Aplikace kamerového dohledového systému pro automatické střežení perimetru

Application of Video Surveillance Systems for Automatic Perimeter Observation

Bc. Jan Procházka

Diplomová práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan Procházka**
Osobní číslo:	**A14343**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Aplikace kamerového dohledového systému pro automatické střežení perimetru**
Téma anglicky:	**A Video Surveillance System Application for Automatic Perimeter Observation**

Zásady pro vypracování:

1. **Zpracujete trendy v bezpečnostních systémech ochrany perimetru.**
2. **Analyzujte integraci bezpečnostních systémů ochrany perimetru.**
3. **Komparujte technický systém perimetru a jeho technické prvky.**
4. **Vytvořte komparativní studii střežení perimetru prostřednictvím vybraných systémů střežení.**
5. **Aplikujete kamerový dohledový systém pro automatické střežení perimetru.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **NILSSON, Fredrik., c2009. Intelligent network video: understanding modern video surveillance systems. 2. Boca Raton: CRC Press. ISBN 14-200-6156-9.**
2. **ANTHONY C. CAPUTO., 2014. Digital video surveillance and security. Second edition. Amsterdam: Butterworth-Heinemann. ISBN 978-130-6516-037.**
3. **AGHAJAN, Hamid K. a Andrea. CAVALLARO, c2009. Multi-camera networks: principles and applications. 1. Boston: Elsevier, AP. ISBN 01-237-4633-7.**
4. **LUKÁŠ, Luděk, 2015. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-05-7.**
5. **HALOUZKA, Kamil, 2014. Fyzická bezpečnost: Perimetrické zabezpečovací systémy. Brno. Projekt: Vzdělávání pro bezpečnostní systém státu. Univerzita obrany.**

Vedoucí diplomové práce: **Ing. Jiří Ševčík**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **3. února 2017**

Termín odevzdání diplomové práce: **24. května 2017**

Ve Zlíně dne 3. února 2017

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování 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/bakalářské 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, dne 14. 5 2017

.....
podpis diplomanta

ABSTRAKT

Teoretická část práce se zaobírá soudobými trendy ochrany perimetru. Postupně seznamuje s jednotlivými systémy ochrany perimetru, jako jsou mechanické zábranné systémy, poplachové zabezpečovací a tísňové systémy a kamerové systémy. Závěrečná kapitola je věnována integraci bezpečnostních systémů a jejich vzájemné spolupráci.

Praktická část práce se věnuje integraci bezpečnostních systémů pro potřeby velké výrobní společnosti. Čtenář je seznámen se současnými systémy ochrany perimetru, které jsou porovnány s dalšími systémy dostupnými na trhu. Závěrečná část práce je věnována konkrétní integraci kamer od výrobců Axis a Hikvision s detekčním systémem Peridect prostřednictvím integrační platformy C4.

Klíčová slova: VDS, MZS, PZTS, IP kamerové systémy, perimetr

ABSTRACT

The theoretical part thesis is concerned with contemporary trends of perimeter protection. The reader is gradually acquainted with individual perimeter protection systems such as Barrier Systems, Intrusion and hold-up Systems, and Camera Systems. The final chapter is devoted to the integration of security systems and their mutual cooperation.

The practical part deals with the integration of security systems for the needs of a large production company. The reader is gradually acquainted with current perimeter protection systems that are compared to other systems available on the market. The final part is devoted to the specific integration of cameras from Axis and Hikvision manufacturers with the Peridect detection system through the integration platform C4.

Keywords: VSS, MZS, I&HAS, integration, perimeter

Tímto bych rád poděkoval mému vedoucímu Ing. Jiřímu Ševčíkovi za vedení, uvedení do tématu a cenné rady, kterými se podílel na mé diplomové práci. Dále bych rád poděkoval pánům Pavlu Poláškovi a Ing. Janu Pavlíčkovi za jejich pomoc a materiály. V neposlední řadě bych rád poděkoval mé rodině, která mě podporovala po celou dobu mého studia.

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

OBSAH

ÚVOD

Původ slova perimetr vychází z řeckých slov peri (kolem, dokola) a metron (měřidlo), s první použitím tohoto slova můžeme setkat v 15. století v matematice a lze ho definovat jako dvoudimenzionální uzavřený prostor.

Ochrana perimetru patří mezi nejnáročnější typy zabezpečení jak z pohledu finančního, tak i náročnosti na provedení a nastavení. Ale v případě správného použití skýtá velkou výhodu včasného zachycení pachatele a minimalizování možné škody. Při reálném použití je perimetrická ochrana nejčastěji umělou překážkou (plot, zeď), která uzavírá prostor a společně se vstupy do objektu ho ohraničuje. Důležité je jasné oddělení vnitřních a vnějších prostor tak, aby nedocházelo k náhodným vstupům do střeženého perimetru. Samotná umělá překážka v podobě plotu nebo zdi ale neposkytuje příliš vysokou ochranu, a proto je třeba tyto mechanické zábranné prostředky doplnit o další prvky perimetrické ochrany, aby tak společně vytvořily funkční systém ochrany perimetru. Mezi další prvky, které nejčastěji doplňují mechanické zabrané prostředky, patří: poplachový zabezpečovací a tísňový systém a kamerové systémy.

Ochrana perimetru je vždy spojena s režimovými opatřeními, která jasně definují oprávnění ke vstupu do chráněného perimetru a vytvářejí pravidla pro pohyb v chráněném prostoru.

Dnešním trendem při ochraně perimetru je spojení perimetrické neboli obvodové ochrany s ochranou prostorovou, kdy je případný pachatel zaznamenán již krátce před překročením vyhraničeného perimetru a jeho monitorování pokračuje i v daném chráněném perimetru. Při tomto typu střežení dochází k vytvoření zón s různými typy poplachu.

I. TEORETICKÁ ČÁST

Trendy v bezpečnostních systémech ochrany perimetru

Ochrana perimetru má za sebou dlouhou historii a postupně prošla velkým množstvím změn od dřevěných palisád kolem prvních lidských osad po dnešní vyspělé technologie, které umožňují v reálném čase chránit celé země nebo rozsáhlá území jako je Schengenský prostor.

Aby perimetrická ochrana správně plnila svou funkci, musí jít o komplexní bezpečnostní řešení, ve kterém dochází k propojení režimových opatření v chráněném objektu, fyzické ochrany, mechanických zábranných a technických opatření určených k detekci a zpomalení případného pachatele.

V oblasti perimetrické ochrany můžeme sledovat prudký nárůst nových řešení a využití nových technologií, které stále více doplňují strážní službu a navyšují bezpečnost. Každý z výrobců se částečně vydává svou vlastní cestou, jakým způsobem vytvořit a propojit tyto systémy. V dalších bodech se práce věnuje postupně jednotlivým trendům ochrany perimetru, které jsou dostupné na trhu, a jejich integraci při vytváření komplexního řešení ochrany perimetru.

1 MECHANICKÉ ZÁBRANNÉ SYSTÉMY PERIMETRICKÉ OCHRANY.

Ačkoliv se jedná o nejstarší typ perimetrické ochrany, patří k nejvíce využívaným a velice populárním. Jejich primárním účelem je zabránit neúmyslnému narušení perimetru, dále pak zpomalit pachatele, případně ho odradit svou robustností.

Kvalitu mechanických zábranných systémů lze určit podle průlomového času, který pachatel potřebuje k překonání mechanické zábrany. Vždy je třeba zhodnotit, jaké znalosti a prostředky má pachatel k dispozici pro překonání mechanické zábrany. Pro základní výpočet lze použít vzorec 1. Kde Δ_t je časový rozdíl mezi časem napadení objektu $\mathbf{t_1}$ a časem dokončení napadení objektu $\mathbf{t_2}$. [1]

$$\Delta_t = t_2 - t_1 \ [s] \tag{1}$$

Při výpočtu je třeba vycházet z normy ČSN EN 1627, která definuje šest bezpečnostních tříd a vychází z evropské normy EN 1627. [2**Chyba! Nenalezen zdroj odkazů.**]

Pro tyto třídy je definován minimální průlomový čas, po který musejí obstát v případě napadení pachatelem s přesně definovanými prostředky a schopnostmi.

