v diplomové práci a take v návrhu technického řešení.

II. PRAKTICKÁ ČÁST

2 ANALÝZA STÁVAJÍCÍHO STAVU VYBRANÝCH PRVKŮ POPLACHOVÉHO SYSTÉMU PRŮMYSLOVÉHO PODNIKU

Modelový objekt, průmyslový podnik je oplocený komplex budov, výrobních hal a přilehlých prostorů, ve kterém platí interní nařízení, a který je smluvně fyzicky střežen bezpečnostní firmou. V areálu má sídlo nebo provozovnu 20 externích firem. Používané vstupy a vjezdy do objektu tvoří tři obslužné a tři bezobslužné vrátnice. Na těchto vrátnicích jsou instalované poplachové systémy. Jedná se zejména o přístupový systém (ACS) a kamerový systém (CCTV). Poplachový zabezpečovací a tísňový systém (PZTS) je instalovaný na vybrané budovy a kanceláře. Elektrický požární systém (EPS) je instalovaný na všech budovách v areálu firmy. V další části kapitoly je provedena analýza stávajícího stavu vybraných prvků poplachového systému.

2.1 Analýza přístupového systému

Hlavním úkolem přístupového systému je umožnění vstupu do průmyslového podniku pouze oprávněným osobám (zaměstnancům, dlouhodobým návštěvám a spolupracujícím firmám a návštěvníkům) v uživatelsky nastavitelné době a rozsahu oprávnění stanovené z bezpečnostních hledisek správcem systému (zaměstnancem odboru bezpečnosti) a zamezení vstupu osobám nepovolaným a nežádoucím.

Přístupový systém (dále jen ACS) je instalovaný na všech obslužných i bezobslužných vstupů do areálu průmyslového podniku. Na vrátnicích obslužných jsou instalované turnikety polovysoké a na vrátnicích bezobslužných jsou instalované turnikety plnovysoké. Přístupový systém je integrovaný s docházkovým systémem a kamerovým systémem.

Vstup do areálu je možný:

- s trvale přidělenou bezkontaktní čipovou kartou s technologií RFID (Radio Frequency Identification), která využívá k přenosu informace mezi čtečkou a čipovým identifikačním médiem radiových vln. Přístupové body představují prvky, které umožní kontrolovaný přístup do areálu firmy, jsou tvořeny docházkovými terminály,
- krátkodobě (časově omezenou) s čipovou kartou zaměstnanci externích firem provádějící v areálu krátkodobé servisní a dodavatelské činnosti,
- náštěvy s čipovou kartou na jednorázový vstup nebo vjezd vozidel.

2.1.1 Závory

Systém ACS ovládá stávající závory pro vjezd vozidel do objektu (pouze na bezobslužné vrátnici u AB, jinak závoru ovládá bezpečnostní služba ručně , až po kontrole auta atd.). Na vrátnici jsou karetní čtečky nainstalované na sloupku pro vjezd i výjezd a to ve dvou výškových úrovních, pro použití osobními a nákladními vozidly. Na vrátnici, která je jako výjezdová jsou čtečky pouze na výjezdu a to opět ve dvou výškových úrovních. Karetní čtečka pro osobní vozidla je instalována v docházkovém terminálu. Vrátnice je uvažována jako brána pouze pro osobní vozidla a čtečky jsou instalovány na vjezdu a výjezdu pouze ve výšce osobních vozidel. Čtečka na straně výjezdu je instalována v docházkovém terminálu.

2.1.2 Turnikety

Turnikety pracují na principu automatické přístupové kontroly s vestavitelnou čtečkou karet. V objektech je karetní čtečka instalovaná v docházkovém terminálu. Turnikety zamezují svou funkcí neoprávněný vstup do objektu bez nutnosti dohledu. Pro případ poruchy je na recepci vrátnice nainstalované tlačítko, kterým je možné všechny turnikety na tomto objektu nouzově otevřít.

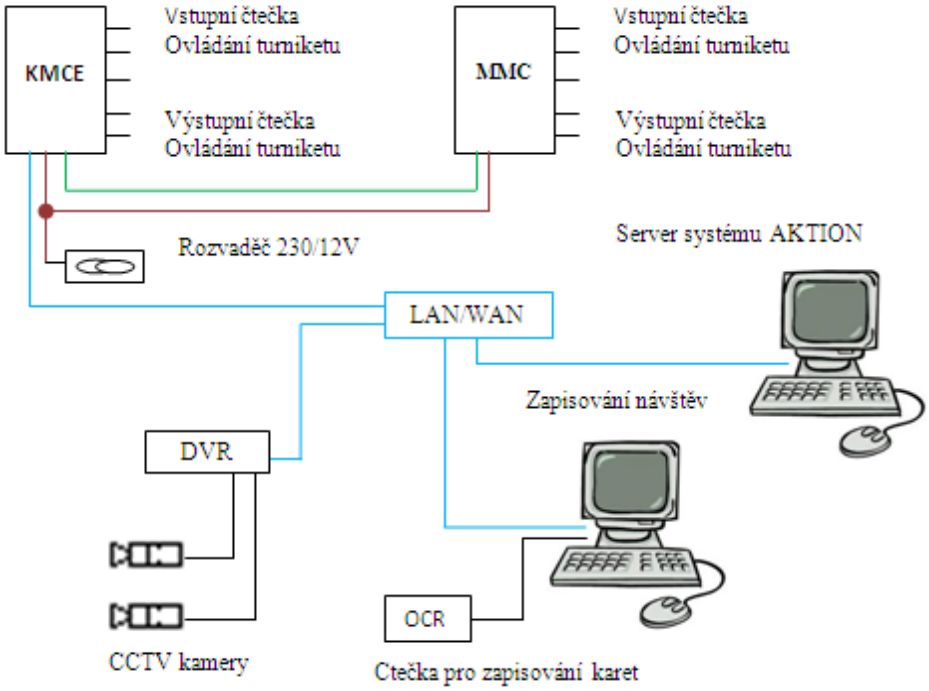
2.1.3 Branky

Součástí vstupního systému je motorická branka na objektu Administrativní budovy, sloužící pro průchod invalidů a pronášení velkých věcí. Branka je ovládaná z recepce objektu a to ve směru požadovaného průchodu.

V rámci zajištění vyšší bezpečnosti celého systému ACS jsou vstupy a výstupy současně monitorovány analogovým kamerovým systémem CCTV.

Bezpečnostní přístupový systém je systémem s tzv. distribuovanou inteligencí**.** Jednotlivá čtecí a ovládací zařízení jsou připojena do vzdálených řídících jednotek KMCE a MMC (kontrolér), které jsou umístěny skrytě v podhledech a u stropu jednotlivých objektů. Vzájemné napojení řídících jednotek na datové linky RS 485 a celá topologie systému kontroly vstupu je znázorněna na blokovém schématu systému kontroly vstupu a evidence docházky. Řídící jednotky mají vlastní paměť a inteligentní procesory, kterými jsou schopny v případě přerušení komunikace s hlavním počítačem ovládat připojená zařízení a uchovat informace o průchodech do doby než bude obnoveno spojení. Schéma definuje i způsob

napájení UPS horizontálních větví a jejich napojení na zálohovací akumulátor, který udržuje v provozu tuto jednotku po stanovenou dobu.



Obr. 1 Blokové schéma přístupového systému

v Administrativní budově.

V objektu jsou použity dva druhy čtecích hlav: skrytá montáž v tělech turniketů a v docházkových terminálech a dále nástěnná montáž na zdech, tělech turniketů a sloupkách.

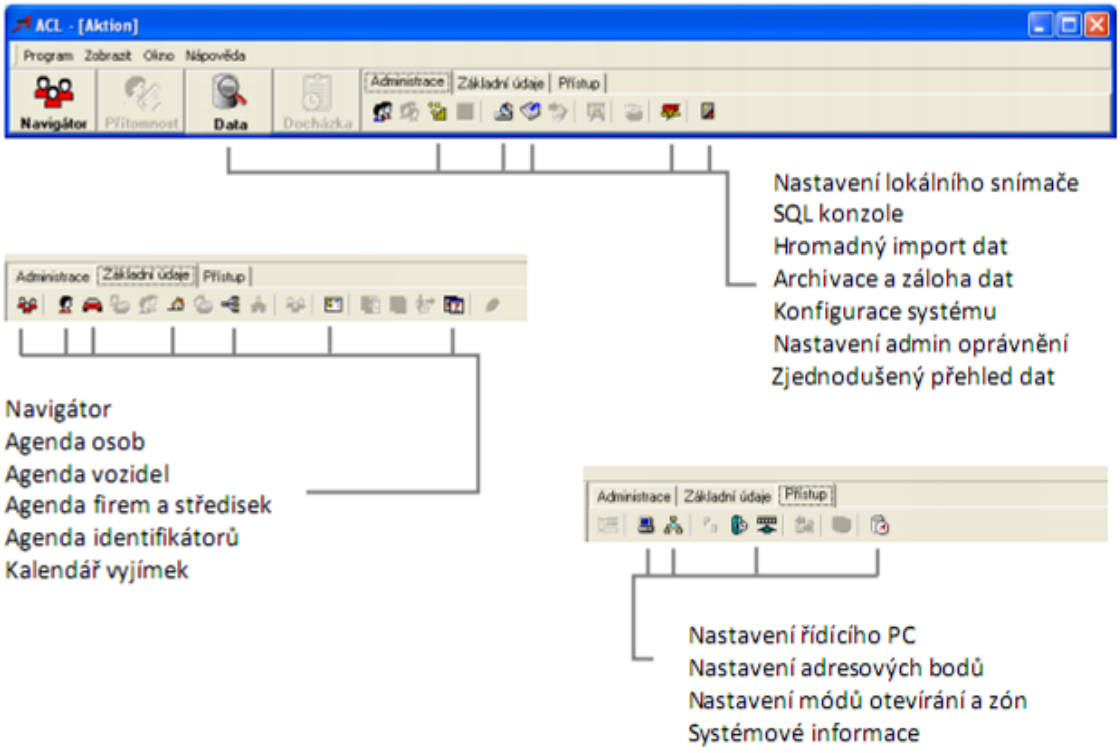
Pro zajištění vracení návštěvních karet je u výstupu z budovy v prostoru turniketů nainstalována lapací čtečka "pohlcovač". Toto zařízení odebere návštěvnickou kartu a teprve poté umožní návštěvě odchod uvolněním turniketu. Zároveň systém zajišťuje monitorování přítomnosti návštěvy, (pohlcovače jsou i na příjezdové a odjezdové bráně).

Celý systém se skládá z těchto prvků:

- řídící centrální počítač s centrálním softwarem,
- systém pro snímání fotografií – fotoaparát, PC, tiskárna karet, osvětlovací technika,
- operátorské terminály,
- elektroniky čtecích zařízení (řídící jednotky KMCE, MMC) s čtecími hlavami pro bezkontaktní vstupní karty, pohlcovače,
- jednotky APR-P20/LEG pro zavádění karet do systému,

- docházkové terminály,
- čtečky pro čtení dat z osobních průkazů,
- elektrické dveřní zárubňové zámky,
- datová a silová kabeláž,
- kabelové přechody,
- zdrojové jednotky se záložní baterií,
- bezkontaktní karty.

Přístupový sytém slouží jako systém zabezpečení pro jeden nebo více vstupů. Vstupem jsou vstupní dveře do budovy, turnikety a vjezdové závory. Skládá se z bezkontaktních snímačů karet, řídících dveřních jednotek (kontrolérů), napájecích zdrojů a externích zařízení (el. zámky, pohony dveří). K nastavení přístupových oprávnění slouží ekonomická verze software Aktion, která obsahuje základní systémové funkce a není omezena celkovým počtem identifikátorů.



Obr. 2 Přehled funkcí SW Aktion, docházkový systém. [5]

Jedná se o sběrnicový systém, jehož základní funkcí je evidování docházky zaměstnanců nebo shromažďují relevantní informace pro mzdovou agendu firmy. Dále je to kontrola

přístupu (dveře, turnikety, závory) a oprávnění osob a vozidel ke vstupu do objektu a jejich pohybu uvnitř nebo částí průmyslového podniku. Vzhledem k tomu, že v rámci přístupového systému je každý zaměstnanec jednoznačně identifikován, jsou data provázány s dalšími funkcemi ACS. Mezi nejčastější provázání je integrace s kamerovým systémem, které jsou instalované u vstupů a vjezdů do areálu firmy.

2.1.4 Docházkový systém

Současná funkce přístupového systému je kontrola docházky. Systém je na všech východech z průmyslového podniku vybaven dotykovým docházkovým terminálem.Při přiložení karty na vstupu do areálu je automaticky zahájena pracovní doba zaměstnance a při odchodu bez udání důvodu je pracovní doba ukončena. Na terminálu je možné po přiložení karty zadat důvod přerušení pracovní činnosti a zároveň je možné zpětné prohlížení pracovního výkazu. Prohlížení a případnou změnu docházky mohou jednotliví zaměstnanci vykonávat i po firemní počítačové síti - na základě přiděleného oprávnění (například mistři atd.)

2.1.5 Umístění prvků napájení zařízení

Pro umisťování prvků platí technické podmínky výrobce. Napájení jednotlivých komponentů systému ACS je zajištěno pomocí napájecích zdrojů, které jsou vybaveny záložním akumulátorem.

2.1.6 Napájení zařízení

Celý systém je napájen ze sítě 230 V/50 Hz. Samostatně jištěný přívod je proveden v rámci elektroinstalace. Zdroje zajišťují převod 230V na bezpečné stejnosměrné napětí 12V.

2.2 Analýza kamerového systému

Kamerový systém (CCTV) je instalovaný na všech vrátnicích, vstupech a vjezdech do areálu a ve vybraných rizikových částech areálu, slouží jako podpora fyzické ostrahy. CCTV je nepřetržitě monitorován z obslužných vrátnic zaměstnanci bezpečnostní firmy, zaměstnanci Hasičského záchranného sboru podniku (dále jen HZSP) z dohledového centra a vybranými zaměstnanci průmyslového podniku vykonávající ochranu společnosti. Provoz CCTV v areálu firmy je plně v souladu se zákonem č. 101/200 Sb.

V areálu průmyslového podniku jsou v systému CCTV použity barevné kamery SANYO VCC pro venkovní použití a SANYO VCC pro vnitřní použití. Všechny kamery mají vysoké rozlišení a vysokou citlivost. Všechny kamery jsou napájeny z externích zdrojů. Všechny venkovní kamery jsou vybaveny odpovídajícím venkovním krytem s krytím IP55, topným tělesem a termostatem. Jejich objektiv je navíc doplněn o funkci automatické DC clony rozšiřující světelný rozsah kamery. Barevné kamery jsou ve vnitřních prostorech s přirozeným či umělým osvětlením.

Kamery jsou instalované na obvodové zdi, na strop místností pomocí držáků a na sloupy veřejného osvětlení. Všechny kamery jsou pevné bez možnosti automatického či manuálního natáčení. Jen u bezobslužné brány pro zaměstnance je na sloupě otočná kamera.

2.2.1 Rozvody a napájení CCTV

Všechny kamery tohoto systému jsou napájeny pomocí externích 12-ti voltových zdrojů.Tyto napájecí zdroje jsou umístěny v jednotlivých technických místnostech nebo v prostorách budovy. Videosignály z kamer jsou přenášeny po koaxiálním kabelu RG 59 B/U s impedancí 75 Ohmů. Tento typ kabelu je použit na všech trasách.

2.2.2 Napájení zařízení

Celý systém je napájen ze sítě 230 V/50 Hz. Samostatně jištěný přívod je proveden v rámci elektroinstalace.

2.2.3 Nahrávání a zálohování dat CCTV

V areálu Průmyslového podniku je na každé vjezdové a vstupní vrátnici digitální videorekordér DEDICATED MICROS s odpovídajícím počtem videovstupů. Do videorekordéru jsou koaxiálním kabelem připojeny příslušné kamery a jsou nahrávány na lokální hard disk DVR. Digitální videorekordér je připojen do lokální počítačové sítě podniku. K systému nejsou připojeny žádné analogové monitory. Sledování, nastavování a vyhledávání záznamů je možné z počítačů v podnikové síti.

U vybraných kamer systému CCTV je možné nahrávání pomocí tzv. videodetektoru pohybu. Tato funkce elektronicky sleduje vymezené oblasti záběru dané kamery (dveře, okna, chodbu apod.) a v případě změny v obraze v této oblasti (= detekování pohybu) se

automaticky spustí nahrávání. Tato funkce šetří záznamovou kapacitu HDD a usnadňuje vyhledávání záznamu. Prohlížení historie záznamu a nastavování lze pouze z počítačů, které mají nainstalovaný NetVu software.

2.3 Analýza poplachového zabezpečovacího a tísňového systému

Poplachové zabezpečovací a tísňové systémy (dále jen PZTS) na chranu budov a zařízení jsou instalovány jen na vybraných a rizikových místech v areálu firmy. PZTS je nepřetržitě monitorován přes dohledové a poplachové přijímací centrum. Monitorování zajišťují zaměstnanci HZSP a zaměstnanci ochrany společnosti průmyslového podniku. Při signalizaci narušení objektu předá zaměstnanec HZSP tuto informaci bezpečnostní službě, která provede:

- výjezd zásahového vozidla BS ke kontrole narušeného objektu,
- v případě fyzického narušení provede opatření k zadržení případného pachatele a opatření ke zmírnění škody,
- zajištění případných svědků a jejich totožnosti,
- zajištění přítomnosti uživatele narušení objektu,
- střežení narušení objektu do příjezdu policie a uživatele. [6]

Vzhledem k tomu, že se v průmyslovém podniku pracuje v nepřetržitém provozu, je PZTS využíván ve skladech a ve vybraných kancelářích. Prvky PZTS jsou napojeny na ústředny Dominus Millenium a ATS, na které jsou připojeny linkové moduly , které zajišťují rozšíření systému (vstupů). Je to stavebnicový systém ústředen, linek a modulů pro stavbu zabezpečovacích systémů v objektech o různé velikosti. Systém je schválen Kriminalistickým ústavem FKP pro objekty s vyššími riziky (2. kategorie) a je způsobilý pro použití k ochraně utajovaných skutečností do a včetně utajení PŘÍSNÉ TAJNÉ (dle zákona č. 412/2005 Sb.). Splňuje ČSN EN 50131-4 (požadavky elektromagnetické kompatibility). PZTS je tak jako EPS a CCTV připojen do softwarové nádstavby C4.

A vše je monitorováno v poplachovém přijímacím centru Hasičského záchranného sboru podniku.

2.4 Instalace technologií a kabeláže

Instalace kabeláže jsou provedeny v souladu s normami ČSN 33 2000[1], ČSN 34 2300[2], ČSN 34 1050[3], ČSN 37 5245[4] a ČSN souvisejících. Kabelové trasy jsou tvořeny PVC lištou LV nebo chráněny PVC trubkami. Trasy jsou vedeny po stěnách povrchově v trubkách nebo lištách. Stoupačky slaboproudých vedení jsou vedeny mezi místnostmi v jednotlivých patrech. Instalace veškerých technologií proběhla podle návodů a pokynů výrobců.

2.5 Napájení a ochrana před nebezpečným dotykovým napětím

Ochrana před úrazem elektrickým proudem je provedena samočinným odpojením od zdroje pomocí jistících prvků, použitím zařízení třídy ochrany II. a malým bezpečným napětím SELV dle ČSN 33 200-4-41. Druhotně je provedena ochrana polohou a zábranou. Prostory instalace technologií jsou projekčně předpokládány jako normální dle ČSN 33 2000–3. Kabelové rozvody slaboproudých systémů jsou slaboproudým vedením malého napětí a z hlediska ochrany před úrazem elektrickým proudem jejich provoz nepředstavuje nebezpečí. Přiměřená ochrana vlastního vedení je zajištěna uložením vedení v instalačních trubkách, lištách a žlabech. Instalované rozvody nezvyšují požární riziko.