Obrázek 1. Bezpečnostní třídy dle normy EN 1627. [3]

Tabulka 1. Charakteristiky bezpečnostních tříd u mechanických zábranných systémů. [4]

Bezpečnostní třída RC	*Čas napadení*	*Předpokládané metody a pokusy o napadení*
RC 1	Neaplikuje se	Příležitostný zloděj se pokouší o vloupání s použitím malého jednoduchého nářadí a fyzickým násilím, např. kopáním, naražením ramenem, zdviháním, vytrháváním. Zloděj nemá žádné zvláštní znalosti o úrovni odolnosti mechanických zábranných systémů (MZS), má málo času a snaží se nezpůsobit hluk.
RC 2	3 min	Příležitostný zloděj se navíc pokouší o vloupání s použitím jednoduchého nářadí a fyzickým násilím. Má malé znalosti o úrovni odolnosti MZS, má málo času a snaží se nezpůsobit hluk.
RC 3	5 min	Zloděj se pokouší překonat MZS při použití páčidla délky 710 mm a dalšího šroubováku, ručního nářadí, jako malé kladívko, důlčíky a mechanická ruční vrtačka. Zloděj má určité povědomí o systému uzávěru a s tímto nářadím je schopen těchto znalostí využít. Při použití páčidla délka 710 mm lze aplikovat zvýšené fyzické násilí.
RC 4	10 min	Zkušený zloděj používá navíc zámečnické kladivo, sekeru, dláta, sekáče, přenosnou akumulátorovou vrtačku atd. Toto další nářadí umožňuje zloději rozšířit počet způsobů napadení, případně jejich kombinace – vrtání, sekání, páčení, atd. Problém hluku zloděj neřeší.
RC 5	15 min	Velmi zkušený zloděj používá navíc jednoruční elektrické nářadí např. úhlovou brusku do průměru kotouče 125 mm, přímočarou pilu atd. Neznepokojuje se hlukem.
RC 6	20 min	Velmi zkušený zloděj používá navíc dvouruční elektrické nářadí např. úhlovou brusku do průměru kotouče 230 mm, přímočarou pilu atd. Neznepokojuje se hlukem.

Mechanické zábranné prostředky, které jsou použity při ochraně perimetru, se dále dělí na:

Umělé oplocení:

- klasické drátěné.
- dřevěné.
- zděné.
- bezpečnostní.
- vysoce bezpečnostní.

Vstupy, vjezdy a jiné jednotky:

- branky.
- brány.
- závory.
- turniket.
- bezpečnostní propusti.

Doplňkové zábrany:

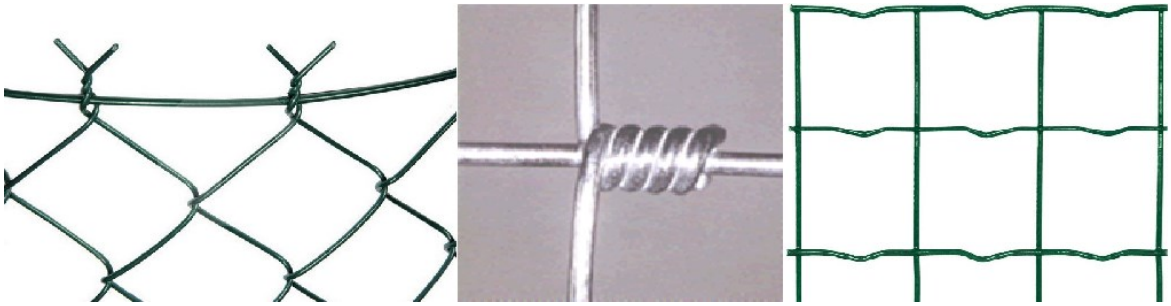
- vrcholové zábrany.
- podhrabové překážky.

1.1 Umělé oplocení

1.1.1 Klasické drátěné oplocení

Klasické drátěné oplocení patří mezi nejběžnější způsoby ochrany a ohraničení perimetru. Je tvořeno železným drátem, který může být ošetřen různými povrchovými úpravami, jako je nátěr nebo poplastování. Samotné pletivo je nataženo mezi sloupky, které ho udržují v kolmé pozici proti zemi. Maximální vzdálenost mezi dvěma slupky by neměla překročit tři metry. U klasického drátěného oplocení se nejčastěji setkáváme s těmito typy:

- **Čtvercové pletivo** nejběžněji nasazovaná varianta, slouží prakticky pouze k vyznačení perimetru, pro případného pachatele nepředstavuje vážnější překážku. Je tvořeno oky o velikosti 5x5 cm s průměrem drátu 2,2-4,4 mm. Výška tohoto pletiva se běžně pohybuje od 1 do 3 m.
- **Cyklonové pletivo** jeho výhodou oproti čtvercovému pletivu je typické zapletení železného drátu, což znesnadňuje rozpletení a zvyšuje odolnost. Běžně se vyrábí v průměru od 2,5-3 mm.
- **Svařované pletivo** vyrobeno z pevného železného drátu svařeného do ok o velikosti 50x50 mm. Tento typ pletiva vyniká v pevnosti oproti dvěma předešlým a je vhodný do horších klimatických podmínek. Svařované pletivo může mít proměnnou velikost ok, kdy jsou ve spodu nejmenší a postupně se zvětšují směrem vzhůru.



Obrázek 2. Klasické drátěné oplocení z leva čtvercové pletivo [5], cyklonové pletivo [6] a svařované pletivo. [7]

1.1.2 Dřevěné a zděné oplocení

Dřevěné a zděné oplocení nachází své využití převážně u rodinných domů a zahrad, kdy odděluje privátní a veřejný prostor. Nasazení tohoto druhu oplocení při ochraně větších objektů není příliš běžné z důvodů pořizovacích a provozních nákladů. Specifickou vlastností je neprůhlednost, tato vlastnost může být k užitku (větší soukromí ve střeženém pro-

storu), ale může znemožnit činnost kamer a poskytnout pachateli krytý prostor, v němž nelze provádět vizuální kontrolu.

1.1.3 Bezpečnostní oplocení

Splňuje vyšší nároky na zabezpečení prostor. Oproti klasickému oplocení se liší svou konstrukcí, která je odolnější a využívá materiály, jako je ocel a beton. Tento typ oplocení se běžně používá na ochranu průmyslových objektů, vodních zdrojů nebo školních pozemků. Bezpečností oplocení může dosahovat výšky až 2,5m a často bývá doplněno o vrcholové zábrany.

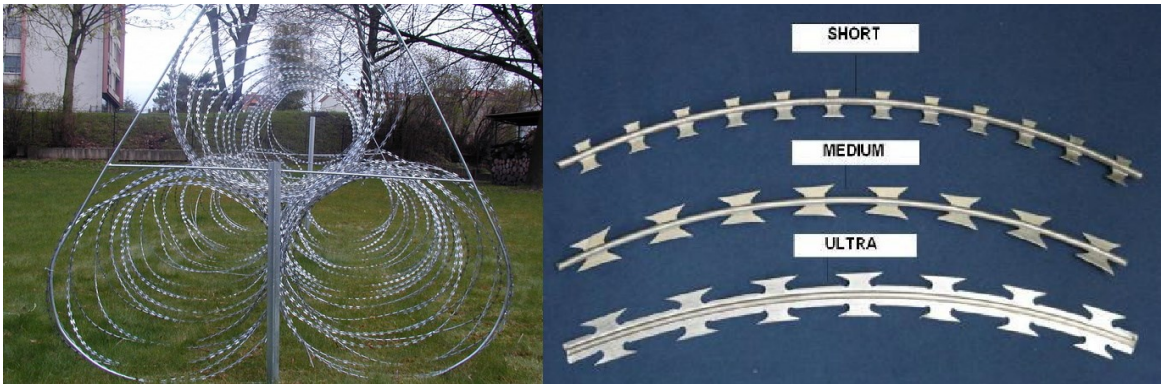
- **Pletivo z vlnitého drátu** je podobné klasickému čtvercovému drátěnému oplocení, výhodou je vlnitost drátu, která znesnadňuje rozpletení. Na horní části je zpevněno horizontálními dráty a zakončené ochrannými trny s délkou 50 mm, které tvoří jednoduchou vrcholovou zábranu, tím znesnadňují přelezení plotu. Pevnost jednotlivých drátů je vyšší než u klasického čtvercového pletiva. [6]
- **Svařované zvlněné pletivo** je opět podobné klasickému svařovanému pletivu s výškou přes 2 m. Tento typ je vyráběn v mnoha variacích často doplňován o trny na horní časti, znesnadňující překonání. Ukotvení je možné jak v zemi, tak i na mobilních betonových blocích, které umožní mobilní výstavbu a dodávají plotu potřebnou stabilitu. Velkou výhodou svařovaného zvlněného pletiva je, že je díky svaření jednotlivých drátů prakticky zabráněno jeho rozpletení. [6]
- **Mřížové oplocení** patří mezi nejvíce estetické a efektivní řešení perimetrické ochrany. Na trhu je velké množství výrobců mřížového oplocení a při výběru je důležité, zaměřit se na použitý materiál a možnost nerozebíratelných spojení jednotlivých dílů.

Obrázek 3. Bezpečnostní oplocení zleva pletivo z vlnitého drátu [6], svařované zvlněné pletivo [7] a mřížové oplocení. [8]

- **Bariéry a oplocení ze žiletkového drátu,** který postupně nahrazuje známější ostnatý drát. Již samotný vzhled toho opocení má vysoký psychologický účinek na případného pachatele. Pachatel, který by se pokusil překonat tento typ mechanické zábrany, riskuje pořezání a uvíznutí v oplocení. [6]

  Samotný drát je vyroben z vysoce tažného ocelového drátu, který je obtížné přestříhnout nebo jinak poškodit. Jeho obvyklý průměr je 2,5mm a v pravidelných rozestupech jsou připevněny ostré „žiletky“. [6]

  Žiletkový drát se dá využít jako vrcholová zábrana nebo jako samostatná zábrana, kdy je několik cívek železného drátu spojeno a vytváří cívkovou barieru. Výhodou žiletkového drátu je možnost mobilního použití, kdy z připravených cívek je v rámci několika minut odvinuta mobilní bariera. [6]



Obrázek 4. Mobilní uspořádání žiletkového drátu v pyramidě a typy žiletkových drátů. [9]

1.1.4 Vysoce bezpečnostní oplocení

Nejvyšší stupeň bezpečnostního oplocení využívaný převážně pro ochranu kritické infrastruktury a dalších citlivých objektů, jako jsou nápravná zařízení, vojenské a sportovní objekty. V této kategorii oplocení se již prakticky vždy bezpečnostní oplocení doplňuje vrcholovými zábranami a často i podhrabovými překážkami. [6]

- **Rovný plot**, je tvořený pozinkovanými ocelovými stožáry, mezi kterými je natažená jedna nebo i dvě vrstvy speciálního nerozebíratelného pletiva s malými oky, které znemožňují zachycení rukou v okách plotu, tím znesnadňují jeho přelezení.

  Typickým představitelem vysoce bezpečnostního oplocení je pletivo **Atlas,** které se svou výškou až 4 m, průměrem drátu 3,9-4 mm a velikostí oka 76,2 x 12,7 představuje absolutní špičku na trhu. Speciální velikost ok znesnadňuje přestřižení jednotlivých drátů. [10]

Dalšími velice často nasazovanými pletivy jsou pletiva **Bastila** a **Axis**, která se taktéž specializují na vysoce bezpečnostní oplocení.

- **Zakřivený plot** se nejčastěji využívá ve věznicích a při ochraně průmyslových staveb. Zakřivený plot patří k nejhůře překonatelným, což je dáno jeho výškou, která může být až 4,5 m, tak i jeho zakřivením, které prakticky neumožňuje zachycení na horní hraně plotu. Zakřivení by mělo směřovat na stranu, ze které se předpokládá pokus o přelezení a vytvářet umělý převis nad případným pachatelem. Zde se již nejedná pouze o plot, ale jde o komplexní řešení často vyráběné a prováděné na zakázku. [6]

  Představitelem zakřiveného plotu může být **Zaun's Flexible Steel Topping (FST),** který byl schválen ve Velké Británii pro nasazení ve věznicích s nejvyšší mírou ostrahy. [11]

Obrázek 5. Vysoce bezpečnostní oplocení zleva zakřivený plot FST [11] a rovný Atlas. [10]

1.2 Vstupy, vjezdy a jiné jednotky

Při vytváření chráněného perimetru je důležité zajistit vstupy do chráněného perimetru tak, aby byla rizika plynoucí z těchto vstupů na co nejnižší úrovni. Je důležité, aby byla vytvořena režimová opatření pro pohyb uvnitř střeženého perimetru. Jakýkoliv vstup je potenciálním rizikem, a proto je třeba, aby byly vstupy jasně označeny, jejich počet je na nezbytné omezit minimum.

Při nejvyšším stupni ochrany se vstup do chráněné zóny řeší takzvaným dvoutaktním způsobem, kdy vede vstup na pozemek přes dva vstupy, mezi kterými je kontrolní zóna zame-

zující přímému průchodu. Tento způsob je nasazován ve věznicích a podobně vysoce střežených objektech. [1]

1.2.1 Branky

Branky jsou mechanická zařízení, která slouží k uzavírání vstupů na oplocené nebo jinak ohraničené pozemky. Se vstupními brankami se setkáváme spíše u rodinných domů a zahrad, kde umožňují pěší vstup do chráněného perimetru. Branka by měla splňovat stejné bezpečnostní nároky, jaké jsou kladeny na oplocení. Nejběžnějším způsobem uzavírání je pomocí zámkové vložky (cylindrická, dozická nebo motýlková), která musí být uzpůsobena pro venkovní použití.

Branky lze dělit na kovové, které jsou tvořeny ze svislých nebo vertikálních mříží, a na rámové, kde je pevný rám branky vyplněn pletivem.

Obrázek 6. Branky kovová a rámová. [12]

1.2.2 Brány

Jsou mechanická zařízení, která slouží k uzavírání vstupů do chráněného perimetru. Brány lze dělit podle více parametrů, jako je způsob otevření:

- **Otočné brány:** jedno nebo dvě křídla brány jsou zavěšena v závěsech na sloupcích. Brána je otevírána ve směru příjezdové cesty a to buď na venkovní stranu, nebo do chráněného perimetru. Nevýhodou tohoto řešení je vyšší zátěž sloupků a složitější elektrická instalace.
- **Posuvné brány:** k otevírání dochází souběžně se směrem plotu. V otevřeném stavu jsou vrata umístěna paralelně s plotem uvnitř střeženého perimetru. Při uzavření vrat dojde k jejich vysunutí, tím i k uzavření perimetru. Ukotvení pohyblivého kří-

dla je buď samonosné, nebo využívá kolejnice, která umožní pojezd. Tento typ brány je velice často využívá pojezdu v kolejnici a zajištění na obou stranách brány proti vytržení, díky čemuž poskytuje vysokou mechanickou odolnost.

- **Výsuvné** brány fungují podobně jako posuvné s tím rozdílem, že místo pohybu do strany dochází k jejich vytažení vzhůru. Výsuvné brány se příliš nepoužívají při ochraně perimetru ale při vjezdu do budov.