[1] Elektrická instalace budov.

[2] Předpisy pro vnitřní rozvody sdělovacích vedení.

[3] Předpisy pro kladení elektrických silových vedení.

[4] Kladení elektrických vedení do stropů a podlach.

Dílčí závěr

V první kapitole praktické části jsem provedl analýzu poplachového systému na modelovém objektu průmyslového podniku. Analýza je zaměřena na stávající stav vybraných prvků poplachového systému jako je přístupový a kamerový systém a poplachový zabezpečovací a tísňový systém. Při posouzení analýzy poplachových systémů jsem dospěl k závěru, že vybrané prvky poplachového systému jsou zaměřeny pouze na prostorovou a plášťovou ochranu. Perimetrická ochrana je řešena přístupovým systémem jen v místech vstupu a vjezdu do areálu. Ve zbývajících místech poplachový systém využíván není, spoléhá se pouze na oplocení lemující celý areál. Protože se, ale jedná o velký areál, kde díky velkému množství budov vznikají slabá místa, která jsou vhodná pro narušitele či lupiče, musí být prioritou vytvoření stoprocentní perimetrické ochrany za použití poplachových systémů.

3 VYMEZENÍ OBLASTÍ PRO OPTIMALIZACI A DOPLNĚNÍ POPLACHOVÝCH APLIKACÍ

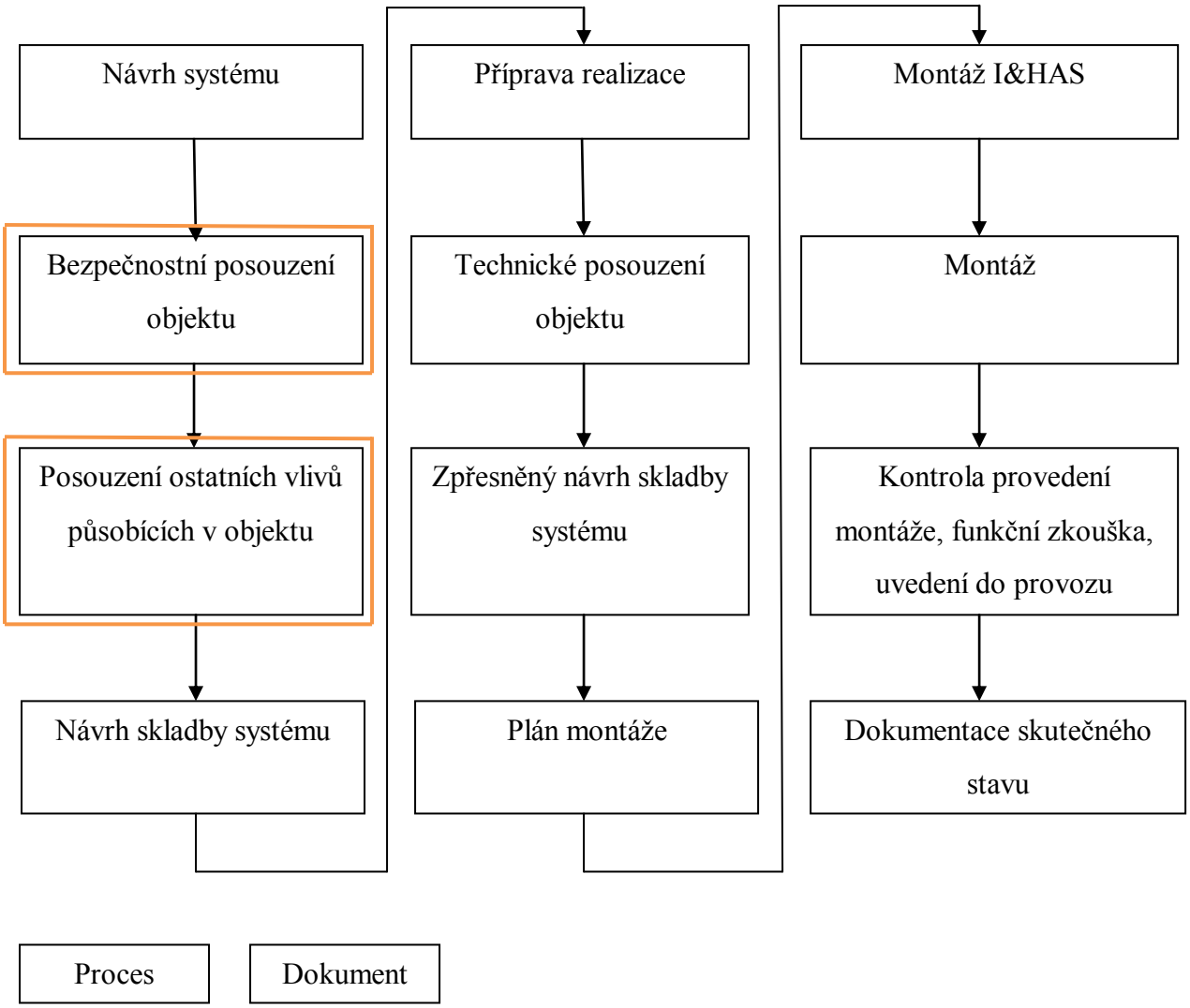
Vymezení oblastí průmyslového podniku pro optimalizaci a doplnění poplachových aplikací je nezbytné u objektů, které jsou z pohledu bezpečnosti rizikové a zájmové pro potenciálního lupiče nebo narušitele. Základním kritériem projektanta poplachových systémů jsou význam a povaha chráněného objektu, stavební struktura objektu, hodnota majetku uvnitř objektu, míra rizika vniknutí a další faktory, které mohou ovlivnit výběr stupně a složení poplachového systému. Na základě těchto skutečností určuje projektant potřebný počet stupňů ochranných bariér, a to jak mechanických zábranných systémů, tak poplachových systémů. [7]

3.1 Vymezení legislativního rámce bezpečnostního posouzení

Vymezení legislativního rámce bezpečnostního posouzení a zhodnocení jeho současného postavení v problematice návrhu poplachových systémů (dále jen PS). Bezpečnostní posouzení má, jako každý z kroků zřizování PS svůj legislativní základ stanoven technickými normami. Jelikož je výstup bezpečnostního posouzení, nebo také zápis o jeho provedení důležitým dokumentem pro pojišťovny, je samotné bezpečnostní posouzení blíže specifikováno taktéž ve směrnicích České asociace pojišťoven. Z výše uvedeného tedy vyplývá, že legislativní rámec bezpečnostního posouzení je v ČR specifikován pro PS především normami ČSN EN 50131-1 ed.2[5], TNI 33 4591-1 a směrnicemi ČAP.

Podle ČSN EN 50131-1 ed.2 a TNI 33 4591-1 je bezpečnostní posouzení považováno za dílčí krok v procesu tvorby návrhu PS. Cílem bezpečnostního posouzení je zjistit do jaké míry je třeba objekt zabezpečit a za pomocí jakých komponentů toto zabezpečení realizovat, při respektování pokud možno všech faktorů ovlivňujících jejich správnou funkci. [3]

[5] (334591) Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky.



Obr. 3 Znázornění místa bezpečnostního posouzení v procesu návrhu poplachového systému. [3]

3.2 Identifikace potencionálních hrozeb

Identifikace potenciálních hrozeb se určuje z bezpečnostního posouzení. Potenciální hrozby je důležité znát pro návrh systému ochrany. Bezpečnostní posouzení rozdělujeme na několik částí, které jsou vysvětleny dále v kapitole.

3.2.1 Bezpečnostní posouzení - zabezpečované hodnoty

Je nutné provést posouzení objektů, které mají být střeženy, s cílem stanovit nezbytnou úroveň systému zabezpečení. Před zpracováním systémového návrhu je nutno posoudit rozsah a charakter majetku vystavený ve střežených objektech nebezpečí.

Při zpracování návrhu poplachového systému by měl bezpečnostní analytik navrhnout použití takového spektra a rozsahu komponentů, aby odpovídal míře rizika vloupání do střežených objektů. Míra rizika závisí, kromě jiného na charakteru střeženého objektu. V této souvislosti by měly být brány v úvahu následující faktory: [3]

Tab. 1 Zabezpečované hodnoty. [8]

Okruh zkoumání (aspekt)	**Charakteristika**
Druh majetku	• snadno postradatelný • atraktivní pro lupiče
Hodnota majetku	• maximální pravděpodobná hodnota přímé ztráty • následné výdaje související se ztrátou • hodnota obliby
Objem nebo velikost	• snadno zcizitelné a přepravitelné • tržně atraktivní
Historie krádeží	• četnost přecházejících krádeží
Nebezpečí	• pro okolní prostředí • zneužití střeženého majetku
Poškození	• vandalismus na střeženém majetku • riziko žhářství na střeženém majetku

Obecně je možné říci, že z hlediska zabezpečení majetku je nutno chránit především prostory obsahující následující aktiva:

- velké hotovosti (např. pokladny),
- velké hodnoty (např. sklady drahých kovů),

- hodnoty, jejichž ztráta vážně naruší provoz organizace (např. technologická zařízení),
- zařízení objektu do kategorie s utajovanými informacemi,
- s umístěním látek, jejichž havárie může znamenat vážnou mimořádnou událost (např. ropné látky, chemikálie, výbušniny). [8]

3.2.2 Bezpečnostní posouzení – budova

Při posuzovaní hlavních rizik objektu bude hlavním určujícím faktorem fyzická struktůra střežených objektů. Cílem obhlídky je identifikace slabých mist objektu. Faktory, které je přitom nutno posoudit, jsou uvedeny v tabulce.

Tab. 2 Stavební provedení objektu. [8]

Okruh zkoumání	**Charakteristika**
Konstrukce	• konstrukce stěn, střech, podlach a sklepení
Stavební otvory	• konstrukce oken, dveří, střešních světlíků, ventilačních kanálů a ostatních otevíraných částí budovy, které mohou usnadnit nepovolený vstup
Režim provozu objektu	• dlouhodobá neosídlenost objektu • přítomnost pracovníků ochrany • přístup veřejnosti
Držitelé klíčů	• osažitelnost držitelů klíčů od objektu
Umístění objektu (lokalita)	• umístění v oblasti s vysokým rizikem kriminality • sousední budovy nebo stavby, které by mohly usnadnit vloupání • rychlost a kvalita předpokládaného zásahu • vzdálenost a ostatní skutečnosti týkajících se sousedních obydlených objektů
Stávající zabezpečení	• kvalita a rozsah jakýchkoliv stávajících MZS • kvalita a rozsah stávajícího technického zabezpečení PS
Historie krádeží	• způsoby vloupání při předcházejících krádežích
Místní legislativa a předpisy	• bezpečnostní požadavky, které mohou ovlivnit návrh • požární předpisy • konstrukce budov
Okolí objektu	• městská zástavba • samota

3.2.3 Odhad možných rizik

Na základě předcházející analýzy je nutno ohodnotit všechna možná nebezpečí a zvážit celkové riziko dané kombinací faktorů vztahujících se ke střeženému majetku (potenciální nebezpečí) a faktorů vztahujících se k fyzické podstatě objektu (slabá místa). Úkolem hodnocení možných rizik je stanovit úroveň rizika, není-li možné nebezpečí v objektu zcela eliminovat a sejde-li se faktor potenciálního nebezpečí s faktorem slabých míst. Riziková analýza určuje rovnováhu nebezpečí odpovídající pravděpodobnost, jež je dána četností a rozsahem možných škod.

Pravděpodobnost vzniku se nechá odvodit z analýzy nebezpečí ohodnocením možných scénářů událostí. Ty jsou dány atraktivitou objektu pro lupiče, náklady na přípravu a provedení trestného činu a v neposlední řadě rizikem lupiče. [8]

3.2.4 Stanovení potřebného stupně zabezpečení objektu

Objekty s vyššími riziky jsou objekty, u nichž je vyšší pravděpodobnost napadení nezávislá na výši finančního ohodnocení. Stupně zabezpečení stanovujeme dle ČSN EN 50131-1 ed.2. [8]

3.2.5 Bezpečnostní posouzení – vlivy působící na poplachové systémy mající původ ve střežených objektech

Ve střežených objektech existuje celá řada faktorů, které mohou ovlivnit funkci PS a vyvolávat plané poplachy. Tyto faktory je nutné vzít v úvahu při volbě typů komponentů PS (zejména prvků PZTS detektorů narušení), jejich umístění i nastavení. Faktory mající původ uvnitř střežených objektů, mohou být ovlivněny i ze strany uživatelů objektu. V takovém případě je nutno zajistit bezchybný chod komponentů jistými režimovými opatřeními. Mezi nejpravděpodobnější vnitřní vlivy, způsobující plané poplachy patří:

- vodovodní potrubí,
- vytápění, vzduchotechnické a klimatizační systémy,
- vývěsní štíty nebo závěsné předměty,
- výtahy,
- zdroje světla,

- elektromagnetické rušení,
- vnější zvuky,
- průvan,
- uspořádání skladových předmětů,
- stavební konstrukce střežených objektů, zvláštní pozornost, riziko planých poplachů. [8]

3.2.6 Bezpečnostní posouzení – vlivy působící na poplachové systémy, mající původ vně střežených objektů

Za vlivy působící na objekt z jeho okolí považujeme ty, které směřují k objektu z vnějšku a nemůžeme je nijak ovlivnit. Současně musíme zhodnotit jejich vliv, jelikož by mohly mít neblahý dopad na funkci zařízení PS. Pro dosažení funkčního modelu zabezpečení je tedy nutné veškeré tyto vlivy specifikovat a rozmístění a volbu detektorů jim přizpůsobit. I z toho důvodu je doporučováno věnovat pozornost těmto faktorům:

- dlouhodobě působící faktory (silnice, železnice, parkoviště),
- krátkodobě působící faktory (okolní výstavba),
- vlivy počasí (silné větry, blesky, silné deště),
- vysokofrekvenční rušení (vysílače veřejné sítě nebo TV, stanice GSM),
- sousední objekty (těžké stroje mohou způsobovat vibrace),
- vlivy klimatických podmínek (využívat taková zařízení, která vyhovují příslušným klimatickým podmínkám). [8]

3.3 Modelový objekt - průmyslový podnik

Areál daného průmyslového podniku se skládá z několikati výrobních hal a prostorů, které musí být otevřené z důvodu nutného pohybu zaměstnanců přepravujících materiál nebo pro pracovníky externích firem vykonávající činnosti související z výrobou a provozem.

3.3.1 Analýza možných nebezpečí

Nejdříve musíme zvážit proti komu nebo před čím je nutné průmyslový podnik, objekt respektive předmět ochrany chránit. Jde tedy o přesné stanovení zdrojů nebezpečí pro

chráněný objekt. Je nutné si uvědomit, že poplachový systém působí jak v prostoru, tak i v určitých časových relacích, závislých na provozním režimu v objektu. [7]

Při návrhu poplachového systému je nutné zvážit i určité rozdíly, které vyplívají ze skutečnosti, že některé objekty budou chráněny pouze proti napadení lupičem nebo narušitelem "zvnějšku" a u ostatních objektů bude nutné zajistit ochranu i před napadením "zevnitř" objektu. Z tohoto důvodu je vhodné rozdělit obecný soubor nebezpečí, která mohou různým způsobem poškodit chráněný zájem na :

- vnější nebezpečí,
- vnitřní nebezpečí.

3.3.1.1 Vnější nebezpečí

Vnější nebezpečí pro chráněný objekt v průmyslovém podniku představuje u poplachových systemů proti krádežím, vloupáním, narušitel nebo lupič snažící se vniknout do objektu. Jestliže má PS plnit i další funkce (např. chránit před sabotáží) může být vnějším nebezpečím i událost nebo jev, jejichž příčina spočívá např. v nedbalostním jednání, jehož důsledky mohou být stejné jako při úmyslném jednání. Proto je nutné při bezpečnostní analýze u zvlášť důležitých objektů prozkoumat z bezpečnostního hledisek i jeho okolí.

Analýzu vnějších vlivů, které by se mohly za určitých podmínek stát vnějším nebezpečím, je nutné provádět zejména u objektů, jejichž poškozením by došlo k mimořádné události většího rozsahu (např. chemické provozy). [7]

3.3.1.2 Vnitřní nebezpečí

Vnitřní nebezpečí lze obecně rozdělit na úmyslné a neúmyslné, tj. nedbalostní jednání, jejichž důsledky však mohou být pro chráněné zájmy stejné:

- u úmyslných jednání (jde především o rozkrádání majetku nebo ochrana utajovaných informací),
- u nedbalostních jednání (v jejichž důsledku může dojít ke vzniku požáru, výbuchu nebo provozní havárii). [7]

3.3.2 Bezpečnostní opatření v modelovém objektu

Účinnost bezpečnostních opatření můžeme chápat jako schopnost eliminovat vznik rizik, případně následků rizik. V praxi jsme tyto zásadní požadavky nuceni korigovat v důsledku objektivních a subjektivních bariér, jako jsou např. ekonomická dostupnost, technická realizovatelnost, legislativní podmínky, sociální a psychologické podmínky apod. Všechny tyto bariéry sice účinnost bezpečnostních opatření snižují, a je třeba je brát jako fakt, avšak vhodným přístupem k řešení problémů zabezpečení objektů s vysokým rizikem napadení a vhodnou kombinací dostupných bezpečnostních opatření lze dosáhnout velmi uspokojivých výsledků. Zabezpečení objektů s vysokým stupněm rizika by mělo plnit především následující funkce:

- odradit pachatele od úmyslu proniknout do objektu,
- znemožnit pachateli vniknout do chráněného objektu nebo alespoň toto vniknutí výrazně zpomalit a ztížit mu postup,
- donutit pachatele k zanechání stop při proniknutí do objektu,
- vyvolat poplach a zajistit včasný přenos této informace ke složkám, které provedou zásah a dopadení pachatele při činu,
- zadokumentovat vniknutí pachatele do objektu a jeho pohyb v něm. [2]

Dále je nutné posoudit stávající způsob zabezpečení objektu, a to včetně posouzení režimových opatření, zejména na organizaci vstupu osob do objektu a jejich pohybu vněm. Pro ohodnocení a popsání rizika je dále důležité i to, co je v objektu chráněno.

V objektech s uskladněnými hořlavinami budeme navíc od poplachového systému vyžadovat, aby elektrické části zařízení byly zajištěny proti způsobení elektrického zkratu, který by byl příčinou výbuchu. [2]

3.4 Riziková místa v modelovém objektu

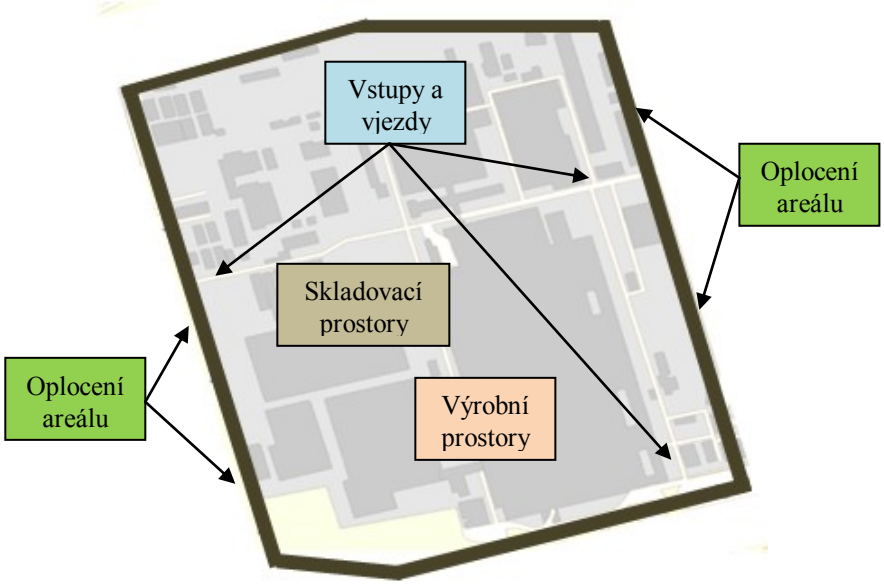
V kapitole (3.4) vymezuji riziková místa. U jednotlivých rizikových míst, jako jsou skladovací prostory, sklady chemikálií a PHM, výrobní prostory s technologickým zařízením, administrativní budova a jiné budovy patřící firmám vykonávající činnost pro průmyslový podnik, jsem uvedl možné varianty poplachového systému a jeho prvky.