Obrázek 7. Typy bran zleva otočné [13] posuvné [14] a výsuvné. [15]

1.2.3 Závory

Závory mohou sloužit jako doplněk k perimetrické ochraně, ale samy o sobě prakticky neposkytují žádnou ochranu. Nejběžněji se používají společně s bezpečnostní službou, která díky nim snadněji reguluje pohyb vozidel přijíždějících do střeženého perimetru. Další možností použití je propojení závory s identifikačním zařízením nejčastěji s RFID kartou, díky tomu umožní vjezd pouze vybraným vozidlům.

Obrázek 8. Závory. [16]

1.2.4 Turnikety

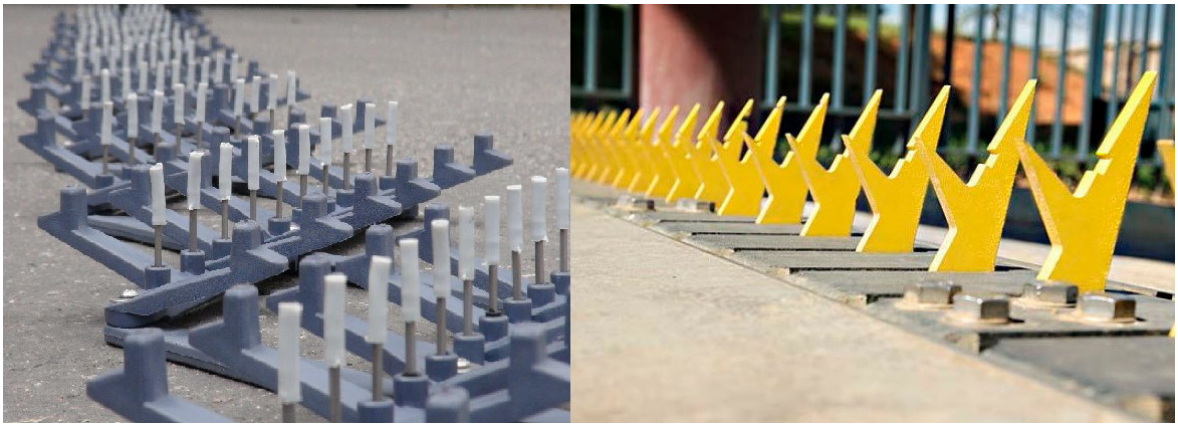
Turnikety nacházejí své uplatnění v rozlehlých objektech, jako jsou velké společnosti, fotbalové stadiony nebo letiště. Turnikety lze rozdělit na **nízké** nejčastěji součástí recepce pod dohledem bezpečnostní služby, nebo **vysoké**, které umožňují jednosměrný vstup do perimetru nebo výstup z perimetru.

Obrázek 9. Turnikety vysoký [16] a nízký [17]

1.2.5 Bezpečnostní propusti

Slouží k regulaci a nouzovému zastavení vozidel, která nerespektují dopravní značení, případně prorazí klasickou závoru. Cílem bezpečnostních propustí je na rozdíl od většiny závor zastavit vozidlo i za cenu jeho poškození nebo i zničení. Z tohoto důvodu není možné tyto propusti instalovat do běžného provozu a je třeba je užívat rozvážně.

Základní dělení bezpečnostních propustí je na mobilní a stálé. Při ochraně perimetru mohou být nasazeny obě varianty.



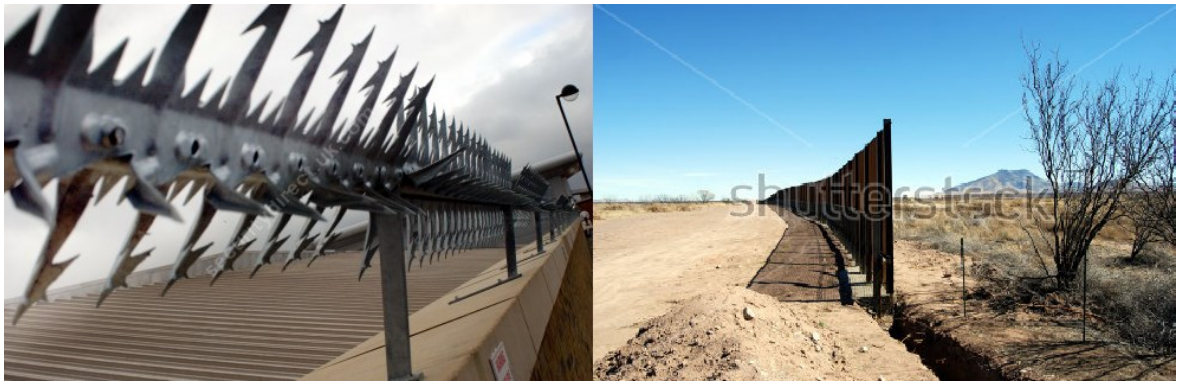
Obrázek 10. Bezpečnostní propusti mobilní [18] a stálá varianta. [19]

Mezi bezpečnostní propusti dále patří různé druhy zastavovacích pásů, speciálních turniketů a jiné prvky.

1.3 Doplňkové zábrany

Doplňkové zábrany složí k navýšení bezpečnosti a jsou využívány společně s ostatními prvky mechanického zabezpečení. Nejčastěji se setkáváme se dvěma typy, což jsou vrcholové zábrany a podhrabové překážky. [6]

- **Vrcholové zábrany**. Cílem vrcholových zábran je zabránit překonání oplocení přelezením. Vrcholové zábrany působí jak na psychiku potencionálního pachatele, tak vytvářejí i účinný mechanický zábranný prostředek. Jako vrcholové zábrany se nejčastěji používají: nástavce s ostnatým drátem, bariery ze žiletkového drátu, pevné a otočné hroty.
- **Podhrabové překážky** zabraňují jednoduchému podhrabání nebo podlezení plotu. Na jejich vybudování je třeba myslet ještě před samotnou stavbou plotu. Nejčastěji se používají podhrabové desky, zděný plot nebo ocelové rošty.



Obrázek 11. Doplňkové zábrany pevné hroty [20] a podhrabové desky. [21]

1.4 Dílčí závěr

První kapitola této práce je věnována mechanickým zábranným systémům. Mechanické zábranné systémy představují ve většině případů nenahraditelný pilíř ochrany perimetru, který ho jasně ohraničuje. Cílem této kapitoly je sumarizovat informace o současných trendech v oblasti mechanických zábranných systémů a představit jednotlivé typy těchto systémů. Při popisu těchto systémů je postupováno od základních systémů s menší úrovní odolnosti po až systémy s velmi vysokou odolností a bezpečností.

2 POPLACHOVÉ ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY VYUŽÍVANÉ PŘI OCHRANĚ PERIMETRU

Poplachový zabezpečovací a tísňový systém (PZTS) často doplňuje mechanické zábranné prostředky, které slouží primárně ke zpomalení a odstrašení případného pachatele. V případě, že má pachatel trestné činnosti dostatek času a prostředků k překonání mechanických zábranných systémů, tak mechanické zábranné systémy nejsou schopny zajistit požadovaný stupeň zabezpečení. Z tohoto důvodu jsou mechanické zábranné prostředky doplňovány o prvky PZTS, které signalizují narušení a umožňují včasný zásah bezpečnostní služby. [22]

Systém PZTS se dále dělí následovně:

- **Poplachový zabezpečovací systém** slouží k detekování vniknutí nebo pokusu o vniknutí narušitele do střeženého prostoru. Dále pak může vyhodnocovat pohyb narušitele ve střežené zóně.
- **Poplachový tísňový systém** umožňuje uživateli vyvolat úmyslně poplachový stav a tímto způsobem informovat o mimořádné události.
- **Poplachový zabezpečovací a tísňový systém** je kombinací dvou předešlých systémů (poplachového zabezpečovacího, poplachového tísňového).