Na areál průmyslového podniku je vypracován na základě příslušných ustanovení Evropské dohody o mezinárodní silniční přepravě nebezpečných věcí (ADR) zveřejněné ve Sbírce mezinárodních smluv a na základě příslušných ustanovení Řádu pro mezinárodní železniční přepravu nebezpečných věcí (RID) bezpečnostní plán. Úkolem bezpečnostního plánu je zvýšení bezpečnosti při nakládání s nebezpečnými věcmi, především omezení rizik vzniku škod v areálu firmy, zneužitím vysoce rizikových věcí, v konkrétním případě automobilových benzínů, technického benzínu a LPG. Modelový podnik je zaměřen na gumárenskou činnost a přijímá i věci, které jsou zařazené jako nebezpečné podle zákona 356/2003 Sb. o chemických přípravcích, a také podle Evropské dohody klasifikovaných dle ADR/RID. [6]

3.4.1 Perimetrická ochrana

Areál modulového podniku je v současné době chráněn perimetrickou ochranou, která je provedena oplocením kolem celého obvodu areálu. V určitých místech jsou vjezdové a výjezdové brány, vstupy a výstupy do objektu podniku. V těchto prostorech je použit poplachový systém CCTV a ACS. V dalších částech oplocení objektu poplachový systém již není využíván, tyto místa jsou pouze kontrolována bezpečnostní službou, a to v daných intervalech.

Oplocení je systém, který se skládá z panelů různých výšek upevňovaných na pravoúhlé EL sloupky, čtyřhranné sloupky nebo sloupky Bekafix či Bekafast pomocí zvláštního upevňovacího systému. Panely s těžkou svařovanou sítí s obdélníkovými oky a vodorovnými výztuhovými dráty jsou zárukou velmi vysokého stupně odolnosti.



Obr. 4 Areál modelového podniku.

3.4.1.1 Poplachové prvky pro perimetrickou ochranu

Zde jsou uvedeny vhodné poplachové prvky na zabezpeční perimetrické ochrany a některé z nich jsou použity v návrhu systému perimetrické ochrany průmyslového podniku.

Detektory pro perimetrickou ochranu

Jsou to detektory, které chrání, respektivě signalizují narušení vnějších částí u rozlehlých objektů, komplexů budov nebo průmyslových podniků. Venkovní detektory a detekční systémy jsou klasifikovány podle hlavních kritérií.

Pasivní detektor – jedná se například o pasivní infračervené detektory, seismické nebo magnetické detektory, plotové detekční systémy nebo digitální detektory pohybu.

Aktivní detektor – jedna se například o mikrovlnné detektory a bariéry, aktivní infračervené závory a systémy na bázi elektromagnetického pole (např. systémy se štěrbinovými kabely).

Detektory s přímou viditelností - mezi tyto detektory patří například mikrovlnné detektory a bariéry, aktivní a pasivní detektory.

Detektory sledující terén – mezi tyto detektory patří systémy se štěrbinovými kabely, signální stěny, plotové systémy kapacitní a s mikrofonními kabely.

Prostorové detektory – příkladem prostorových detektorů mohou být mikrovlnné a aktivní nebo pasivní infračervené detektory, systémy na bázi elektrického pole, digitální detektory pohybu nebo systémy se štěrbinovými kabely.

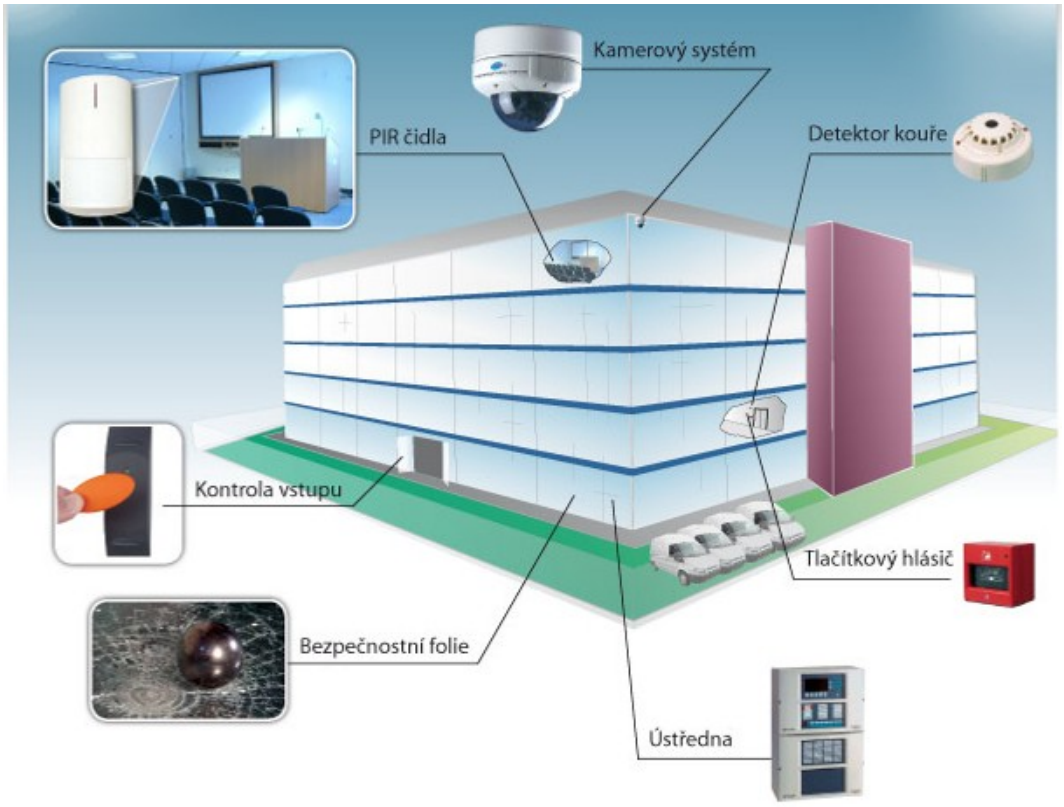
Liniové detektory – takovým detektorem může být například systém s mikrofonními kabely nebo signální stěna. V objektech s vyššími riziky se většinou používá vice prostorově rozložených komplementárních detektorů, zvláště pokud je jeden z nich liniový. [4]

Cílem perimetrické ochrany je především odstrašení, odhalení a zpoždění narušitele. Perimetrická ochrana by měla signalizovat narušení obvodu objektu. Detektory narušení, použité v rámci perimetrické ochrany, mají obvykle delší dosah a užší detekční charakteristiku, musí splňovat požadavky vyšší klimatické odolnosti a být odolné vůči planým poplachům. Vzhledem k různorodosti vnějšího venkovního prostředí i široké škále pohybujících se objektů bývá odolnost vůči planým poplachům problematickou. [3]

Výběr vhodné variant střežení perimetru tedy musí vycházet z důkladné znalosti zabezpečovaného objektu. Podněty, které se svým charakterem přibližují situaci narušení, nelze nikdy zcela eliminovat. Nejen z tohoto důvodu se často kombinuje systém venkovní perimetrické ochrany s kamerovým systémem CCTV. [8]

3.4.2 Skladovací prostory

Modelový podniky je vybaven většími či menšími, jak sklady pro uskladnění vstupních surovin a technických dílů, tak sklady pro uskladnění svých finálních výrobků. Skladovací prostory jsou tedy rizikovým místem a musí být důkladně zabezpečeny poplachovým systémem, tak aby nedošlo k jakémukoliv narušení bezpečnosti (z vnitřní nebo ze vnější strany) těchto objektů. Ve skladovacích prostorech se nejčastěji používají kombinace poplachových prvků, které reagují na veškeré nežádoucí podněty.



Obr. 5 Poplachové prvky ve skladech. [9]

3.4.2.1 Poplachové prvky pro skladovací prostory

Pro zabezpečení skladů využíváme převážně poplachové zabezpečovací a tísňové systémy, které kombinujeme s kamerovými a přístupovými systémy

Dále jsou uvedeny poplachové zabezpečovací a tísňové prvky, které nám zajistí pláštovou, prostorovou i předmětovou ochranu.

Prvky plášťové ochrany:

- magnetické kontakty,
- detektory na ochranu prosklených ploch,
- mechanické kontakty,
- poplachové fólie, tapety, polepy a poplachová skla,
- drátové detektory,
- rozpěrné tyče.

Prvky prostorové ochrany:

- pasivní infračervené detektory,
- aktivní infračervené detektory,
- ultrazvukové detektory,
- mikrovlnné detektory,
- kombinované duální detektory.

Prvky předmětové ochrany:

- otřesové detektory,
- detektory na ochranu zavěšených předmětů
- kapacitní detektory. [8]

Těžištěm prostorové ochrany jsou centrální body budovy – schodišťové přístupy či výstupy, haly, spojovací chodby a vnitřní komunikační uzly. Díky nižší náročnosti na montáž mnohdy supluje prostorová ochrana ochranu plášťovou. V odůvodněných případech, zvláště v objektech s vysokými riziky napadení a při umístění detektorů v takových místech, aby skutečně pokrývala nejpravděpodobnější místa vniknutí narušitele nebo lupiče z vnitřní strany pláště budovy, lze tento především ekonomický argument připustit. Nahradit plášťovou ochranu však nikdy nemůže, neboť plášťová ochrana je na rozdíl od ochrany prostorové schopna detekovat vniknutí lupiče s minimální časovou prodlevou. Zůstává pak delší čas na zásah bezpečnostní službou. [8]

3.4.3 Sklady chemikálií a PHM

Sklady chemikálií jsou objekty s vysokým rizikem napadení a lze je charakterizovat jako objekty, u nichž je výrazně vyšší předpoklad vzniku rizikové situace a následně i vzniku škod na majetku, na zdraví či životech lidí nebo u nichž v důsledku vzniku rizikové situace dojde k poškození, zničení, zneužití nebo ztrátě dat a informací významného charakteru, která se projeví vysokou škodou.

Pro všechny je však společné to, že riziko jejich napadení je buď zjevně vyšší než u objektů ostatních, nebo škoda vzniklá v důsledku havárie může být značně vysoká. Rizika, která u těchto objektů přicházejí v úvahu, jsou různorodá od úmyslného útoku na chráněný předmět

přes nedbalostní jednání až po živelné katastrofy nezávislé na vůli člověka. Také prostředky ochrany před vzniklými riziky jsou různorodé od technického zabezpečení prostřednictvím poplachových systémů, mechanických zábranných systémů, režimová opatření či pojistné smlouvy. Smyslem nasazení těchto prostředků je eliminovat nebo alespoň minimalizovat rizika, kterým může být předmětný objekt vystaven. [2]

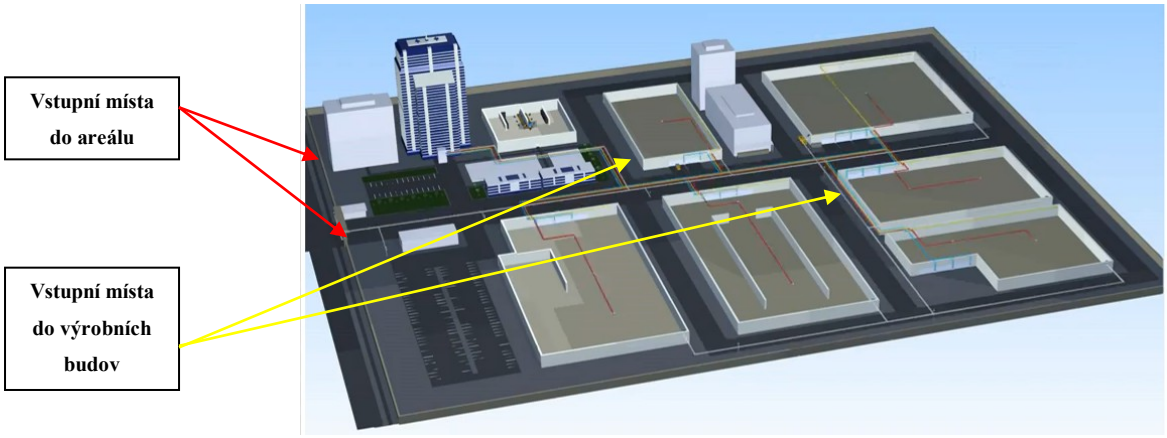
Dále uvádím příklad možných prvků PZTS na zabezpečení skladů pro chemikálií a pohoné hmoty a maziva (dále jen PHM). Poplachové prvky PZTS se v těchto rizikových prostorech kombinují s prvky elektrické požární signalizace EPS.

3.4.3.1 Poplachové prvky pro sklady chemikálií a PHM

Duální detektory kombinující PIR a MW detekci se používají do vyloženě problematických prostor s vysokým nárokem na odolnost proti falešným poplachům. PIR detektor snímá teplo a zajišťuje aby předmět na který bude vyhlášen poplach byl teplý, MW detektor snímá pohyb a zajišťuje aby předmět, na který bude vyhlášen poplach byl hmotný a v pohybu. Tímto způsobem se velmi účinně eliminuje například vliv teplého vzduchu, který dokáže narušit PIR detektor, ale MW složku neaktivuje.

3.4.4 Výrobní prostory

Vzhledem k tomu, že se přístupový systém v kombinaci s docházkovým nachází na dvou hlavních vstupech do komplexu, dochází k tomu, že se pracovní doba zaměstnanců začíná počítat již průchodem jednoho z těchto dvou vstupů. Přičemž se nezohledňuje vzdálenost těchto vstupů k jednotlivým výrobním provozům. Což způsobuje rozdílné doby potřebné k překlenutí těchto vzdáleností, nemožné kontrole a eventuálnímu zneužívání. Z těchto důvodů by bylo efektivnější umístit přístupový systém ve formě docházkového terminálu u vstupů do jednotlivých výrobních budov. Na obou zmiňovaných hlavních vstupech do komplexu, by byla použita jen základní varianta přístupového systému umožňující jen přístup a odchod. Výhoda systému je, že máme přehled o přesném počtu kmenových zaměstnanců na jednotlivých výrobních provozů a docházka zaměstnancům se počítá až při vstupu na pracoviště.

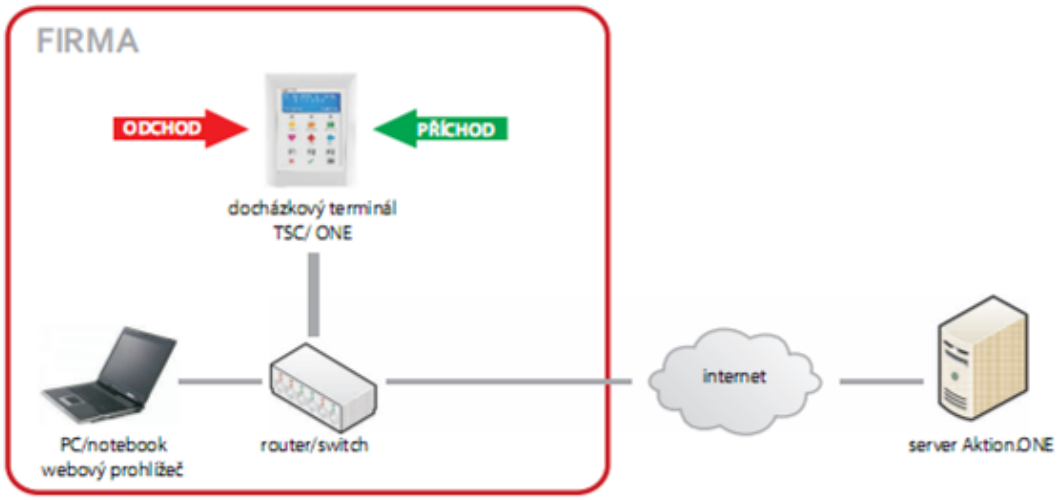


Obr. 6 Příklad rozmístění výrobních prostorů. [5]

3.4.4.1 Přístupový systém pro výrobní prostory

Docházkový systém urychluje a zpřesňuje evidenci docházky zaměstnanců a sleduje aktuální přítomnost osob na pracovišti. Umožňuje automatické převody dat do informačních, personálních, mzdových a výrobních programů. [5]

Dále je uvedeno blokové schéma docházkového systému, který by byl vhodný instalovat u vstupů jednotlivých výrobních budov. Docházkový systém by byl pouze pro kmenové zaměstnance výrobního provozu, a pro jiné zaměstnance vykonávající činnost dodavatelským způsobem by neplatil.

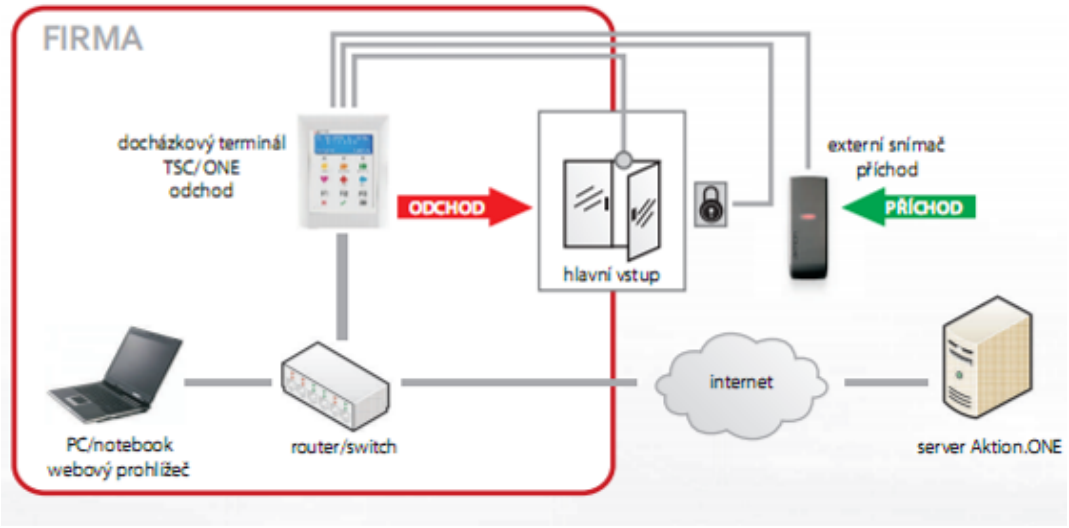


Obr. 7 Docházkový terminál, návrh přístupového systému. [5]

3.4.5 Energo rozvodny

Energo rozvodny jsou rizikovými místy v průmyslovém podniku, kde může dojít jak k úmyslné nebo neúmyslné chybě, která znamená pro průmyslový podnik ohrožení části nebo celého výrobního provozu. Dnešní využití přístupových systémů je výhodné jak z pohledu identifikace přístupu do prostoru rozvodny, tak i sledování času práce na konkrétním úkolu. Nynější zabezpečení pouze uzamykacím klíčovým systémem je nedostačující (při ztrátě, klíč může použít kdokoliv). Dále jsou uvedeny dvě varianty možného řešení.

3.4.5.1 Přístupový systém pro energo rozvodny



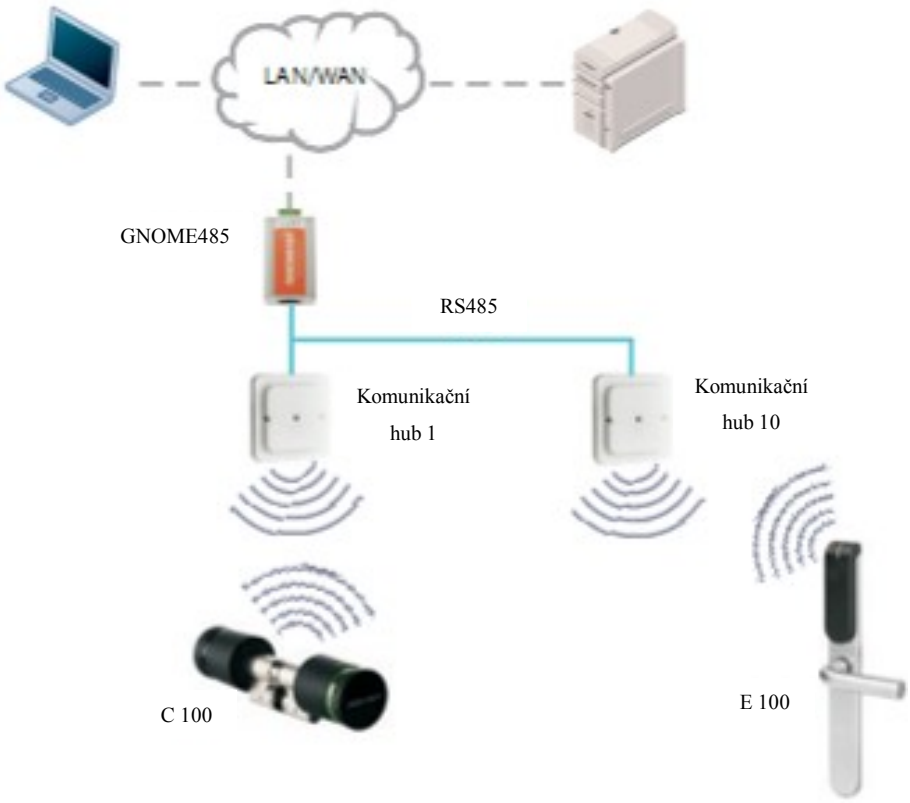
Obr. 8 Docházkový terminál rozšířený o ovládání dveří, návrh přístupového systému. [5]

Další možnou variantou je použití bezdratových zámků.

Bezdrátová cylindrická vložka s integrovanou bezkontaktní čtečkou a on-line komunikací s nadřízeným GNOME485 systémem kontroly vstupů. Vytvoření bodů v rámci stávajícího nebo nově realizovaného systému bez nutnosti použití kabelů ke vstupním dveřím. Kompaktní pro všechny zadlabávací zámky a kování. Komunikační Hub pro bezdrátové spojení s vložkou a propojení s PC prostřednictvím RS485[6].

[6] Průmyslová komunikace, umožňuje vytvoření dvouvodičového poloduplexního vícebodového sériového spoje.

Obr. 9 Bezdrátový zámek. [5]



Obr. 10 Bezdrátové zámky. [5]

3.4.6 Monitorování hlavních pozemních komunikací

Nynější provedení analogového kamerového systému (CCTV), které je instalováno na všech vrátnicích, vstupech a vjezdech do areálu, je zastaralé a mělo by být nahrazeno moderními IP kamerami, které svojí kvalitou, přístupností a jednoduchostí umožňují lepší záznam. Sledování hlavních pozemních komunikací IP kamerovými systémy, které by sloužilo

především k monitorování aktuální obecné a dopravní situace a zároveň mělo odstrašující efekt pro případné narušitele.

Kamerový systém slouží jako funkce přehledová a informační, protože počet členů bezpečnostní služby není obvykle velký a je nutné reagovat např. na příjezdy vozidel a jiné standardní provozní záležitosti. V průmyslových objektech ještě občas přistupuje funkce monitoringu např. výroby, kdy je sledován určitý výrobní postup nebo záznam expedovaných beden apod.

3.4.6.1 Možnosti kamerových systémů

Bezpečnostní kamery monitorující určitý zájmový prostor bývají obvykle kamery pevné. To umožňuje buď kontinuální záznam, nebo možnost aktivace detekce pohybu v daném prostoru. Doplňkem mohou být kamery pohyblivé. Jejich výhodou je, že ve spojení s ovládaným objektivem s proměnlivou ohniskovou vzdáleností („zoom" objektiv) umožňují obsluze prohlížet velké plochy a zobrazit potřebné detaily. Nevýhodou samozřejmě může být skutečnost, že nelze zaručit, aby pohyblivá kamera sledovala prostor právě tam, kde se něco děje. Tyto kamery v provedení „dome" (kompaktní kamera s integrovaným pohonem i řízeným objektivem ve vhodném krytu) jsou výborným pomocníkem. Pokud počítáme s nočním záznamem videosignálu s IR přisvětlením, je vhodné volit kamery i objektivy přizpůsobené pro tento přísvit. Kameru lze propojit s PZTS a v době poplachu se může automaticky natočit na místo poplachu. [10]

Pro zvláštní účely (snímání technologických procesů, snímání RZ vjíždějících a odjíždějících vozidel, sledování terénních koridorů ve dne i v noci, pro práci v provozech s vysokými hodnotami vlhkosti a teploty, apod.) lze navrhnout řadu speciálních kamer různého provedení.

Zvláštními jsou systémy s analogovým přenosem signálu. Jsou to klasické kamerové systémy s koaxiálními kabely. O analogovém přenosu se zde zmiňuji proto, že zpracování signálu v kameře a záznamy na TV rekordérech jsou dnes zcela běžně digitální a záznamy lze prohlížet běžně z PC pracovišť LAN sítě pomocí systémového programového vybavení.

Další možností využívanou v komerčních a průmyslových objektech jsou IP kamerové systémy. Zde probíhá přenos v datové podobě kompatibilní s LAN sítěmi. Vlastní kamera

má vlastní IP adresu a je zapojena do LAN sítě a do sítě musí být připojeno i záznamové zařízení. Možností zpracování a ukládání signálu je zde, stejně jako u klasických kamerových systémů mnoho.

Výhodou IP systémů je, že při několika požadovaných standardních IP kamerách lze využít stávající LAN[7] sítě a ušetřit na nových rozvodech. Navíc je možné kamery přemísťovat mezi volnými zásuvkami (při zajištění napájení). U větších systémů už je ale nutné pečlivě zvážit datové toky od jednotlivých kamer a prudce roste pravděpodobnost toho, že bude nutné vybudovat vlastní síť pro kamerový systém a pečlivě navrhovat servery pro zpracování a záznam snímků. IP kamery mají lepší kvalitu obrazu – rozlišení. Tím pádem potřebují větší kapacitu uložiště (HDD). [10]

Dílčí závěr

V další části Diplomové práce jsem vymezil rizikové oblasti a doplnil poplachové aplikace na základě bezpečnostního posouzení a analýzy stávajícího stavu. U jednotlivých rizikových míst jako jsou skladovací prostory, výrobní prostory, energo rozvodny a hlavní pozemní komunikace, jsem navrhl možnosti použití poplachového systému a jeho prvků, které lze aplikovat a které povedou ke zkvalitnění stávající ochrany.

[7]Zkratka LAN znamená Local Area Network a je to jedna z několika dalších druhů počítačových sítí určena pouze pro jednu budovu nebo celou firmu.

4 INTEGRACE POPLACHOVÝCH A NEPOPLACHOVÝCH APLIKACÍ

Na základě analýzy a bezpečnostního posouzení jsem vymezil oblasti pro optimalizaci, u kterých je nezbytný komplexní přístup k řešení problémů spojených s ochranou na modulovém objektu. Komplexní přístup a vhodná kombinace použitých poplachových systémů přináší integrovaný bezpečnostní systém, který umožní eliminovat nebo alespoň výrazně minimalizovat rizika, která objektu hrozí. Jestliže má být totiž zabezpečení opravdu účinné, budou opatření aplikována nejen na zabezpečení samotného objektu, ale i na chod celého průmyslového podniku.

Důležité je si uvědomit, že budování integrovaného bezpečnostního systému není nezbytně určeno jen pro objekty s vysokým rizikem napadení, ale je to i cesta pro zabezpečení konkrétního modulového objektu.. Cílem a účelem těchto bezpečnostních systémů není nic jiného, než nám již známa snaha ochránit majetek, zájmy firmy a její pracovníky před možnou škodou. Komplexní přístup k bezpečnostnímu řešení představuje proces, na jehož začátku je sběr informací vztahující se k dané problematice, definování bezpečnostní strategie, bezpečnostní politiky a informační strategie společnosti jako součásti celkové strategie firmy, jejich důkladná analýza a na konci pak fungující integrovaný bezpečnostní systém firmy. Ten ochraňuje organizaci, jednotlivé a její oblasti aktivit, její majetkové hodnoty a zájmy i jednotlivé zaměstnance před vnějšími i vnitřními hrozbami. [2]

Integrace poplachových a nepoplachových systémů je potřeba brát jako investici do budoucna. Počáteční náklady se postupně vrátí (například snížením počtu pracovníků fyzické ochrany atd).

4.1 Definice

Poplachová aplikace – aplikace určená na ochranu života, majetku nebo prostředí, jako jsou:

- poplachový zabezpečovací a tísňový systém (PZTS),
- uzavřené televizní okruhy používané pro účely zabezpečení a dohledu (CCTV),
- přístupové systémy (ACS). [11]

Nepoplachová aplikace – systémy určené k ovládání a jejichž primární funkcí není ochrana života, majetku nebo prostředí, jako jsou:

- ovládání topení a větrání (ventilace),
- řízení energetických systémů,
- osvětlení. [11]

Poplachový stav - stav poplachového systému nebo jeho komponentů, který je výsledkem odezvy systému na přítomnost nebezpečí. [11]

Integrace – sjednocení, ucelení, splynutí, proces spojování ve vyšší celek.

Integrovaný poplachový systém - systém mající jedno nebo vice společných zařízení, alespoň jedním z nichž je poplachová aplikace. [11]

4.2 ČSN CLC/TS 50398

ČSN CLC/TS 50398 Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky. Norma uvádí všeobecné požadavky a typy struktur kombinovaných a integrovaných poplachových systémů. Norma má zajistit integraci jedné nebo více aplikací do jednoho integrovaného systému. Tento dokument poskytuje další informace týkající se prvotního návrhu (projektu) systému, plánování, instalace, předávání, provozu a údržby (servisu) kombinovaného a integrovaného systému. Tato norma specifikuje požadavky na poplachové systémy, které jsou kombinovány nebo integrovány s jinými systémy, které mohou a nemusí být poplachovými systémy. Definuje požadavky týkající se pravidel integrace s cílem zdůraznit význam jednotlivých aplikačních poplachových norem a objasnit případné rozpory. [11]

4.3 Systémové požadavky a stanovení kompatibility

Integrovaný poplachový systém musí být navržen tak, aby nebyla žádná aplikace v normálním stavu (včetně poplachového stavu) nepříznivě ovlivňována žádnou jinou aplikaci. V rámci kombinovaných a integrovaných systémů mohou být povelové signály přenášeny z jedné aplikace do jiné nebo z ústředního ovládacího zařízení do dalších částí aplikace. Příkladem je dálkové vypínání detektorů z ústředního ovládacího zařízení nebo blokování

CO2 hasícího systému systémem kontroly vstupů, když osoba vstoupí do chráněného prostoru.

Použití povelových signalů může být užitečné pro organizaci správy velkých budov (objektů) nebo areálů, skládajících se z většího počtu budov, může však take snížit bezpečnost a zabezpečení, je-li takové zařízení nesprávně použito. Příkladem může být dálkové odemykání přístupových dveří systémem elektrické požární signalizace, aniž by nebyly vzaty v úvahu možné důsledky pro zabezpečení objektů. [11]

Základní funkční princip integrovaných zabezpečovacích systémů je založen na kategorii charakteristických rysů nebezpečí, avšak cílová funkce je širší, složitější a na realizaci náročnější. Kromě narušitele nebo lupiče zde hraje roli i řada dalších faktorů, v jejichž důsledků může dojít k požáru, výbuchu nebo provozní havárii. Je samozřejmé, že většina nebezpečných výrobních technologií má svůj vlastní zabezpečovací systém, který je však laděn na nebezpečné situace spojené právě s výrobní technologií. Úmysl nebo hrubá nedbalost se většinou nepředpokládají. Stejně tak výskyt dalších rizikových faktorů v prostoru objektu, závisející na předem těžko definovatelných okolnostech, většinou vnitřní bezpečnostní systém výrobní technologie nerespektuje. [12]

4.4 Prostředky systémové integrace

Existuje mnoho výhod, které je možné vytěžit, pokud zvážíme možnost návrhu a implementace bezpečnostního systému v integrované podobě. Tato část předkládá některé výhody, které by měly být zváženy, když se kombinuje systém do integrovaného řešení. V modelovém objektu se jedná o poplachové systémy PZTS, CCTV a ACS.

4.4.1 Přístupový systém ACS

Integrací přístupových systémů s jinými poplachovými systémy můžeme získat mnoho výhod, například:

- evakuace v případě požárního nebezpečí – budete znát, které osoby se v prostoru nachází,
- dozvíme se, kterými vchody nebo místy osoby vstupují, nebo se pokouší vstoupit,
- propojit záznamy průmyslové televize s událostmi vzniklými v přístupovém systému,

- můžeme propojit do jednoho systému přístupový a docházkový systém,
- můžete propojit do jednoho systému přístupový, návštěvní systém s podporou CCTV,
- můžeme zvýšit úroveň bezpečnosti zavedení duálních identifikačních karet nebo biometrie,
- kontrolní funkce poplachového systému mohou být řízeny přístupovým systémem. [12]

4.4.2 Kamerový systém CCTV

Přímým datovým propojením kamerového systému s takovými systémy jako je například přístupový systém získáte mnohé výhody a mnohem účinnější řešení bezpečnostního systému, například:

- okamžité kamerové pohledy přístupné přímo z aplikačního programového vybavení přístupového systému, nebo jiných integračních uživatelských programů,
- přístupový systém nebo poplachový detekční systém mohou iniciovat předpoplachové a situační nahrávky, což je zajištěno nastavením vazeb mezi vzniklými událostmi a nahráváním bezpečnostních videosekvencí. Toto činí vyhledávání archívních záznamů mnohem efektivnější a jednodušší, neboť sama poplachová událost je linkována na odpovídající nahrávku, například je okamžitě dostupná poplachová nahrávka k události typu – „Násilně otevřené dveře – dveře skladu “, nebo „Zóna 3 – narušení obvodové ochrany“,
- sledování jedinců a monitorování jejich pohybu v objektu pomocí označení „podezřelá osoba“ nebo „zcizená identifikační karta“,
- nastavení specifických kamerových prepozic (záběrů) otočných kamer, například při průchodu osoby vstupními dveřmi banky se kamera natočí a přiblíží přímo na horní polovinu těla vstupující osoby (přesný záznam obličeje osoby),
- využití kamerových systémů pro vyloučení možných podvodů v evidenci pracovní doby, kdy zaměstnanci mohou označovat identifikační karty za jiné zaměstnance. [12]

4.4.3 Poplachový zabezpečovací systém PZTS

Rovněž integrace poplachového systému PZTS se ACS přináší velmi výhodná řešení a významné posílení bezpečnostních funkcí, například:

- zapínání a vypínání detekční funkce poplachového systému jako odezva na označení platné identifikační karty přístupového systému,
- provoz poplachového systému bez časového zpoždění při násilném otevření hlavních vchodových dveří. Časovač vstupního zpoždění je vyřazen, což má za následek okamžitou signalizaci poplachové události,
- blokování funkce snímačů identifikačních karet při zapnuté detekční funkci poplachového systému,
- využití funkce čítače přítomnosti osob (přístupový systém) ke zjištění, zda je možné v objektu zapnutí detekční funkce poplachového systému, což má za následek významné snížení počtu falešných poplachových hlášení poplachová přijímací centra (PPC). [12]

4.4.4 Integrace poplachových a nepoplachové aplikací

V našem průmyslovém podniku jsou prostory jak výrobní tak i nevýrobní (kanceláře atd.), kde můžeme využívat systémy technického řízení budov, které jsou odpovědné za monitorování a řízení prostředí uvnitř objektů. Do těchto systémů patří například osvětlení, centrální vytápění, vzduchotechnika a klimatizace. Nastavením automatických vazeb mezi těmito systémy a přístupovým systémem, případně poplachovým systémem lze dosáhnout úspor v nákladech na vytápění nebo osvětlení objektu. Odchodem osob z objektu lze snížit provozní osvětlení na nezbytné minimum a vnitřní teplotu lze nastavit na teplotu temperování objektu (na noční provoz, na víkend). Dále jsou uvedeny konkrétní aplikace integrace poplachových a nepoplachových systémů v modelovém průmyslovém podniku. [12]

4.4.5 Řízení výtahu

Řízení výtahu v Administrativní budově (dále jen AB) průmyslového podniku dle nastavených oprávnění v přístupovém systému společně integrovaný s řízením výtahu, který nám umožní přístupu osob do určitých pater. Pokud propojíme řídicí jednotky výtahových

systémů s přístupovými systémy, zajistíme omezení přístupu osob nebo návštěv do určitých pater budov, v nichž je pohyb neoprávněných osob nevhodný.

Zajištění vstupů do určitých pater u požárního schodiště v AB, lze realizovat použitím bezdrátové cylindrické vložky s integrovanou bezkontaktní čtečkou a on-line komunikací s nadřízeným GNOME485 systémem kontroly vstupů.

4.4.6 Ovládání osvětlení

Osvětlení ve výrobních prostorech považujeme za nepoplachové aplikace, které integrujeme s poplachovými aplikacemi nejčastěji, a to:

- poplachové zabezpečovací a tísňové systémy (PZTS),
- kamerové systémy (CCTV).

Vzájemná integrace uvedených aplikací nám ve výrobních prostorech umožňuje minimalizovat náklady na osvětlení a rovněž nám poskytne zabezpečení zesílením osvětlení při vniknutí nežádoucí osoby do konkrétních předem nadefinovaných prostorů při výrobní odstávce.

4.4.7 Identifikace na strojním zařízení

V daném průmyslovém podniku se nachází složitá strojní zařízení, která pro spuštění a následný provoz vyžadují odbornou obsluhu. Vzhledem k tomu, že se jedná o velmi drahá zažízení a při neodborném a neoprávněném spuštění by mohlo dojít k poškození a tím tedy velkým finančním ztrátám. Doporučuji instalaci přístupových systémů integrovaných s řízením těchto zařízení. Integrace těchto systémů by zamezila spuštění nežádoucí osobou.