2.1 Stupeň zabezpečení u PZTS

Norma ČSN EN 50131-1 udává čtyři základní stupně zabezpečení, které napomáhají při návrhu PZTS zabezpečení. Stupně jsou vytvořeny na základě předpokládaného pachatele, jeho znalostí a vybavení. Tyto stupně se využívají jak pro zabezpečení objektů kritické infrastruktury (jaderné elektrárny, sklady zbraní, vojenské objekty), tak i pro pojišťovny, které na základě stupně zabezpečení určí maximální výši pojistné částky. [23]

- **Stupeň 1:** nízké riziko (byty, domy, garáže a menší provozovny). Předpokládaný pachatel má malé znalosti PZTS a disponuje pouze omezenými běžně dostupným nástroji.
- **Stupeň 2:** nízké až střední riziko (obchody s elektronikou, skladiště, provozovny s větším rizikem). Předpokládaný pachatel má určité znalosti ohledně PZTS a disponuje základním sortimentem nástrojů.

- **Stupeň 3:** střední až vysoké riziko (obchody se zbraněmi, klenotnictví, pošty). Předpokládaný pachatel disponuje úplným množstvím nástrojů a má znalosti ohledně poplachových zabezpečovacích a tísňových systémů.
- **Stupeň 4:** vysoké riziko (jaderné elektrárny, sklady vojenského materiálu, sklady rizikových chemikálií). Předpokládaný pachatel disponuje plánem PZTS a je vybaven nástroji k jeho nahrazení.

2.2 Třídy prostředí využívaných u PZTS

U prvků PZTS a zvláště u prvků perimetrické ochrany je třeba brát ohled na typ prostředí, ve kterém je daný komponent nasazen tak, aby bylo zaručeno jeho správné fungování. Tyto požadavky definuje norma ČSN EN 50130-5 ed.2 a dělí prostředí do čtyř tříd. Každý výrobce je povinen uvést třídu prostředí v technické dokumentaci daného výrobku. [24]

- **Třída I-vnitřní.**

Nejčastěji trvale obydlené prostory, kde se teplota pohybuje od +5 °C až +40 °C bez extrémní vlhkosti a její kondenzace.

- **Třída II vnitřní všeobecné.**

Obvykle jde o vnitřní prostory, které nejsou trvale obydleny (chodby, sklady). Předpokládané rozmezí teplot je od -10 °C až +40 °C. Při střední relativní vlhkosti 75 % bez kondenzace.

- **Třída III venkovní chráněné nebo extrémní vnitřní podmínky.**

Popisuje vlivy prostředí vyskytující se obvykle vně budovy, komponenty bezpečnostního systému nejsou plně vystaveny povětrnostními vlivům. Teplotní rozsah je od -25 °C až 50 °C při střední relativní vlhkosti 75 % bez kondenzace. Po dobu 30 dní se mohou v průběhu roku změny relativní vlhkosti pohybovat v rozmezí 85 % až 95 % bez kondenzace.

- **Třída IV venkovní všeobecné.**

Vlivy prostředí vyskytující se obvykle vně budovy, přičemž komponenty jsou plně vystaveny povětrnostním vlivům. Předpokládaný rozsah teplot je -25 °C až +60 °C při střední relativní vlhkosti 75 % bez kondenzace. Po dobu 30 dní se mohou v průběhu roku změny relativní vlhkosti pohybovat v rozmezí 85 % až 95 % bez kondenzace.

2.3 Typy PZTS ústředen

Ústředna plní v systému PZTS nezastupitelnou roli, kdy spravuje veškeré informace přicházející z detektorů, klávesnic a dalších prvků a na základě těchto informací vyhlašuje poplach. Existuje velké množství výrobců bezpečnostních komponentů, kteří vyrábějí ústředny, nebo prvky, které by se daly za ústředny označit. Cílem této práce je zabývat se prvky perimetrické ochrany a z tohoto důvodu bude uvedeno pouze základní dělení podle způsobu připojení detektorů k ústředně.

- **Kabelové:** spolehlivé, nižší cena, vyšší úroveň zabezpečení proti rušení, větší množství dostupných prvků na trhu, výrazně složitější instalace vyplývající z kabelových rozvodů. Kabelové ústředny se dále dělí podle způsobu připojení detektorů k ústředně na **smyčkové** a **sběrnicové.**
    - Smyčkové ústředny (analogové) využívají pro detekci poplachu takzvaných smyček a změny odporu v dané smyčce, ke kterému dojde v případě vyhlášení poplachu na detektoru. Na jedné smyčce může být připojeno i více analogových detektorů. Nejčastějším typem zapojení v detektoru jsou NC (normally closed) a NO (normally open)
    - Sběrnicové ústředny (digitální), veškerá komunikace probíhá přes datovou sběrnici. Každý detektor má svou vlastní adresu, přes kterou komunikuje s ústřednou. Výhodou je přená lokace poplachu.
- **Radiové** – snadná instalace, možnost snadného dodatečného rozšíření systému, menší spolehlivost při přenosu signálu, snadnější napadení systému pomocí rušičky.
- **Hybridní** – kombinace předešlých typů.

2.4 Typy PZTS detektorů využívaných u perimetrické ochrany

Vybrat ten správný typ detektoru pro nasazení při ochraně perimetru představuje náročný úkol z důvodu venkovního prostředí, které je náchylné k rušivým jevům, jako je počasí, hromadná doprava, divoce žijící zvířata a další jevy, se kterými je třeba počítat již od samotného návrhu zabezpečení.

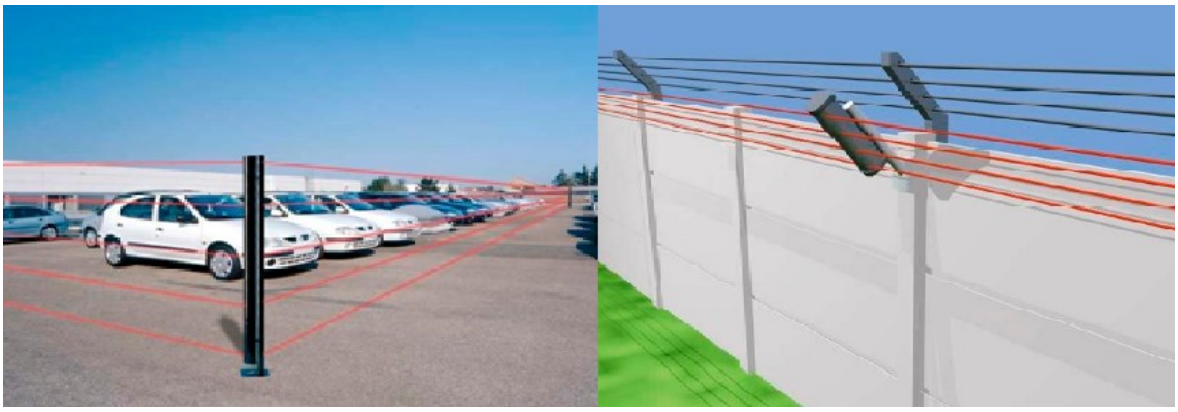
V současné době se při ochraně perimetru nejčastěji využívají tyto typy PZTS detektorů: [1]

- Infračervené bariéry.
- Mikrovlnné bariéry.
- Plotové detekční prostředky.
- Systémy se zemními detekčními kabely, hadicemi a detektory.
- Laserové detektory.
- Venkovní PIR detektory.
- Kombinované detektory.

2.5 Infračervené bariery

Princip fungování je založen na vysílací a přijímací jednotce, které jsou od sebe vzdáleny nejčastěji desítky až stovky metrů. Samotný princip fungování je založen na infračerveném paprsku, který je vyslán z vysílací jednotky (vysílače) a zachycován v přijímací jednotce (přijímači). Infračervená bariera je tvořena více infračervenými paprsky, které utvářejí detekční zónu. V případě přerušení těchto paprsků dochází k vyhlášení poplachu. Pokud je použit jen jeden paprsek, tak se jedná o infračervenou závoru, která neposkytuje příliš vysokou ochranu.

Instalace infračervené bariery může být provedena jako PZTS doplněk k bezpečnostnímu oplocení tak i samostatně, viz Obrázek 12.