Instalované přístupové systémy na strojním zařízení pracují se software Aktion EVO, který následovně zajišťuje evidenci odpracované doby pracovníků na jednotlivých zakázkách formou identifikace časové práce. Tento systém je určen zejména pro souhrnné sledování odpracované doby na výrobcích, zakázkách, výrobních operacích, službách, apod. Displej terminálu umožňuje zobrazovat přímo názvy nebo čísla zakázek. Začátek či konec práce se aktivuje stiskem příslušného řádku a přiložením ID karty. [5]

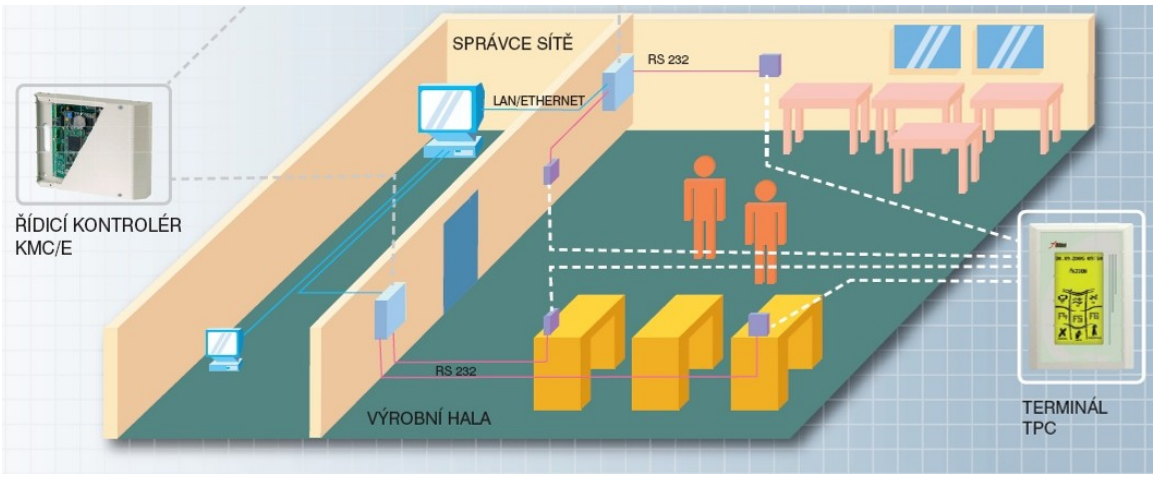
Obr. 11 Identifikace a sledování výroby na strojním zařízení. [5]

Příklady evidencí:

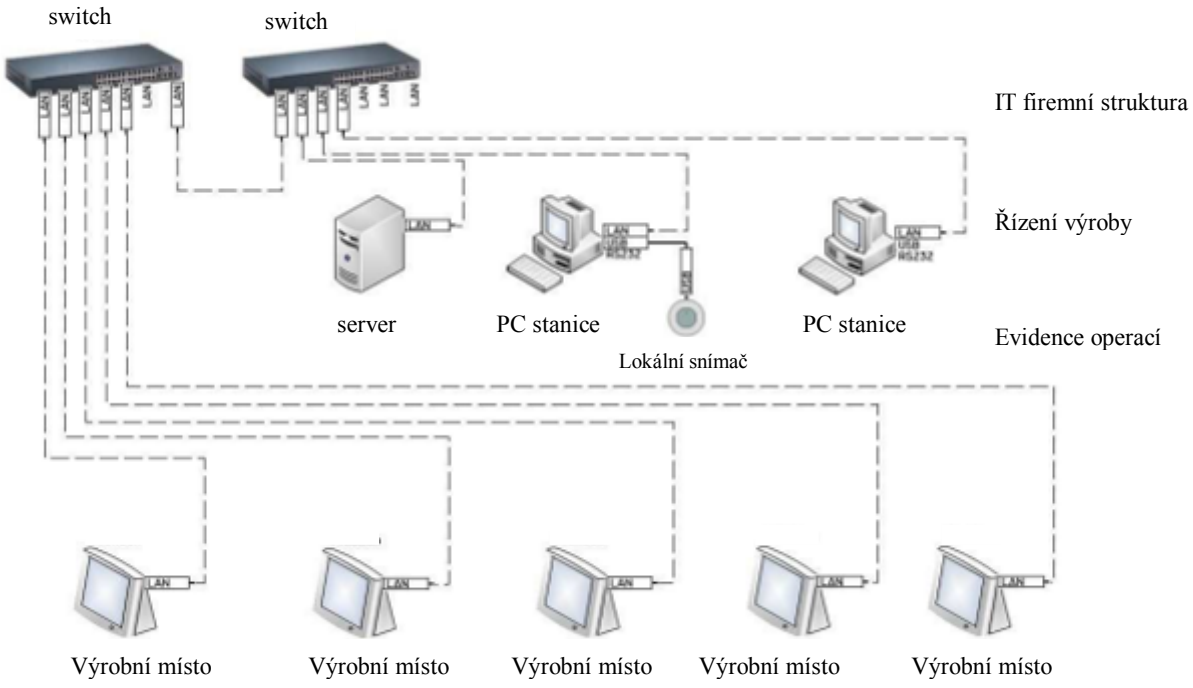
- sledování pohybu výrobku po dobu výrobního procesu,
- kontrola dodržování časových limitů na výrobní operaci,
- sledování provádění jednotlivých úkonů na výrobku,
- přihlašování a odhlašování pracovníka na výrobním místě,
- sledování času stráveného na daném úkonu,
- odvádění počtu kusů výrobků,
- evidence zmetků.

Sledování odpracované doby na zakázkách a výrobních operacích. Software Aktion zajišťuje rychlé a efektivní zpracování dat pomocí průmyslových terminálů. Systém poskytuje přehled o počtu odpracovaných hodin a odvedených kusů výrobků do informačních systémů řízení výroby. [5]

Další obrázek znázorňuje pracovníky, kteří přicházejí na pracoviště. Pracovníci před začátkem pracovní činnosti se musí identifikovat na terminálu TPC, který je instalovaný na strojním zařízení. Kontrolér MultiCon KMC/E je hlavní mikroprocesorová jednotka systému Aktion, která vyhodnocuje identifikaci (řídící jednotka přístupového systému).



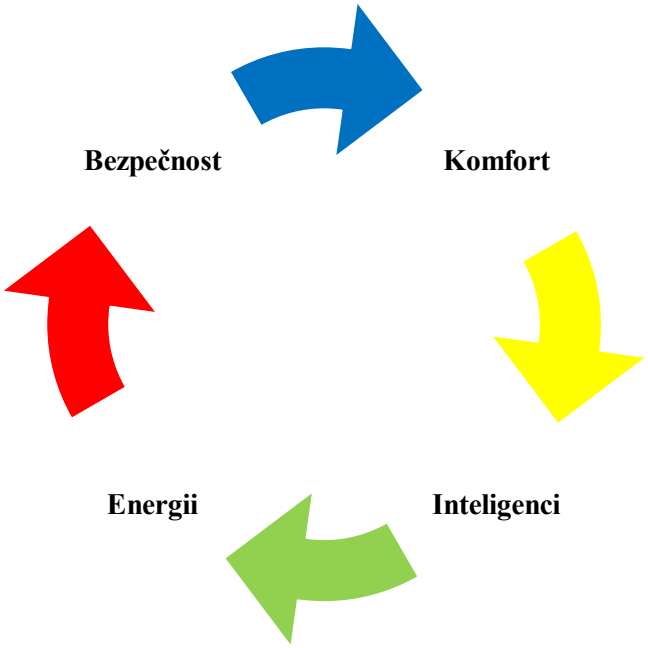
Obr. 12 Evidence výrobních operací. [5]



Obr. 13 Příklad blokového zapojení přístupového systému, identifikace na strojním zařízení. [5]

4.5 Výhoda integrace poplachových a nepoplachových aplikací

Integrací poplachových a nepoplachových aplikací na vybraném modelovém objektu získáme bezpečný, komfortní a inteligentní systém a současně šetříme energii.



Obr. 14 Integrace aplikací.

Dílčí závěr

V předposlední části se zabývám základními principy integrace poplachových a nepoplachových aplikací a uvádím možnosti integrace ve vymezených oblastech, jako je například povinná identifikace na jednotlivých technologických zařízeních s využitím instalovaného přístupového systému a ovládání osvětlení za pomocí poplachových zabezpečovacích nebo kamerových systémů ve výrobních prostorech a nebo skladech. Propojení poplachového zabezpečovacího a tísňového systému, přístupového a kamerového systému, řízení výtahů, ovládání osvětlení, klimatizace a dalších technologických a administrativních procesů přináší přehled o celkové bezpečnostní situaci objektu, řízení přístupu osob do jednotlivých částí objektu, kontrolu osob v rámci mzdového systému a v neposlední řadě kontrolu odběrů a úsporu energií.

5 NÁVRH TECHNICKÉHO ŘEŠENÍ OPTIMALIZACE A ROZŠÍŘENÍ POPLACHOVÉHO SYSTÉMU

Následující kapitola představuje návrh optimalizace a rozšíření poplachového systému průmyslového podniku. Návrh systému je zaměřen na perimetrickou ochranu modelového podniku. Při posouzení analýzy poplachových systémů jsem dospěl k závěru, že vybrané prvky poplachového systému jsou zaměřeny pouze na prostorovou a plášťovou ochranu. Perimetrická ochrana je řešena přístupovým systémem jen v místech vstupu a vjezdu do areálu. Ve zbývajících místech poplachový systém využíván není, spoléhá se pouze na oplocení lemující celý areál. Protože se, ale jedná o velký areál, kde díky velkému množství budov vznikají slabá místa, která jsou vhodná pro narušitele či lupiče, musí být prioritou vytvoření stoprocentní perimetrické ochrany za použití integrovaných poplachových systémů.

5.1 Požadavky na projekt

Návrh systému byl zpracován v souladu s doporučením obsahu dokumentu „Návrh skladby sytému" dle ČSN CLC/TS 50131-7 a ČSN EN 50132-7.

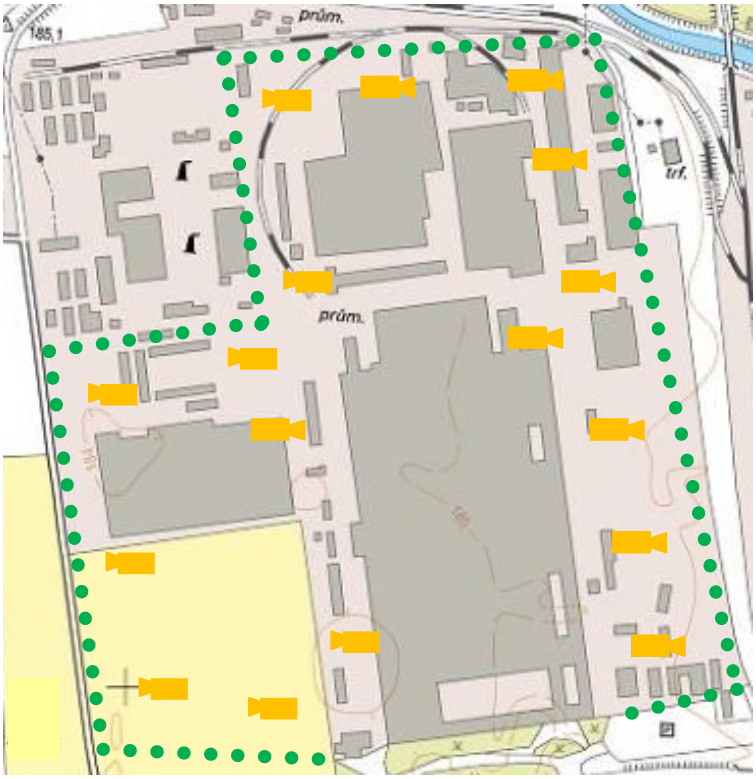
Norma ČSN CLC/TS 50131-7 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace. Tyto pokyny pro aplikace poskytují návod pro navrhování, montáž, provoz a údržbu poplachových zabezpečovacích a tísňových systémů (Intruder and Hold-up Alarm Systems - I&HAS). Účelem této technické specifikace je zajistit, aby systémy I&HAS splňovaly požadované funkční vlastnosti při minimálním množství planých poplachů. [13]

Norma ČSN EN 50132-7 Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikaci. Norma stanovuje doporučení pro výběr, plánování a instalaci systémů uzavřených televizních okruhů, které zahrnují kamery s monitory a/nebo s videorekordéry, řídicí a další pomocná zařízení nutná pro použití v bezpečnostních aplikacích. Cílem této normy je: a) poskytovat pracovní rámec umožňující zákazníkům, montérům a uživatelům stanovit jejich požadavky, b) pomoci projektantům a uživatelům při volbě optimální varianty zařízení, c) poskytnout prostředky k objektivnímu hodnocení vlastností instalovaného systému. [14]

5.1.1 Údaje o modelovém objektu

- výrobní průmyslový podnik,
- rozsáhlý komplex s velkým počtem budov a s volným pohybem osob,
- součástí komplexu jsou i budovy externích firem,
- 24 hodinový provoz.

Obrázek znázorňuje navrhované rozmístění prvků poplachového systému, které je tvořeno kombinací plotového detekčního a kamerového systému. Kamerový systém tvoří 16 IP kamer, které jsou rozmístěny tak, aby mohly monitorovat oplocení areálu, hlavní pozemní komunikace a vybraná riziková místa.



Obr. 15 Návrh perimetrické ochrany průmyslového podniku.

Tab. 3 Legenda použitých prvků.

CCTV	Návrh umístění kamerového systému.
● ● ● ● ●	Perimetrický plotový detekční systém Peridect.

5.1.2 Stupeň zabezpečení

Dalším stupněm při návrhu systému je stanovení stupně zabezpečení. Stupeň zabezpečení se stanovuje dle ČSN EN 50131-1 ed. 2.

Vzhledem ke komplikovanosti areálu a výši možných rizik jsem navrhl stupeň zabezpečení 3.

Tab. 4 Stupeň zabezpečení. [4]

Stupeň 3: Střední až vysoké riziko **SR / VR**
Předpokládá se, že narušitelé jsou obeznámeni s PZTS a že mají úplný sortiment nástrojů a přenosných elektronických přístrojů.

5.1.3 Klasifikace prostředí

Dalším částí při návrhu systému je klasifikace prostředí dle ČSN EN 50131-1 ed. 2. Prvky I&HAS musí správně pracovat, jsou-li vystaveny působení vlivů prostředí dle specifikace I. až IV. třídy.

Navržené prvky jsem zařadil dle klasifikace prostředí do třídy IV.

Tab. 5 Klasifikace prostředí. [4]

Třída IV: Prostředí venkovní všeobecné
Komponenty PZTS musí správně pracovat při působení vlivů prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty PZTS jsou vystaveny plně vlivům počasí. Předpokládají se změny teplot v rozmezí – 25 °C až + 60 °C při střední relativní vlhkosti okolo 75 % bez kondenzace. V průběhu roku se po dobu 30 dnů předpokládají změny relativní vlhkosti v rozmezí 85 % až 95 % bez kondenzace.

5.2 Seznam materiálu

Seznam materiálu (přehled zařízení) je dalším krokem v návrhu systému dle ČSN CLC/TS 50131-7.

5.2.1 Prvky PZTS

Pro perimetrickou ochranu navrhuji systém PERIDECT, který detekuje vibrace oplocení, způsobené mechanickými podněty, vznikajícími při pokusech o jeho překonání (přelezení, prostříhání, nadzvednutí).

5.2.1.1 Plotový perimetrický detekční systém PERIDECT

Plotový perimetrický detekční systém, který k detekci využívá senzory rozmístěné na oplocení (obvykle jeden detektor na jeden plotový dílec). Každý detektor obsahuje piezoelektrický element doplněný mikroprocesorovým zpracováním signálu. Použitím tzv. diferenční logiky systém výrazně potlačuje plané poplachy, způsobené běžnými povětrnostními vlivy (déšť, vítr). Přesnost detekce systému je s rozlišením na každý jednotlivý detekční senzor PDS, přičemž lze nastavovat nezávisle parametry libovolného senzoru. Typické zabezpečení jednou vyhodnocovací jednotkou je linie o délce cca 1300 m s rozlišením průniku po 2,5 m. [15]

Systém PERIDECT je zcela autonomní zařízení s plně konfigurovatelnými vlastnostmi a s poplachovými výstupy, které umožňují jednoduše připojit systém PERIDECT do všech PZTS systémů jako běžný detektor. Systém PERIDECT je navíc vybaven vstupně/výstupními moduly, které umožňují kdekoliv na trase perimetru jednoduché připojení jiných zařízení (např. kontaktu, IR bariéry) do systému a zároveň ovládání dalších zařízení (např. reflektor).

Větší komfort obsluhy poskytuje jeho připojení k vizualizačnímu programu pro integraci bezpečnostních systémů, např. C4. Zde je možno zobrazit přímo zabezpečenou oblast graficky, a to i se stavem jednotlivých komponentů zařízení. [15]

Peridect, přesný perimetrický detekční systém chránící objekty a oblasti proti neoprávněnému průniku.

Základem systému jsou vzájemně digitálně komunikující unikátní senzory a vyhodnocovací jednotka. Celý systém je variabilní co do vlastního nastavení, použitelnosti pro nejrůznější typy oplocení i integrovatelnosti s dalšími zabezpečovacími technologiemi. Pro maximální spolehlivost sytému je vyvinuta funkce diferenční logiky, díky které dochází ve srovnání s ostatními běžnými systémy k významnému snížení počtu falešných poplachů způsobených vlivy venkovního prostředí (silný vítr, déšť, kroupy, hromobití), a to při současném zachování jednoduchosti a nízké finanční a časové náročnosti instalace a údržby systému. [15]

Systém je zcela autonomní zařízení, které lze jednoduše připojit do standardních bezpečnostních a řídicích systémů, jeho propojení se systémem CCTV pak přináší moderní

řešení odpovídající nejvyšším požadavkům na bezpečnost za všech klimatických podmínek. Jeho modulární bloková architektura umožňuje v případě potřeby kdykoliv chráněný perimetr rozšířit, větvit, atp. bez výměny již instalovaného zařízení. [15]

Velmi jednoduše a bez dodatečných nákladů na existující technologii lze plotový detekční systém doplnit o přesný podzemní perimetr. Tato kombinovaná sestava pak v podstatě nedává běžnému narušiteli reálnou možnost k překonání.

Peridect je certifikován pro zabezpečení objektu do stupně zabezpečení 4 – vysoké riziko a je testován v rozsahu pracovních teplot –55 °C až do +85 °C. [15]

Výhody systému Peridect:

- přesná detekce místa narušení,
- velice nízký počet planých poplachů způsobených povětrnostními vlivy,
- jednoduchá montáž a servis,
- nezávislé nastavení jednotlivých detekčních senzorů,
- dlouhá životnost (žádné pohyblivé prvky),
- jednoduché připojení k ústřednám PZTS,
- možnost připojení prvků PZTS i na trase perimetru,
- možnost ovládání jiných zařízení i na trase perimetru,
- jedna vyhodnocovací jednotka zabezpečí oplocení o délce cca 1300 m,
- systém je velmi vhodný pro spolupráci s kamerovým systémem. [15]

Obr. 16 Plotový perimetrický detekční systém Peridect. [15]

Obr. 17 Peridect na ochranu průmyslových podniků. [15]

5.2.1.2 Prvky systému Peridect

Systém PERIDECT tvoří vyhodnocovací jednotka (PVJ), ke které jsou datovým kabelem připojeny detekční senzory (PDS), případně vstupně/výstupní moduly (PIO).

PVJ – Vyhodnocovací jednotka

Vyhodnocovací jednotka je umístěna v plastovém krytu, vhodném pro instalaci ve venkovním prostředí, s průchodkami pro kabeláž. K jednotce jsou připojeny datovým a zároveň napájecím kabelem (dvoudrátová sběrnice) jednotlivé detekční senzory PDS a vstupně/výstupní moduly PIO. Jednotka obsahuje 10 programovatelných výstupů. Tyto mohou být připojeny např. ke klasické PZTS ústředně s tím, že každému výstupu lze přiřadit aktivaci z jakýchkoliv skupin senzorů PDS nebo stav vstupu modulu PIO. Vyhodnocovací jednotka dále obsahuje osm dvojitě vyvážených vstupů, které mohou být použity pro připojení prvků PZTS systémů, jako např. kontaktů a PIR, IR, MW detektorů.

Popis PVJ:

Napájecí napětí: 9 – 16 Vdc. Odběr: 200 mA (bez připojených modulů PDS a PIO), 600 mA max. (s připojeným maximálním počtem jednotek tj. 246x PDS a 8x PIO). Pracovní

teplotní rozsah: -55°C až +85°C. Krytí: IP65. Datová linka: délka max. 1300 m. Rozměry: 150 x 200 x 80 mm

PDS – Detekční senzor

Detekční senzor vyhodnocuje pomocí piezoelektrického čidla mechanické otřesy z oplocení. Je umístěn v dvouplášťové plastové krabičce a k oplocení se upevňuje pomocí čtyř šroubů a plastového třmenu. Standardně se montuje doprostřed pole oplocení. Jednotlivé senzory jsou výrobcem propojeny datovým kabelem s roztečí dle konkrétních podmínek. [15]

Popis PDS:

Napájení: ze sběrnice vyhodnocovací jednotky PVJ. Odběr: 1mA max.. Pracovní teplotní rozsah: -55°C až +85°C. Krytí elektroniky detektoru: IP65. Rozměry: 70 x 80 x 35 mm

PIO – Vstupně/výstupní modul

Vstupně výstupní modul je určen pro zavedení logického stavu (např. kontaktu) do systému, a pro sepnutí jakéhokoliv zařízení na trase perimetru. PIO modul má vlastní adresu a může být připojen kdekoliv na datový kabel. PIO modulem lze velice jednoduše vyřešit např. kontrolu otevření dveří na zabezpečené trase pouhým připojením magnetického kontaktu k modulu PIO. Výstupem se může dálkově spínat např. osvětlení nebo siréna. [15]

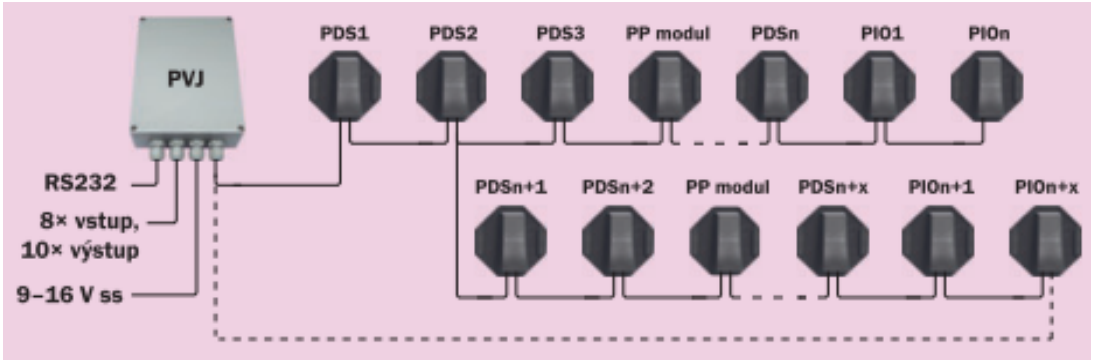
Popis PIO:

Napájení: ze sběrnice vyhodnocovací jednotky PVJ. Odběr: 2mA max.. Pracovní teplotní rozsah: -55°C až +85°C. Krytí elektroniky: IP65. Rozměry: 70 x 80 x 35 mm.

Blokové zapojení:

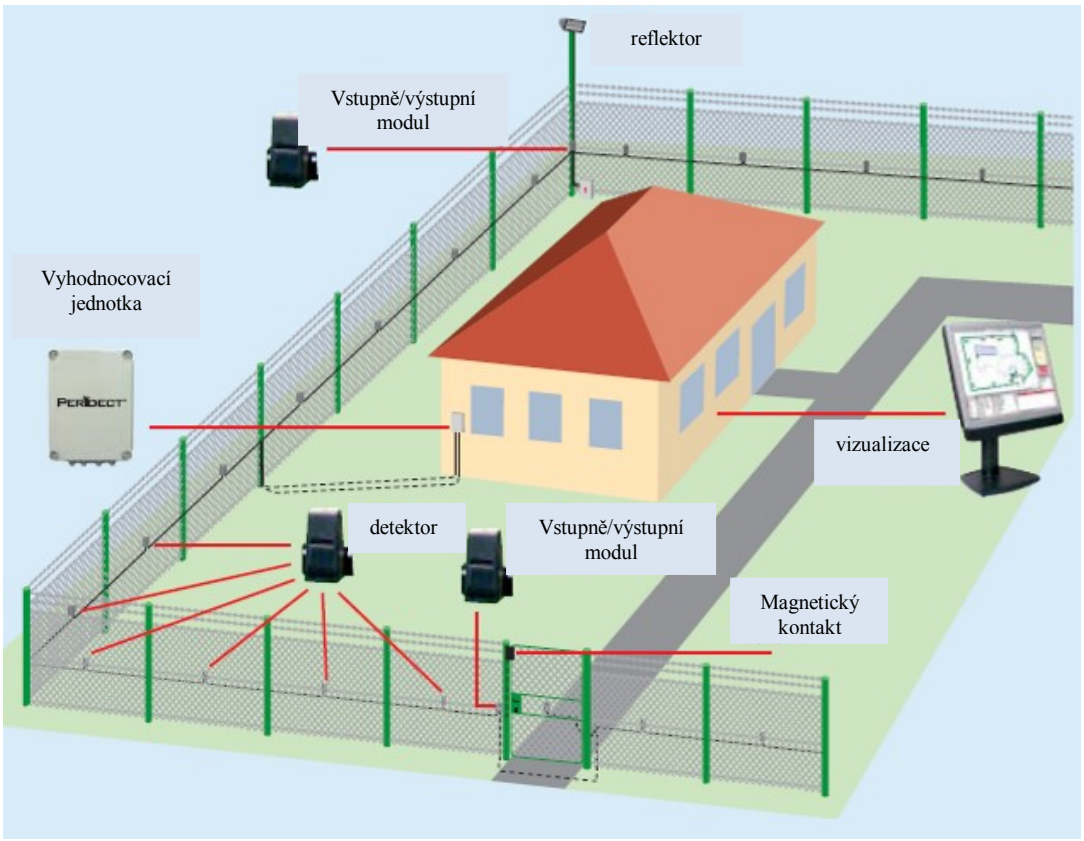
PVJ – vyhodnocovací jednotka, PDS – detekční senzor, PIO – vstupně/výstupní modul, PP modul – přepěťová ochrana. Kapacita jedné vyhodnocovací jednotky umožňuje připojení:

- max. délka datové linky 1300 m,
- max. počet připojených detekčních senzorů je 246,
- max. počet připojených PIO modulů je 8.



Obr. 18 Blokové zapojení perimetrického detekčního systému Peridect. [15]

Obrázek znázorňuje objekt, který je střežen plotovým perimetrickým detekčním systémem, který má na modulu PIO připojený reflektor a magnetický kontakt. Při napadení objektu přes oplocení nám systém Peridect detekuje nežádoucí narušení a výstupem z modulu PIO se dálkově sepne osvětlení. Otevření vstupní branky se na zabezpečené trase kontroluje pouhým připojením magnetického kontaktu k modulu PIO.

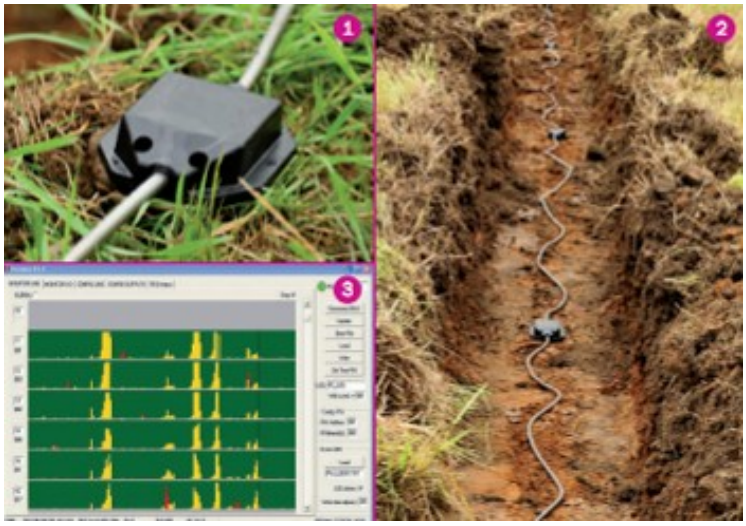


Obr. 19 Příklad ochrany perimetrickým detekčním systémem Peridect. [15]

V technickém řešení navrhuji plotový perimetrický detekční systém Peridect (dále jen PDS) v integraci s poplachovým systémem CCTV. PDS lze také kombinovat s podzemním detekčním systémem Peridect a tím zajistíme maximální perimetrickou ochranu.

Přesný podzemní detekční systém – zde je uvádím několik informací o podzemním detekčním systému Underground.

Podzemní detekční systém je založen na stejném detekčním a vyhodnocovacím principu jako jeho plotové varianty. Vyhodnocovací jednotka, zemní detektory, speciálně chráněná linka a vyhodnocovací software tvoří páteř systému. Instalace se obvykle provádí přímo do výkopu ve všech typech podloží bez jakýchkoli omezení a dodatečných terénních úprav. Přitom podzemní zůstává plně funkční při měnících se klimatických podmínkách. Systém Underground lze jednoduše připojit do standardních bezpečnostních a řídicích systémů, jeho integrace s CCTV přináší moderní řešení odpovídající nejvyšším požadavkům na bezpečnost za všech klimatických podmínek. Samozřejmostí pak je vzdálený přístup k zařízení a úpravy nastavení systému přes internet. Jeho modulární bloková architektura umožňuje v případě potřeby kdykoliv chráněný perimetr rozšířit, větvit, atp. bez výměny již instalovaného zařízení. Velmi jednoduše a bez dodatečných nákladů na existující technologii lze podzemní systém kombinovat s přesným plotovým detekčním systémem. [15]

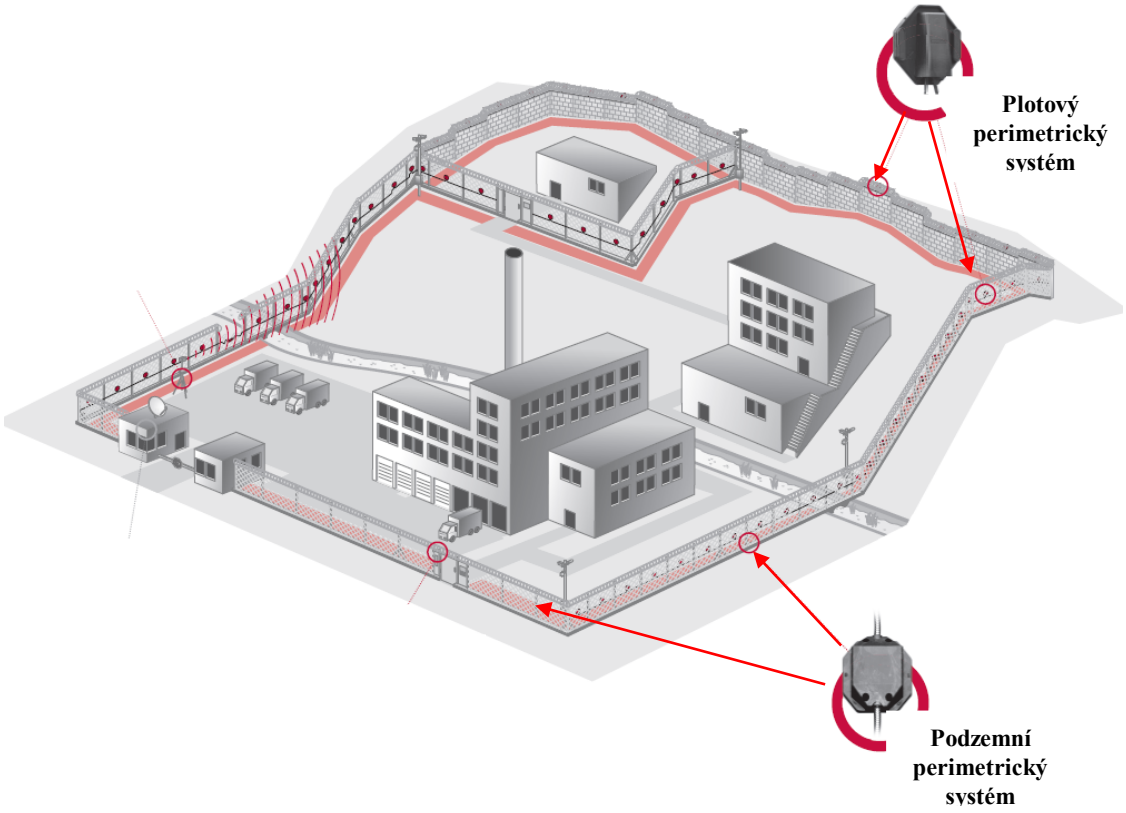


Obr. 20 Podzemní detekční perimetrický systém Underground. [15]

Popis obrázku:

1) detail podzemního detektoru Underground (doporučená hloubka zakopání 40cm),
2) umístění podzemních detektorů (vzdálenost mezi detektory od 1,5 m do 3 m),
3) ukázka výstupu z konfiguračního program.

Obrázek znázorňuje perimetrickou ochranu v kombinaci s plotovým a podzemním detekčním perimetrickým systémem.



Obr. 21 Perimetrická ochrana ze systémů Peridect. [15]

5.2.2 Prvky CCTV

Na modelový objekt průmyslového podniku navrhuji IP kamery, které budou tvořit s plotovým perimetrickým detekčním systémem Peridect perimetrickou ochranu. Kamerové systémy (CCTV) umožňují vizuální kontrolu a monitorování oblastí střeženého prostoru a plní tak funkci bezpečnostního nebo dohledového systému. Prvky CCTV snímají obraz ve

zvoleném místě, zajišťují jeho přenos a zobrazení na stanovišti obsluhy. Pořizovaný záznam je používán k prozkoumání rizikových situací a může plnit i roli důkazního materiálu.

5.2.2.1 IP kamery

IP kamery přenášejí obraz v digitální podobě v komprimovaném stavu pomocí krouceného čtyřpárového datového vodiče ve standardu počítačové sítě Ethernet. Samostatný přenos z IP kamery končí u nejbližšího aktivního prvku, poté je již přenášen souběžně s dalšími daty. Signál není degradován ani při přenosu na velké vzdálenosti. Výhodou IP kamer je dále vysoké rozlišení (MPix), možnost inteligentní analýzy obrazu, možnost bezdrátového přenosu dat, zajištění centrální správy, snadná rozšiřitelnost systému, součinnost s dalšími systémy v objektu (např. s PZTS).

Navrhuji IP kameru SANYO – typ VCC-XZN600P

Barevná IP kamera s režimem den/noc a 30× optickým zoomem. Provedení s krytím IP66.

Popis kamery:

- 1/4" CCD snímač,
- rozlišení 752×582 obrazových bodů,
- 16x digitální zoom,
- kompenzace protisvětla,
- inteligentní detekce pohybu,
- přenosové kodeky H.264 a JPEG,
- napájení 12V DC, 24V AC, Power over Ethernet 802.2af, odběr 4,5W.

Obr. 22 IP kamera SANYO. [16]

Dalším navhovaným prvkem v systému CCTV je síťový bezpečnostní videorekordér NVR.

SANYO DSR 2116

Digitální rekordér s vestavěným multiplexerem pro 16 kamer, HDD 1000 GB, live zobrazení 200 obr./s, záznam 200 obr./s, záznam 4x audio, ovládání telemetrie, LAN/WAN vzdálený přístup; kompozitní a VGA výstup na monitor; dálkové IR ovládání, snadné zálohování přes USB, vestavěná mechanika DVD-R/RW; alarmové výstupy; české menu; rozměry 432 x 89 x 349 mm.

Obr. 23 Sanyo DSR 2116. [16]

Na obrázku je integrace perimetrické ochrany zabezpečena poplachovým zabezpečovacím a tísňovým systémem s kamerovým systémem.

Obr. 24 Plotový perimetrický detekční systém Peridect integrovaný se CCTV. [15]

5.2.3 Ústředna PZTS

Dalším navrhovaným prvkem v systému pro perimetrickou ochranu je ústředna PZTS, která tvoří jádro zabezpečení. Zpracovává informace od detektorů (v našem případě od vyhodnocovací jednotky PVJ peridect) a systémových prvků a komunikuje přenosovým systémem prostřednictvím s poplachovým příjmovým centrem.

Perimetrický systém je zaintegrovatelný do ústředny PZTS ATS4099/1. Současně je zajištěna integrace do grafického nadstavbového systému C4, kde poplachové i poruchové stavy budou graficky a textově zobrazeny na podkladových půdorysech a lokalizují tak přehledně jejich umístění.

Popis navrhované ústředny:

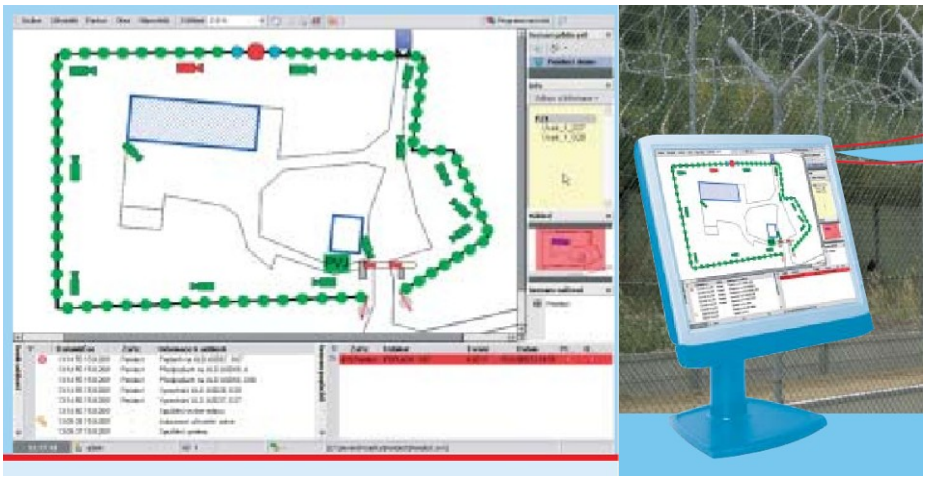
- integrovaný zabezpečovací a přístupový systém, až 256 vstupů, 16 oblastí a 64 dveří,
- dvojitě vyvážené vstupní smyčky,
- až 255 volných programovatelných výstupu,
- modulární sběrnice RS485 s možností připojení až 16 ovladačů a 15 modulů,
- plně programovatelná logika - až 24 makro logik,
- vestavěný telefonní komunikátor, volitelný ISDN a GSM komunikátor,
- programování, monitorování a údržba z lokálního nebo vzdáleného PC,
- spínaný zálohovaný zdroj s ochranou baterie proti úplnému vybití,
- schválení EN50131, NBÚ, T/3, verze ATS4099/1 pro PT/4.

Obr. 25 Ústředna ATS-4099/1. [21]

5.2.4 Vizualizační program

Vizualizační program použijeme stávající (C4), který je v modelovém objektu využíván pro jiné poplachové systémy.

Poplachový systém integrujeme do grafického nadstavbového systému, kde poplachové či poruchové stavy jsou graficky a textově zobrazeny na podkladových půdorysech, a lokalizují tak přehledně jejich umístění. Jako podklady pro náhled se s výhodou používají vektorové výstupy z aplikací CAD, lze též použít fotografie objektu nebo rastrované obrázky. Systém C4 umožňuje integraci bezpečnostních, CCTV, požárních, přístupových a dalších systémů včetně přehledné vizualizace.



Obr. 26 Vizualizační program poplachového systému. [15]

Integrační bezpečnostní systém C4

C4 je integrační bezpečnostní systém, který zabezpečuje centralizované řešení pro správu zařízení objektové bezpečnosti. Uživateli poskytuje rozsáhlé nástroje pro:

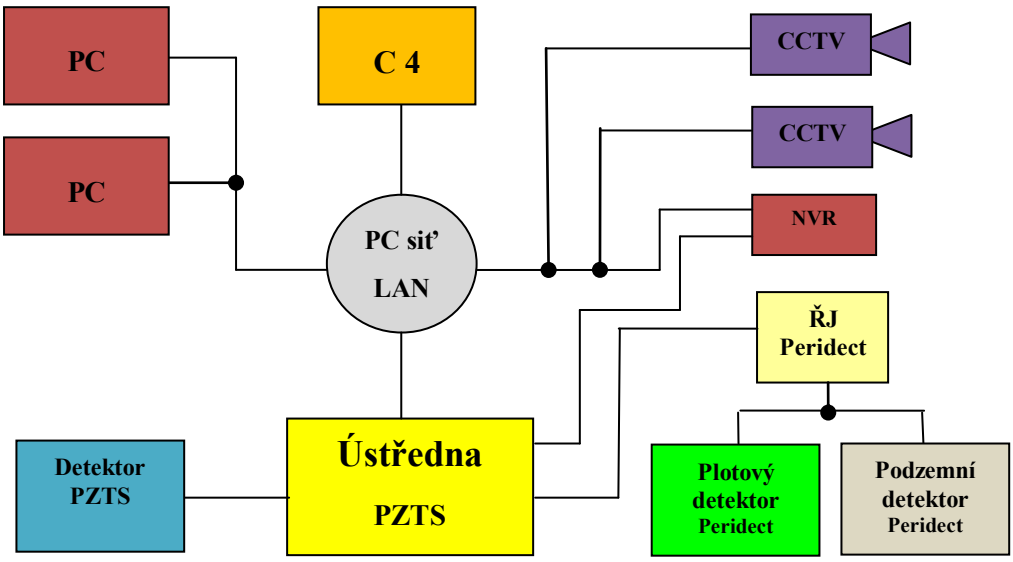
- centrální správu bezpečnostních zařízení,
- vizualizaci a monitoring zařízení,
- automatizaci bezpečnostních procesů,
- analýzu a vyhodnocování bezpečnostních informací,
- centrální identity management,
- podporu krizového řízení.