Obrázek 12. Infračervená bariera použitá samostatně i jako doplněk MZS. [24]

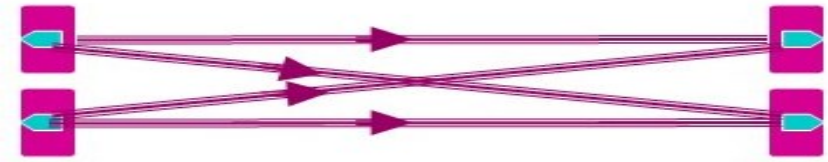
2.5.1 Způsob přenosu infračerveného paprsku

Samotný infračervený paprsek o vlnové frekvenci 900nm je pouhým okem neviditelný a pro jeho přenos se využívá několik způsobů:

- **Stálý přenos paprsku -** infračervený paprsek je po celou dobu provozu vyzařován z vysílače a zachycován v přijímači. Tento jednoduchý typ přenosu nezaručuje vysokou spolehlivost a je náchylný na falešné poplachy. [25]

Obrázek 13. Jednoduchý přenos signálu u infračervené bariery. [25]

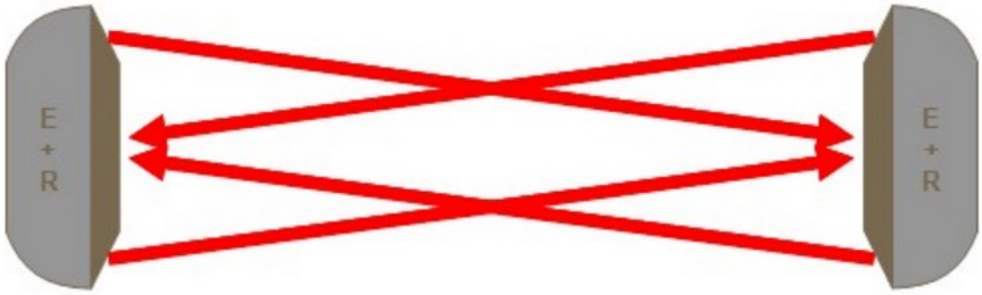
- **Pulzní přenos paprsku -** k přenosu dochází v pravidelných intervalech a infračervené světlo může být zachyceno ve více nezávislých snímajících buňkách přijímače. Díky tomuto jsou více eliminovány falešné poplachy a dochází k vyšší úrovni bezpečnosti. Tato technologie dále umožňuje vytvoření multiplexových kanálů, kdy dochází k seskupení kanálů a je možno určit, který přijímač a vysílač bude zpracovávat určitý paprsek. [25]



Obrázek 14. Pulzní přenos signálu u infračervené bariery. [25]

- **D.I.S. 100 Hz Technology -** tato technologie vyvinutá společností SORHEA již nepoužívá klasické rozdělení na přijímač a vysílač signálu a umožňuje obousměrnou komunikaci všech prvků v systému, tato komunikace je synchronizována na frekvenci 100 Hz.

  Díky tomu, že o případném poplachu ví oba dva obousměrné prvky, dochází k navýšení bezpečnosti a spolehlivosti systému. [25]



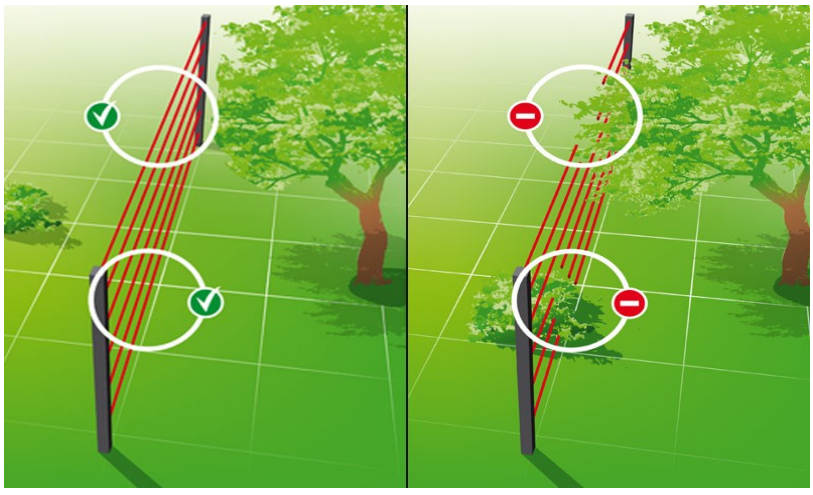
Obrázek 15. Princip fungování D.I.S 100 Hz - emitter (zářič) a receiver (přijímač) fungují jako jeden bod. [25]

2.5.2 Správná instalace infračervené bariery

Snímač přerušení se nachází na přijímači infračerveného paprsku a vyhodnocuje čas přerušení paprsku. Toto je důležité pro správné nastavení času přerušení t, kdy je třeba odhadnou předpokládanou rychlost narušitele a nastavit čas tak, aby byl pachatel zachycen a současně nedocházelo k falešným poplachům. Protože čím je kratší čas t, tím je spolehlivější detekce a současně vyšší náchylnost k falešnému poplachu.

Instalace se provádí na stabilní konstrukci, v přímém dohledu a ve stejné výšce. Při instalaci je dobré zkontrolovat okolní vegetaci a ubezpečit se, že nedojde k přerušení infračerveného paprsku.

Dalšími možnými zdroji falešných poplachů jsou klimatické jevy: nízká oblačnost, sněhové srážky nebo mlha. Těmto jevům se dá částečně předcházet instalací v menších rozestupech mezi vysílači a přijímači. [24]

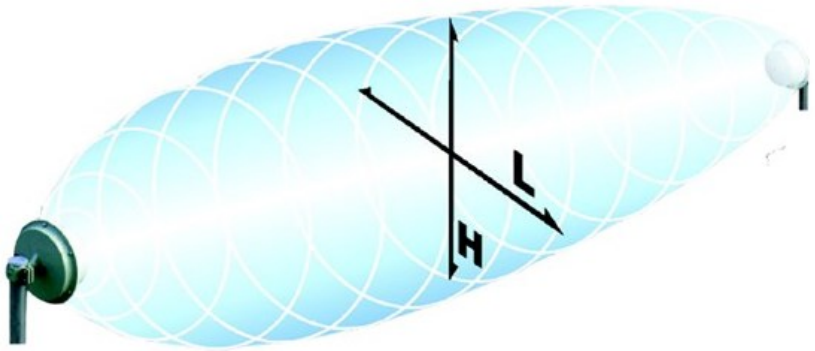


Obrázek 16. Správná instalace infračervené bariery. [26]

2.6 Mikrovlnné bariery

Stejně jako infračervené bariery fungují na principu vysílač a přijímač, kdy vysílač vytváří směrově orientované elektromagnetické pole o frekvenci 9900 Mhz v podobě protáhlého doutníku a přijímač toto pole sleduje a je schopen rozpoznat jeho narušení. Vzdálenost mezi vysílačem a přijímačem je obvykle desítky až stovky metrů.

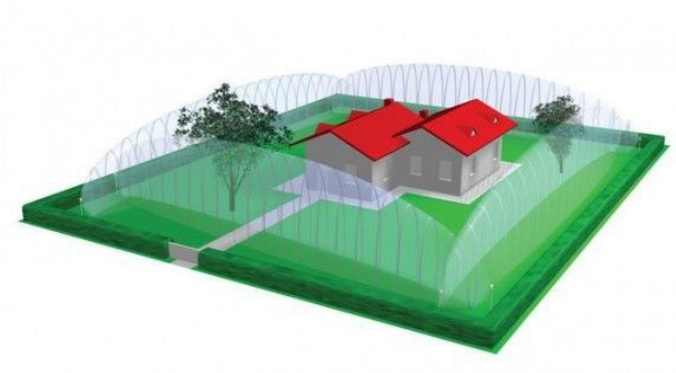
Výhodou oproti infračervené bariéře je menší náchylnost na počasí. Někteří výrobci kombinují mikrovlnou barieru s infračervenou barierou a tímto způsobem zvyšují bezpečnost a zabraňují falešným poplachům.



Obrázek 17. Mikrovlnná bariera. [25]

2.6.1 Použití mikrovlnné bariery

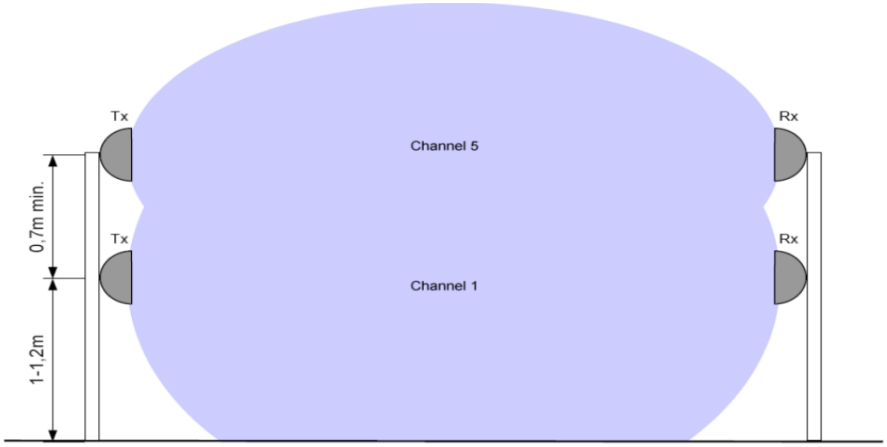
Mikrovlnné bariery se nejčastěji používají pro ochranu uvnitř střeženého perimetru a jejich instalace přímo na obvodové oplocení není příliš vhodná kvůli šíření signálu, který by v takovém to případě zasahoval i mimo střežený a ohraničený perimetr.



Obrázek 18. Použití mikrovlnné bariery. [18]

Výhodou mikrovlnných bariér je možnost kombinovat v jedné bariéře i větší množství vysílačů a přijímačů a vytvořit prakticky libovolné ochranné pole. Při kombinování není

možné umístit vysílač a přijímač do těsné blízkosti z důvodu možného rušení přijímaného signálu. [18]



Obrázek 19. Kombinace detekčních polí u mikrovlnných bariér. [18]

2.7 Plotové detekční prostředky

Složí k detekci napadení mechanických zábranných prostředků nejčastěji plotů. Jejich instalace se nejčastěji provádí na drátěné oplocení. Podle způsobu detekce je lze dělit na adresné, které přesně lokalizují místo napadení, a zónové signalizující pouze určitou zónu, ve které došlo k napadení.

- **Vibrační detektory:** tento typ detektorů je možné instalovat na různé typy pletiv a mřížová oplocení. Instalace je prováděna na každý jednotlivý díl pletiva obvykle do středu mezi dva sloupky. Výhodou tohoto typu je možnost nastavení adresné lokace, která zaručuje přesné určení místa poplachu. Vibrační detektory mohou pracovat na principu piezoelektrického jevu nebo jiného otřesového čidla. [27]
- **Plotové tenzometrické detektory** využívají pro detekci kombinaci mechanické a elektronické ochrany. Mechanická ochrana je tvořena pomocí žiletkového nebo ostnatého drátu s roztečí 10 cm, který je napnut tak, aby při zátěži 15 kg vyvolal poplach. Poplach je vyhodnocován pomocí tahové diference (napnutí, přestřižení nebo roztažení) drátu příslušným čidlem a jeho převodem na elektrický signál. Nevýhodou tohoto systému jsou vyšší náklady na mechanickou část plotu, která musí být stabilní. [27]
- **Detekce pomocí drátěné osnovy** využívá k detekci 4 až 20 vodičů (ostnatého nebo žiletkového drátu), které jsou umístěny v pletivu. Poplach je zaznamenán při

zkratu nebo přerušení vodičů. Výhodou systému je odolnost proti planým poplachům a nevýhodou možnost roztažení vodičů bez vyhlášení poplachu. [27]

- **Mikrofonní kabely** (speciální koaxiální kabely) umožňují zaznamenat jak přestřižení, tak otřesy na všech různých typech pletiva, mřížového nebo svařovaného oplocení. [27]
- **Optické kabely:** pro ochranu se využívá optické vlákno, do kterého je přiveden periodický signál. Tento signál je vyhodnocován, a pokud dojde k jeho změně, která je způsobena mechanickými změnami (otřesy, pokusy o překonání plotu, přestřižením), dochází k vyhlášení poplachu. Optické vlákno představuje dobrý způsob ochrany všech drátěných pletiv. Výhodou optického kabelu je elektrická nevodivost, která umožňuje použití ve výbušném, hořlavém nebo vodním prostředí. [27]
- **Kapacitní kabely** jsou tvořeny třemi kabely, které jsou v různých výškách instalovány na plot. Mezi těmito kabely vzniká elektrostatické pole a dielektrikem je vzduch. Toto pole je citlivé na jakékoliv předměty či osoby uvnitř. Kapacitní kabely jsou více náchylné na falešné poplachy a je vhodné kombinovat je i s dalšími prvky perimetrické ochrany. [27]

2.8 Systémy se zemními detekčními kabely, hadicemi, detektory

Tento typ detektorů je možno využít nezávisle na mechanických zábranných prostředcích. Jejich výhodou je částečné nebo i absolutní zakrytí pod zeminou a snížená šance na odhalení a zneškodnění. Další výhodou je, že nenarušují estetický dojem z chráněného perimetru. [27]

- **Štěrbinové kabely** fungují na principu vysílače a přijímače, kdy je použit speciální koaxiální kabel, který má ve svém stínění vzduchovou mezeru, která mu umožní fungovat jako vysílač či přijímač. Samotná instalace štěrbinových kabelů probíhá do země v hloubce přibližně 0,3m a kabely jsou vždy položeny v párech s rozestupem 2 m. Jeden z kabelů (vysílač) vysílá vysokofrekvenční elektromagnetické pole o eliptickém průřezu a tento signál je zachycován v kabelu, který slouží jako přijímač. Poplach je vyhlašován na základě změny elektromagnetického pole. [27]

- **Seismické detektory** reagují na otřesy v okolí detektoru. Nejčastěji se používají v otevřeném prostoru a využívají bezdrátový přenos signálu mezi jednotlivými detektory a vyhodnocovací jednotkou. Podle typu detektoru lze počítat jeden detektor přibližně na 300 m^2 pro detekci chůze. Výhodou tohoto řešení je rychlá a snadná montáž bez stavebních úprav. Nevýhodou možnost rušení otřesy z okolí (stavby, silnice…). [27]
- **Detektory magnetických anomálií** fungují na principu detekce proudů, které vznikají při pohybu feromagnetických materiálů v blízkosti citlivých senzorů (desky, tyče, kabely). Tyto senzory jsou skryty pod zemí. Detektory magnetických anomálií jsou považovány za vysoce spolehlivé a jsou často nasazovány při zabezpečení letišť a věznic. [27]

2.9 Laserové detektory

Laserové detektory jsou aktivním prvek perimetrické ochrany. Jsou tvořený vysílačem a přijímačem. Výhodou laserových detektorů je široké spektrum použití a poměrně jednoduchý způsob fungování založený na přenosu laserového paprsku a reakce v případě jeho přerušení. [27]

- **Laserové závory** se využívají pro monitoring vstupních a vjezdových prostorů. Maximální dosah laserové závory se pohybuje v desítkách metrů. Závora funguje na principu vyslání paprsku o vlnové frekvenci 850 nm a při jeho zachycení na citlivé ploše fototranzistoru v případě přerušení paprsku dochází k rozpojení relé obvodu a přenosu této informace do zabezpečovací ústředny. [27]
- **Laserové radiolokátory** neboli Lidar (Light Detection And Ranger) slouží k detekci pachatele ve střeženém prostoru. Tato technologie se běžně využívá pro letecké mapování terénu a na podobném principu funguje i při bezpečnostním použití. Do prostoru je vyzařován laserový paprsek o vlnové frekvenci 905 nm a následně je zachycován jeho odraz. Pokud je zaznamenána změna dopadajícího paprsku, dochází k vyhlášení poplachu. Tento systém umožňuje nejen zaznamenat narušení, ale v reálném čase prostor i monitorovat. [27]

2.10 Venkovní PIR (Pasiv Infra Red detector)

Fungují na stejném principu jako u vnitřního použití, kdy je snímáno tepelné spektrum v prostoru a vyhodnocován tepelný rozdíl mezi jednotlivými segmenty snímající čočky. PIR detektory pracují v rozsahu 760nm až 1mm. Při venkovním použití se nejčastěji využívá detekční zóna záclona. Dosah PIR detektoru je až 150 m. Výhodou PIR detektoru je jeho pasivní provoz, který šetří baterii a znesnadňuje jeho odhalení. V případě, že se v perimetru pohybují menší zvířata je možno detektor nastavit tak, aby nedocházelo k falešným poplachům. [27]

2.11 Dílčí závěr

Druhá kapitola pojednává o poplachových zabezpečovacích a tísňových systémech používaných při ochraně perimetru. V první části nejprve seznamuje se stupni zabezpečení a třídami prostředí, které jsou využívány PZTS prvků zabezpečení. Dále pak kapitola popisuje detektory používané při ochraně perimetru. Postupně představuje infračervené bariery, mikrovlnné bariery, plotové detekční prostředky, systémy s detekčními kabely, laserové detektory a venkovní PIR detektory. Cílem této kapitoly je představit jednotlivé detektory a prostředí vhodné pro tyto detektory.

3 KAMEROVÉ SYSTÉMY

Kamerové systémy jsou vysoce účinným prvkem zabezpečení perimetru, mohou být provozovány samostatně nebo jako doplněk k PZTS systému, kdy reagují na vyhlášení poplachu v daném sektoru. Tento sektor je možno díky kamerám v reálném čase visuálně prověřit a o veškerém dění může díky kamerám vzniknout záznam. [29]

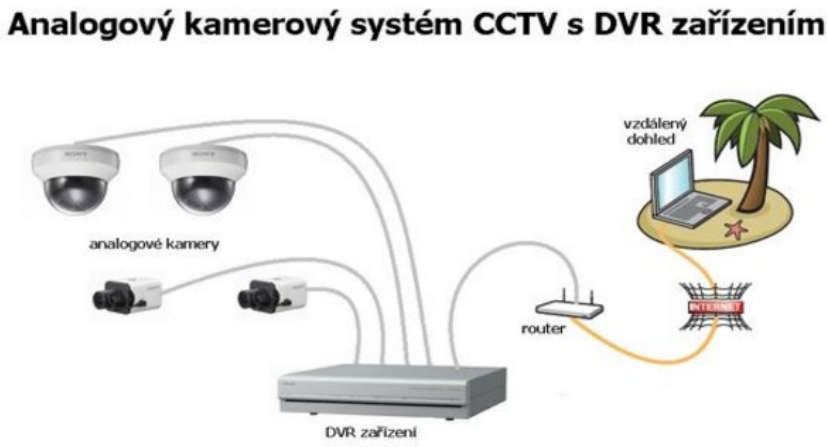
Kamerové systémy patří k nejrychleji rostoucím odvětvím ochrany perimetru. Díky vyspělé video analýze, která může probíhat jak v samotné kameře, tak i na serveru, jsou kamery schopny rozpoznat napadení objektu. [29]

Dnes se můžeme setkat se dvěma základními typy kamerových systému. Prvním a starším je analogový kamerový systém často označovaný zkratkou VDS (Video Dohledový Systém) a druhým novějším je **IP** (Internet Protocol) kamerový systém. Mezi těmito dvěma technologiemi můžeme najít různé hybridní technologie, které umožní kombinace těchto technologií.

3.1 Analogový kamerový systém

Známý také pod zkratkou **VDS** (Video Dohledový Systém) neboli uzavřený televizní okruh. Jedná se o poměrně starší technologii, která na svém počátku využívala jednoduchý systém zachycení obrazu pomocí analogové kamery a jeho přenos pomocí koaxiálním kabelu a zobrazení na analogovém monitoru nebo televizi. Data mohla být ukládána na magnetické pásky. Pro zobrazení na monitoru či televizi byly využity normy **PAL**/**NTSC** či **SDI** s maximálním rozlišením 1,3 Mpx. Tento první systém neobsahoval žádnou digitální část, která by umožnila přenos na počítač nebo mobilní telefon, tudíž se jednalo o uzavřený televizní okruh. [28]

S postupující digitalizací a zvyšujícími se nároky na přenos signálu byly analogové kamerové systémy doplněny o **DVR** (Digital Video Recorder) zařízení, které převádí analogový signál na digitální a umožní jeho přenos pomocí protokolu **TCP/IP**. Nevýhodou je částečná ztráta kvality způsobená digitalizací. [28]



Obrázek 20. Analogový kamerový systém VDS s DVR. [28]

V současné době jsou standardní analogové kamerové systém spíše na ústupu, což je dáno zastaralými televizními normami, které neumožňují zobrazení v HD rozlišení. Velcí výrobci postupně ukončují vývoj této technologie. Jako možná alternativa pro budoucnost analogových kamerových systémů jsou hybridní technologie, které stále pro přenos využívá analogové vedení (koaxiální nebo optické kabely), ale nabízejí již HD rozlišení a další pokročilé vlastnosti pokročilejších IP kamer. [29]

3.2 Hybridní kamerové systémy

Potřeba kombinace analogových a IP kamerových systémů vznikla ve chvíli, kdy došlo k masivnímu rozšíření protokolu TCP/IP a sítě Internet jako globální světové sítě. Dalšími faktory, které přispěly k rozšíření této technologie, byly neustále se zlepšující IP kamery, jež hlavně v rozlišení překonaly klasické analogové kamery.

Analogové kamery drží některé výhody oproti novějším IP kamerám, jako možnost zobrazit obraz bez ztrátové komprimace nebo mnohem lepší odezva zobrazení obrazu než je u IP kamer, kde dochází ke zpoždění až 1sekunda, které je způsobené komprimací a dekomprimací obrazu.

Mezi výhody hybridních kamerových systémů patří možnost zachovat kabeláž po předchozích analogových kamerách a pro přenos obrazu i nadále využívat koaxiální kabel nebo zachovat část starších analogových kamer v místech, kde není třeba snímat obraz ve vysokém rozlišení a systém doplnit novými hybridními kamerami s vysokým rozlišením.

Mezi nejznámější technologie navazující na předchozí analogové kamerové systémy patří:

- SDI (Serial Digital Interface).
- TVI (Transport Video Interface).
- CVI (Composite Video Interface).
- AHD (Analog High Definition).

3.2.1 SDI technologie

SDI (Serial Digital Interface) je technologie, která byla do nedávna využívána výhradně ve studiové televizní technice (Broadcast Television) pro přenos analogového signálu. Tato technologie vznikla na základě standardů SMPTE (Society of Motion Picture and Television Engineers), které byly uvolněny od licenční ochrany na základě meziodborové licenční smlouvy mezi SMTPE a HDcctv Aliancí, což umožnilo požití této technologie u bezpečnostních kamerových systémů. [30]

3.2.1.1 Přenos signálu u SDI

SDI představuje standard pro přenos videosignálu ve vysokém rozlišení na kratší vzdálenosti bez nutnosti komprimace signálu. Přenos probíhá mezi vysílačem a přijímačem, na data je aplikovaná detekce chyb a jejich případná oprava pomocí Hammingova kódování s paritou a paritním bitem. Samotný přenos je zajišťován pomocí vysoce kvalitního koaxiálního kabelu s BNC konektory (Bayonet Neill Concelman), teflonovou izolační vrstvou a impedancí 75 Ω. Maximální