Systém C4 je otevřený modulární systém, který umožňuje monitorovat jednu samostatnou budovu, nebo robustní řešení monitorující různá bezpečnostní zařízení velké organizace ve všech jejích objektech bez ohledu na vzdálenost.

Systém C4 v rámci monitorovacího modulu umožňuje propojení s geografickými informačními systémy, které poskytují podpůrné informace při řešení krizových situací. Příkladem je zobrazení rozložení elektroinstalace, potrubí a vzduchotechniky v prostoru, ve kterém systém C4 hlásí bezpečnostní incident. Data jsou získávány on-line na požádání z datového serveru, který spravuje GIS data.

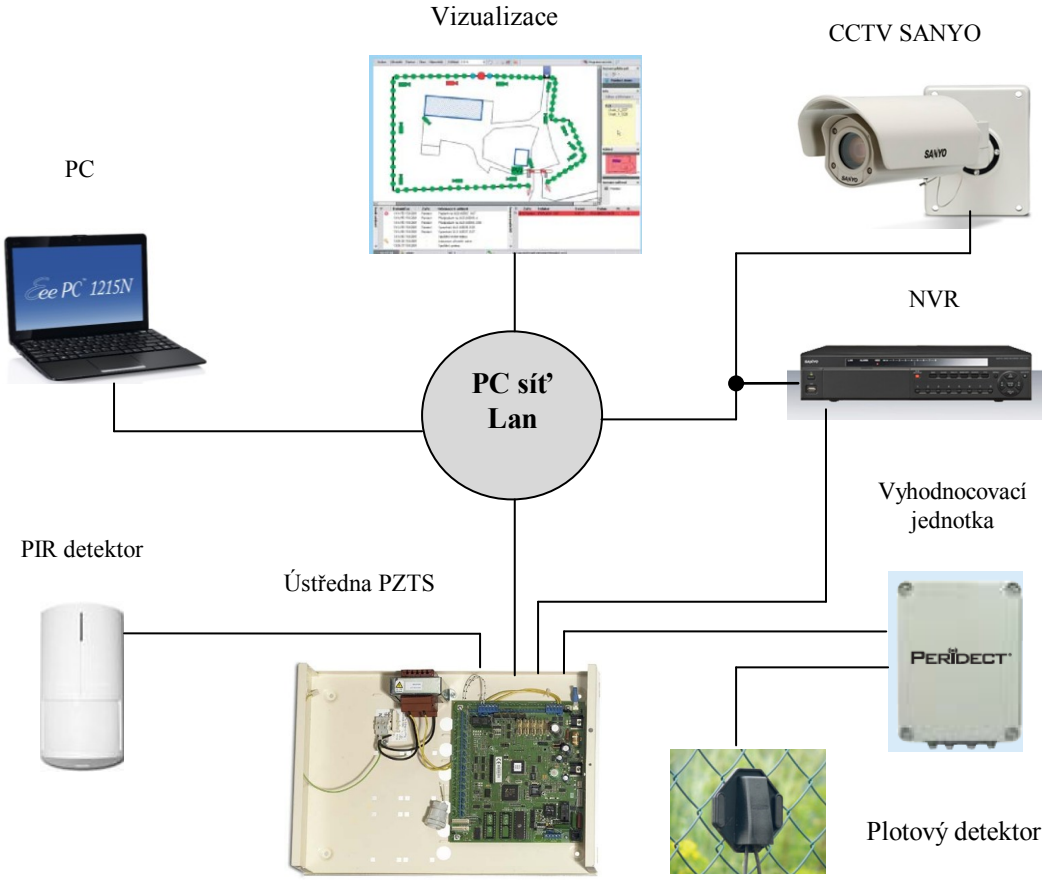
C4 umožňuje sledovat všechny monitorované bezpečnostní zařízení v jednotném prostředí včetně jejich jednotného ovládání z téhož prostředí. [17]

5.2.5 Blokové schéma navrhované perimetrické ochrany



Obr. 27 Blokové schéma znázorňující návrhované perimterické ochrany.

Blokové schéma znázorňuje propojení poplachových prvků. Ústředna PZTS, NVR, CCTV, C4, a PC mají IP adresu a komunikace probíhá přes lokální síť. Volné výstupy ústředny slouží k připojení dalších prvků PZTS.



Obr. 28 Blokové schéma s navrhovanými prvky poplachového systému.

5.2.6 Výpočet ceny navrhovaného poplachového systému

Výpočet ceny plotového perimetrického detekčního systému Peridect. Cena je 300 kč na 1 metr oplocení, v ceně jsou zahrnuty všechny prvky systému.

Tab. 6 Cena za systém Peridect.

Prvky systému Peridect	**množství**	**cena systému za 1 m = 300 Kč**
Vyhodnocovací jednotka - PVJ	3 ks	885 000 Kč
Vstupně/výstupní modul - PIO	24 ks	
Plotový detekční senzor - PDS	570 ks	
Detekční kabel	2950 m	

Tab. 7 Cena za navrhovaný poplachový systém.

Použité prvky	množství	Cena za 1ks	celková cena
Systém Peridect	2950 metrů	300 Kč za běžný metr	885 000
IP kamera SANYO – typ VCC-XZN600P	16	21 390	342 240
Digitální rekordér – Sanyo DSR 2116	1	18 950	18 950
Ústředna ATS4099/1	1	17 295	17 295
Celková cena v Kč včetně DPH			**1 263 485 Kč**

Celková cena za navrhovaný poplachový systém je 1 263 485 Kč. Do ceny není započítaná instalační práce, nastavení a oživení systému, zaškolení obsluhy, projektová dokumentace, doprava a předpokládaný pozáruční servis. Vzhledem k tomu, že se jedná o velký projekt můžeme očekávat lepší cenovou nabídku za systém Peridect a cenu IP kamer.

5.3 Zapojení poplachových systémů

Poplachové systémy jsou navrženy a softwarově centralizovány v grafické nádstavbě (software) C4 s dálkovým propojením přenosu dat na poplachové přijímací centrum (dále jen PPC) se stálou službou HZSP. Obousměrná komunikace ze zabezpečených míst s řídícím centrem se předpokládá v protokolu TCP/IP. Z tohoto důvodu jsou sériové kanály RS232 bezpečnostních systémů PZTS převedeny na protokol TCP/IP a společně s ethernetovým portem záznamového zařízení (DVR) kamerového systému (CCTV) připojeny na porty ethernet switch. Switch je umístěn ve společné RACK skříni, v rozvodně. Volný port switch bude využit pro komunikaci s řídícím centrem. V případě poruchy ethernetové přenosové cesty je v omezené míře zajištěna jednosměrná komunikace ze zabezpečených míst na PPC prostřednictvím GSM modulu a telefonní linky.

Ochrana průmyslového podniku poplachovými systémy je navržena jako ochrana dvoustupňová. Základní ochranou je ochrana perimetru (obvodu) areálu podniku. Druhou ochranou je zabezpečení vytipovaných prostor vybraných objektů na oploceném pozemku. První zóna ochrany perimetru, konkrétně oplocení areálu, je navržena kombinací perimetrického detekčního systému PERIDECT instalovaného na jednotlivých polích oplocení a kamerovým systémem CCTV. Rozmístění kamer CCTV je navrženo tak, aby jimi

snímané prostory pokrývaly sto procent obvodu perimetru areálu. Vytipované prostory vybraných objektů jsou monitorovány kamerovým systémem CCTV.

Dále navrhuji umístění kamer na perimetru podél oplocení na ocelových kamerových sloupech s protikorozní úpravou, s výškou 4m. Sloupy budou uchyceny na betonových patkách, kterými bude procházet kabeláž. Všechny sloupy budou zemněny. Na každém sloupu bude umístěn rozvaděč s příslušným osazením. Kamery jsou rozmístěny tak, že zajišťují kvalitní monitoring celého perimetru. Kamery jsou umístěny v temperovaných krytech se skrytou kabeláží a s krytím min. IP66.

Kamery na kamerových sloupech a případné IR reflektory budou propojeny kabely a napájecím vedením se zamykatelnou kamerovou rozvodnou skříní s krytím minimálně IP 66 umístěnou na kamerovém sloupu. V rozvodné skříni budou umístěny PoE switche, media konvertory pro převod na optiku, optický rozvaděč, jistič, proudový chránič a přepěťová ochrana. Napájení bude provedeno z místně příslušných silnoproudých rozvaděčů. Media konvertory budou připojeny prostřednictvím průmyslového LAN standardu optickými single-mode kabely do serverovny v PPC centru HZSP. Pro kabelové rozvody bude podél oplocení vybudován krytý kovový kabelový krytý žlab.

5.4 Konfigurace systému

Centrem ochrany je místnost velínu v PPC HZSP. V této místnosti bude instalován společný RACK pro všechny bezpečnostní systémy. Ve skříni bude instalována ústředna PZTS, vyhodnocovací jednotka perimetrického systému, digitální záznamové zařízení CCTV, záložní napájecí zdroj UPS, převodníky, napájecí zdroje, záložní akumulátory, svorky pro připojení nn napájecích přívodních a odchozích kabelů, přepěťová ochrana a komunikační switch. V rozvaděči budou ukončeny napájecí kabely, datovými kabely CCTV a kabely zabezpečovacího systému PZTS. Rozvaděč bude propojen komunikačním kabelem sériové linky a napájecím kabelem s rozvaděči.

Kamerový systém je řešen jako síťový kamerový systém s IP kamerami připojenými do IP serveru umístěného v PPC HZSP s minimální dobou záznamu 30 dnů. Pro přenos obrazové informace bude vybudována lokální síť na bázi metalických a optických průmyslových standardů. Systém bude v provozu 24 hodin denně a podle zadání jsou zajištěny potřebné

provozní funkce, zejména automatické zobrazení kamer v zóně poplachu detekční bariéry systému PZTS a manuální přepínání signálu jednotlivých kamer podle potřeby.

Systém umožňuje komplexní nastavení konfigurace systému oprávněným správcem, včetně nastavení priorit přístupu jednotlivých klientských pracovišť k jednotlivým kamerám a záznamům. Rozmístění monitorovacích pracovišť je věcí volby, obecně platí, že monitorovací pracoviště mohou být kdekoliv na počítačové síti. Záznamové zařízení bude umožňovat záznam textových řetězců přímo do obrazu ze sériového portu. Záznamové zařízení bude softwarově integrované do integrovaného poplachového systému včetně alarmových hlášení stavu systému, alarmů detektoru, vyhledávání záznamu, spojování obrazových informací poplachů ze systému PZTS. Systém budou ovládat proškolené osoby (nebo-li dispečeři PPC) a určení a proškolení pracovníci bezpečnostní služby a zaměstnanci ochrany společnosti. Za zastřežování systému zodpovídají dispečeři PPC.

5.4.1 Hlášení poplachu

Při vzniku narušení perimetrické ochrany ústředna ATS zpracovává informace od vyhodnocovací jednotky peridect, která dostane informaci od jednoho nebo více plotových detektorů. Ústředna dá impuls kameře (povel k natočení do prostoru narušení) a zároveň přenáší data prostřednictvím telefonní linky a sítí GSM na PPC.

Monitorování zajišťuje dispečer HZSP a při signalizaci narušení objektu předá dispečer HZSP tuto informaci bezpečnostní službě, která provede výjezd zásahového vozidla ke kontrole narušeného objektu nebo prostoru. Dispečer PPC může přímo na půdorysech daného objektu prostřednictvím monitorů sledovat detektory v poplachovém stavu, časovou posloupnost událostí a koordinovat činnost zásahové jednotky.

5.4.2 Nahrávání a zálohování dat CCTV

V poplachovém příjímacím centru bude umístěn síťový bezpečnostní videorekordér NVR s odpovídajícím počtem videovstupů. Do videorekordéru jsou datovým kabelem připojeny příslušné kamery, které jsou nahrávány na lokální hard disk NVR. Digitální videorekordér je připojen do lokální počítačové sítě podniku. K systému nejsou připojeny žádné analogové monitory. Sledování, nastavování a vyhledávání záznamů je možné z počítačů v podnikové síti. U požitého typu kamer systému CCTV je možné nahrávání pomocí tzv. videodetektoru

pohybu. Tato funkce elektronicky sleduje vymezené oblasti záběru dané kamery (například dveře, okna, prostor u oplocení apod.) a v případě změny v obraze v této oblasti (= detekování pohybu) se automaticky spustí nahrávání. Tato funkce šetří záznamovou kapacitu HDD a usnadňuje vyhledávání záznamu. Prohlížení historie záznamu a nastavování lze pouze z počítačů, které mají nainstalovaný NetVu software.

5.4.2.1 Ochrana osobních údajů

Při návrhu systému CCTV jsou respektovány požadavky Úřadu pro ochranu osobních údajů, zejména pak zákon č. 101/2000 Sb., o ochraně osobních údajů. Jak vyplývá z povinností správce, stanovených v ustanovení zákona č. 101/2000 Sb. je správce povinen zajistit řádný souhlas monitorovaných osob, pokud budou záběry z kamer uchovávány pro pozdější použití. Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličej) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby. Snímané osoby musí být o užití kamerového systému vhodným způsobem informovány (např. nápisem a piktogramem kamery umístěným u vjezdu nebo na vstupech do budovy). V neposlední řadě musí správce zajistit podání vyplněného registračního formuláře s jednoznačně stanoveným účelem pořizování záznamu na Úřad pro ochranu osobních údajů. Dle zákona č.101/2000 Sb. má správce při provozování kamerového systému vybaveného záznamovým zařízením následující povinnosti:

- kamerové sledování nesmí nadměrně zasahovat do soukromí,
- musí být jednoznačně stanoven účel pořizování záznamů, který musí korespondovat s důležitými právem chráněnými zájmy správce (např. ochranou majetku a osob před krádeží). Záznamy tak mohou být využity pouze v souvislosti se zjištěním události, která poškozuje tyto důležité, právem chráněné zájmy správce.
- bude stanovena lhůta pro uchovávání záznamů. Doba uchovávání dat by neměla přesáhnout časový limit nutný pro naplnění účelu provozování kamerového systému. Pouze v případě existujícího bezpečnostního incidentu by měla být data zpřístupněna orgánům činným v trestním řízení, soudu nebo jinému oprávněnému subjektu.
- bude řádně zajištěna ochrana snímacích zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy, před neoprávněným nebo nahodilým přístupem, změnou,

zničením či ztrátou nebo jiným neoprávněným zpracováním, viz. § 13 zákona č. 101/2000 Sb.

Shodně se stávající zákonnou úpravou mohou v případě potřeby se záznamem kamer manipulovat pouze pověřené osoby. Pro tuto činnost jsou vyhrazeny pracovní stanice připojené na síti LAN. Jedná se o stanice umístěné přímo v areálu průmyslového podniku a o stanice na poplachovém příjmovém centru. [18]

5.5 Napájení a zálohování

Poplachové systémy budou napájeny ze stávajícího nn rozvaděče objektu. Vývod bude přiveden do RACK skříně, kde bude provedeno rozjištění přívodu do jednotlivých napájecích větví pro napájení zařízení PZTS a CCTV. Mezi rozvaděčem a rozvodnicí bude položen napájecí kabel CYKY 5J2,5. Z RACK skříně poplachových systémů budou vyvedeny samostatně jištěné vývody, kabely CYKY 3Cx2,5 k rozvaděčům poplachových systémů. V případě výpadku napájení 230V/50Hz se systém PZTS automaticky přepne na vlastní záložní zdroje s bezúdržbovými akumulátory 12V. Kamerový systém CCTV bude při výpadku napájení napájen ze záložního zdroje UPS. Navrženy jsou zdroje se zálohovaným napájením vlastním bezúdržbovým akumulátorem, který zajistí chod systému i při výpadku síťového napájení ve smyslu ČSN EN 50131-1 minimálně po dobu 30 hodin. Součástí systému PZTS je signalizace poruchy napájení napájecích zdrojů. Poruchové signály jsou přivedeny formou beznapěťových kontaktů na volné vstupy expandérů.

Vnější kabelové rozvody

Vnější kabelová propojení jsou navržena metalickými vícežilovými sdělovacími kabely, napájecími kabely a systémovým kabelem PERIDECT. Vnější kabelové rozvody jsou vedeny ve společném kabelovém výkopu, který je převážně trasován podél oplocení areálu.

5.5.1 Uzemnění

Neživé kovové části bezpečnostních systémů budou propojeny vodičem o průřezu 6mm2 a místně spojeny s objektovým uzemněním vodičem o průřezu min. 6mm .

5.6 Použitá legislativa

Pokud jsou v diplomové práci odkazy na české technické normy ČSN, pak se odkazovaná ustanovení stávají jeho nedílnou součástí vždy v platném znění normy.

Tab. 8 Použitá legislativa.

Předpis	**Název předpisu**
TNI 33 4591 – 1	Komentář k ČSN CLC/TS 50 131-7 – Část1: Návrh EZS.
TNI 33 4591 – 2	Komentář k ČSN CLC/TS 50 131-7 – Část2: Montáž EZS.
TNI 33 4591 – 3	Komentář k ČSN CLC/TS 50 131-7 – Část3: Prohlídky a funkční zkoušky PZTS, revize elektrické instalace EZS.
ČSN CLC/TS 50398	Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky.
ČSN EN řady 50 130	Poplachové systémy – Všeobecně.
ČSN EN řady 50 131	Poplachové systémy – Poplachové zabezpečovací a tísňové systémy.
ČSN EN řady 50 132	Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikací.
ČSN EN řady 50 132 - 7	Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikací – Část 7: Pokyny pro aplikace.
ČSN EN řady 50 133	Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikací.
ČSN 33 2000-1 ed. 2	Elektrické instalace nízkého napětí – Část 1: Základní hlediska, stanovení základních charakteristik, definice.
ČSN 34 7402	Pokyny pro užívaní nn kabelů a vodičů.
ČSN 33 4010	Elektrotechnické předpisy. Ochrana sdělovacích vedení a zařízení proti přepětí a nadproudu atmosférického původu.
ČSN 34 2000-1 ed.2	Elektrické instalace nízkého napětí – Část1: Základní hlediska, stanovení základních charakteristik, definice.
ČSN 33 1500	Elektrotechnické předpisy. Revize elektrických zařízení.
ČSN EN 61000-6-3 ed.3	Elektromagnetická kompatibilita (ECM) – Část 6-2: Kmenové normy – Odolnost pro průmyslové prostředí.
Zákon č. 183./2006 Sb.	Zákon o územním plánování a stavebním řádu (stavební zákon).
Zákon č. 101/2000 Sb.	Zákon o ochraně osobních údajů.
Vyhláška 591/2006 Sb.	Nařízení vlády o bližších minimálních požadavcích na bezpečnost a ochranu zdraví při práci na staveništích.

5.7 Společné pokyny a funkčnost poplachových prvků

Další požadavky na projekt podle návrhu systému dle ČSN CLC/TS 50131-7 jsou funkčnost a údržba systému a prvků poplachového systému. Dle uvedené normy se musí na zařízení provést:

- kontrola detekce sabotáže,
- nastavení do střežení a klidu,
- kontrola napájecích zdrojů,
- funkčnost detektorů,
- funkčnost výstražných zařízení.

5.7.1 Pokyny pro funkčnost PZTS

Po instalaci PZTS je nutné v modelovém objektu dodržovat určité zásady. Před zprovozněním PZTS se provedou zkoušky, jimiž se prověří soulad funkce namontovaného zařízení s funkcí předepsanou. Zařízení PZTS může být uvedeno do trvalého provozu až po vypracování výchozí revize (dle ČSN 33 2000-1, a ČSN 33 1500). Předání a převzetí musí být provedeno neprodleně po dokončené montáži a po provedené výchozí revizi. Před zprovozněním musí mít uživatel zajištěna režimová opatření pro činnost v případě poplachu a musí zajistit osobu zodpovědnou za provoz, která:

- zodpovídá za provoz zařízení, vede provozní knihu,
- musí být znalá dle ČSN 34 3100[8] a prokazatelně proškolená, provádí prohlídku a údržbu,
- musí být prokazatelně zaškolena montážní firmou.

Před uvedením do trvalého provozu musí být zařízení PZTS podrobeno minimálně 14dennímu nepřetržitému zkušebnímu provozu s vyhodnocením výskytu falešných poplachů.

[8] Bezpečnostní předpisy pro obsluhu a práci na elektrických zařízeních.

Ve smyslu ČSN 33 2000-1[9] musí dodavatel zajistit dokumentaci umožňující stavbu, provoz, údržbu a revizi zařízení. Tato dokumentace musí umožnit zaznamenávání všech změn oproti dokumentaci původní, které vznikly před uvedením systému PZTS do trvalého provozu. Na základě této dokumentace se vypracuje dokumentace skutečného provedení stavby, která je dokladována po celou dobu technicko-ekonomického významu systému PZTS. Do dokumentace skutečného provedení se zaznamenávají změny vzniklé po uvedení systému do trvalého provozu.

5.7.2 Pokyny pro funkčnost CCTV

Před realizací díla budou provedeny komplexní kamerové zkoušky, spojené s případnou korekcí výběru stanovišť tak, aby možné nedostatky (vzhledem k případným nepřesnostem nebo ke změnám provedeným v průběhu stavby) v zobrazení navrženého systému CCTV byly odstraněny. Kamerové zkoušky budou provedeny v podmínkách, ve kterých bude kamera provozována (den, noc, slunečno, zataženo, déšť). Po provedení výchozí revize se CCTV uvede do zkušebního provozu, který prověří nainstalovaný systém. Případně se vzniklé závady prošetří a budou přijata nápravná opatření. CCTV se doporučuje zkušebně provozovat nejméně po dobu 14 dní nebo se zákazníkem odsouhlasenou delší dobu. Po skončení odsouhlaseného období zkušebního provozu je možno zařízení CCTV plně schválit k provozu, pokud se v jeho průběhu nevyskytly závady, nasvědčující o případné provozní nespolehlivosti instalovaného systému.

5.7.2.1 Údržba a oprava CCTV

Na kamerovém systému CCTV bude nutné provádět pravidelné revize, údržbu včetně čištění optiky a venkovních krytů od prachu a kontrolu stability mechanické aretace polohy kamer. Jedenkrát měsíčně se musí provést vizuální kontrola kamer. Tuto kontrolu si zajišťuje uživatel prostřednictvím prokazatelně poučené osoby. Obsluha systému bude dále kontrolovat případné odchylky od normální činnosti systému. Tyto odchylky se musí

[9] Elektrické instalace nízkého napětí. Část 1: Základní hlediska, stanovení základních charakteristik, definice.

neprodleně hlásit servisnímu místu. Zkoušky činnosti zařízení CCTV budou prováděny jedenkrát za půl roku. Jednou ročně bude provedena revize zařízení CCTV. Tato revize bude provedena v půlročním odstupu od zkoušky zařízení a bude nahrazovat jednu půlroční zkoušku činnosti zařízení CCTV. Zkoušky činnosti a revize systému CCTV budou provádět servisní technici. O provedených zkouškách a odchylkách budou prováděny zápisy do provozní knihy CCTV.

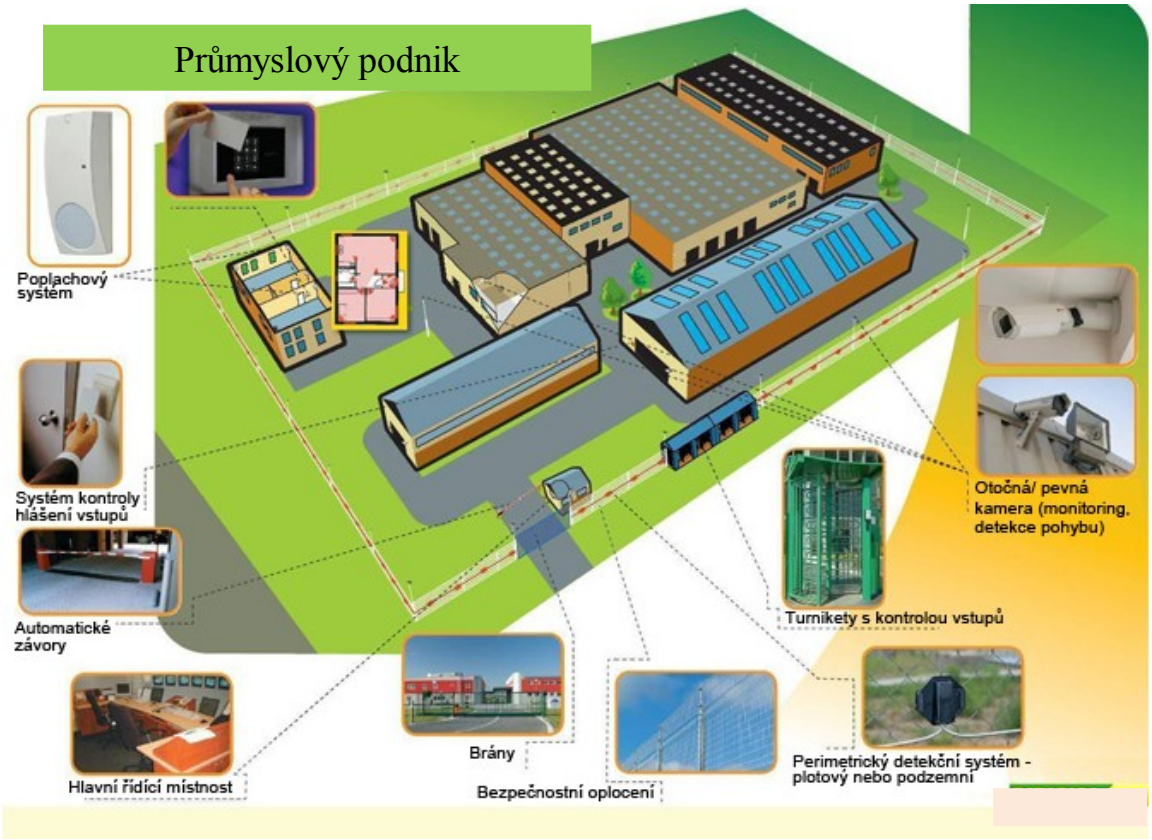
5.7.3 Elektromagnetická kompatibilita (EMC)

Podle zákona o technických požadavcích na výrobky č.22/1997 Sb. a nařízení vlády č. 616/2006 Sb. musí být přístroje včetně vybavení a instalací provedeny a namontovány tak, aby elektromagnetické rušení, které způsobují, nepřesáhlo povolenou úroveň a naopak musí mít odpovídající odolnost vůči vystavenému elektromagnetickému rušení, která jim umožňuje provoz v souladu se zamýšleným účelem.

5.7.4 Bezpečnost a ochrana zdraví při práci

Při výstavbě musí být dodržována ustanovení platných norem a předpisů o bezpečnosti práce. Je nezbytné, aby všichni pracovníci dodavatele byli prokazatelně seznámeni s předpisy o bezpečnosti práce a ochraně zdraví při práci ve všech v úvahu přicházejících prostorách. Montáž zařízení smí provádět pracovníci s předepsanou kvalifikací, proškolení dle vyhlášky č. 50/1978[10] Sb. Z pohledu bezpečnosti práce je dokumentace zpracována dle platných ČSN a bezpečnostních předpisů.

[10] Odborná způsobilost v elektrotechnice.



Obr. 29 Ochrana průmyslového podniku poplachovými systémy [9]

Dílčí závěr

V poslední části diplomové práce práce jsem navrhl technické řešení, které je zpracováno v souladu s doporučením obsahu dokumentu „Návrh skladby systému" dle ČSN CLC/TS 50131-7. Nejprve jsem vymezil požadavky na projekt, uvedl seznam materiálů, blokové schéma, integraci, konfiguraci, obsluhu a údržbu systému. Na závěr uvádím pokyny pro funkčnost PZTS a CCTV. Uvedeným návrhem jsem rozšířil poplachový systém pro perimetrickou ochranu. Tato ochrana je řešena perimetrickým detekčním systémem Peridect a kamerovým systémem. Součástí je i kalkulace navrženého řešení.

ZÁVĚR

V první části diplomové práce jsem provedl analýzu poplachového systému na modelovém objektu průmyslového podniku. Analýza je zaměřena na stávající stav vybraných prvků poplachového systému jako je přístupový a kamerový systém a poplachový zabezpečovací a tísňový systém. Při posouzení analýzy poplachových systémů jsem dospěl k závěru, že vybrané prvky poplachového systému jsou zaměřeny pouze na prostorovou a plášťovou ochranu. Perimetrická ochrana je řešena přístupovým systémem jen v místech vstupu a vjezdu do areálu. Ve zbývajících místech poplachový systém využíván není, spoléhá se pouze na oplocení lemující celý areál. Protože se, ale jedná o velký areál, kde díky velkému množství budov vznikají slabá místa, která jsou vhodná pro narušitele či lupiče, musí být prioritou vytvoření stoprocentní perimetrické ochrany za použití poplachových systémů.

V další části Diplomové práce jsem vymezil rizikové oblasti a doplnil poplachové aplikace na základě bezpečnostního posouzení a analýzy stávajícího stavu. U jednotlivých rizikových míst jako jsou skladovací prostory, výrobní prostory, energo rozvodny a hlavní pozemní komunikace, jsem navrhl možnosti použití poplachového systému a jeho prvků, které lze aplikovat a které povedou ke zkvalitnění stávající ochrany.

V předposlední části se zabývám základními principy integrace poplachových a nepoplachových aplikací a uvádím možnosti integrace ve vymezených oblastech, jako je například povinná identifikace na jednotlivých technologických zařízeních s využitím instalovaného přístupového systému a ovládání osvětlení za pomocí poplachových zabezpečovacích nebo kamerových systémů ve výrobních prostorech a nebo skladech. Propojení poplachového zabezpečovacího a tísňového systému, přístupového a kamerového systému, řízení výtahů, ovládání osvětlení, klimatizace a dalších technologických a administrativních procesů přináší přehled o celkové bezpečnostní situaci objektu, řízení přístupu osob do jednotlivých částí objektu, kontrolu osob v rámci mzdového systému a v neposlední řadě kontrolu odběrů a úsporu energií.

Stěžejní výstup práce představuje v závěrečné části diplomové práce návrh systému, který je zpracován v souladu s doporučením obsahu dokumentu „Návrh skladby systému" dle ČSN CLC/TS 50131-7. V návrhu jsem vymezil požadavky na projekt, uvedl seznam materiálů, dále blokové schéma, integraci, konfiguraci, obsluhu a údržbu systému. Dále jsem navrhl technické řešení, čímž došlo k rozšíření poplachového systému pro perimetrickou ochranu.

Tato ochrana je řešena integrací perimetrickým detekčním systémem Peridect a kamerovým systémem. Součástí je i kalkulace navrženého řešení.

Diplomová práce by měla být inspirací pro zabezpečení perimetrické ochrany průmyslových podniků a jiných rozlehlých areálů s velkým počtem zaměstnanců a otevřeným pohybem mezi výrobními prostory. Průmyslové podniky, které přistupují k zabezpečení integrovanějším způsobem, mají lepší předpoklady k ochraně svého majetku a reputace, ke snížení nákladů, jakož i k poskytnutí lepšího prostředí svým zaměstnancům a kvalitnějších služeb svým zákazníkům.

ZÁVĚR V ANGLIČTINĚ

In the first part of the dissertation I performed an analysis of alarm system on a model object of an industrial company. The analysis is focused on the current state of selected elements of an alarm system such as access control, CCTV and intrusion and hold-up alarm systems. By considering the analysis of alarm systems I came to the conclusion that the selected elements of the alarm system are focused only on the spatial and shield protection. The perimeter protection is designed by access system only at entry to the compound of the industrial company. In the other places is used only fencing around the compound without using an alarm system. But because we are talking about an large compound of an industrial company, where due to too many buildings are formed risky places, which are suitable for the intruders and/or thieves it must be priority to create extra safe perimeter protection by using alarm systems.

In the following part of the dissertation I defined the unsafe zones and added alarm applications in according to the result of security appraisal and the analysis of the current state. For each unsafe place, like are storages, production facilities, energo substation and main rouds I designed the possibility of using an alarm system and its elements, which can be applied and will improve the quality of current protection.

In the penultimate part I am busy with the fundamental principles of alarm and no-alarm applications and I mention the possibilities of the integration of these applications in the determined areas, such as compulsory identification on each technological equipment with using a installed access control system and a lighting control with using the security alarm and camera systems in the production facilities and storages. Interconnection of the intrusion and hold-up alarm system, access and camera systems, the elevator steering, lighting control, air conditioning and other technology and business processes provides an overview of the overall security situation in the building, access control of persons to various parts of the building, checking people within the payroll system and but also the consumption control and saving energy.

The key output of the work present in the last part of the dissertation a system proposal, that is created in accordance with the contents of the document named Proposal of the structure of the system according to ČSN CLC/TS 50131-7. In the proposal I defined the

requirements for the project, mentioned the list of material, block diagram, integration, configuration, operation and maintenance of the system. Further I suggested technical solution, thus exceeding the alarm system for perimeter protection. This protection is designed by the integration of perimeter detection system PERIDECT and CCTV. The work includes also a calculation of the proposed solution.

My dissertation should be an inspiration for perimeter security protection all of industrial company´s and other large compound with a huge number of employees and free movement between production areas. Companies that approach to security of more integrated manner, have better assumptions to protect their property and reputation, to reduce costs as well as providing a better surroundings to its employees and better services to its customers.

SEZNAM POUŽITÉ LITERATURY

[1] BRABEC, František. *Ochrana bezpečnosti podniku*. 1. vyd. Praha: Eurounion, 1996. 203 s. ISBN 80-85858-29-0.

[2] BRABEC, František, Ivo LÁTAL, Rudolf MUSIL, Miloš URBAN, Tomáš VEJLUPEK a Ivan PILNÝ. *Bezpečnost pro firmu, úřad, občana*. Praha: Public History, 2001. ISBN 80-86445-04-06.

[3] LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management. 1. vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.

[4] KINDL, Jiří. Projektování bezpečnostních systémů I. [skriptum]. Zlín: UTB, 2007. ISBN 978-80-7318-554-1.

[5] AKTION. EFG CZ SPOL. S R.O. *Služby a řešení* [online]. [cit. 2012-05-02]. Dostupné z: http://www.aktion.cz/cs.html.

[6] ŘEDITEL DIVIZE ESH. *Směrnice výkonného výboru*: *Řízení činnosti bezpečnostní služby*. Vydání 2. 01.04.2009. 2009, 9 s. S03OS II.

[7] UHLÁŘ, Jan. Technická ochrana objektů: II. díl. Elektrické zabezpečovací systémy. 1. vyd. Praha: Policejní akademie České republiky, 2005. 230 s. ISBN 80-7251-189-0.

[8] KŘEČEK Stanislav. Příručka zabezpečovací techniky. Vydání 3. Blatná: Cricetus, 2006. 315 s. ISBN 80-902938-2-4.

[9] Alkatraz Alarm, s.r.o.: Průmyslové objekty. *Http://www.alkatraz.cz* [online]. [cit. 2012-05-02]. Dostupné z: http://www.alkatraz.cz/prumyslove-objekty-1-14.html.

[10] LOVEČEK, T., NAGY, P. Bezpečnostné systémy: kamerové bezpečnostné systémy. Žilina: Žilinská univerzita v Žilině, 2008. 272 s. ISBN 978-80-8070-893-1.

[11] ČSN CLC/TS 50398. Poplachové systémy- Kombinované a integrované systémy- všeobecné požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. 20 s. Třídící znak 334597.

[12] Objevte nový bezpečný svět. JIŘÍ ŠEJNOHA. *Průvodce integrovanými systémy* [online]. [cit. 2012-05-02]. Dostupné z: http://www.ijs-security.cz/.

[13] ČSN CLC/TS 50131-7. Poplachové systémy- Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. 44 s. Třídící znak 334591.

[14] ČSN EN 50132-7. *Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikaci*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 1999. Třídicí znak: 334592.

[15] Komplexní zabezpečení objektů. SIEZA. *Peridect - perimetrický detekční systém* [online]. [cit. 2012-05-02]. Dostupné z: http://www.sieza.cz/index.html.

[16] SANYO: Produkte - Securite CCTV. [online]. [cit. 2012-05-03]. Dostupné z: http://sanyo.de/products/cctv/cameras/product.asp?lg=D&PID=108&product=VCC-XZN600P&n1=1&n2=6.

[17] C4 Zlepčujeme vašu bezpečnosť. *Oblasti nasadenia integračného bezpečnostného systému C4*: *Priemyselné parky* [online]. [cit. 2012-05-03]. Dostupné z: http://www.c4portal.com/areas-of-service.aspx?lng=sk.

[18] Zákon č. 101/2000 Sb., o ochraně osobních údajů. *Hlava II: Práva a povinnosti při zpracování osobních údajů*: *§ 5, § 13*. vyd. 2000.

[19] ČSN 33 2000-1 ed. 2. *Elektrické instalace nízkého napětí - Část 1: Základní hlediska, stanovení základních charakteristik, definice*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. Třídicí znak: 332000.

[20] ČSN EN 61140 ed. 2. *Ochrana před úrazem elektrickým proudem - Společná hlediska pro instalaci a zařízení*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2003. Třídicí znak: 330500.

[21] ATIS group s.r.o.: Zabezpečovací ústředna. [online]. [cit. 2012-05-03]. Dostupné z: http://www.atisgroup.cz/show_product.php?id=019+00200.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AB – administrativní budova.

ACS – přístupový systém.

C4 – vizualizační program, integrační bezpečnostní systém, otevřený modulární systém, který umožňuje monitorovat jednu samostatnou budovu, nebo robustní řešení monitorující různá bezpečnostní zařízení velké organizace ve všech jejích objektech bez ohledu na vzdálenost.

CCTV – uzavřené televizní okruhy používané pro účely zabezpečení a dohledu.

PPC – poplachová přijímací centra.

DVR – digitální videorekordér.

HDD – pevný disk, k ukládání dat.

HZSP – hasičský záchranný sbor podniku.

Integrace – sjednocení, ucelení, splynutí, proces spojování ve vyšší celek.

I&HAS – (Intrusion and hold-up alarm systems) poplachové zabezpečovací a tísňové systémy.

MW detektor – k prostorové detekci pohybu osob (vnitřní/venkovní).

PS – poplachový systém.

PIR detektor – detektor pohybu osob, je určen k prostorové ochraně objektů (vnitřní/venkovní).

PZTS – poplachový zabezpečovací a tísňový systém.

RACK - je standardizovaný systém umožňující přehlednou montáž a propojování různých elektrických a elektronických zařízení spolu s vyústěním kabelových rozvodů do sloupců nad sebe v ocelovém rámu.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK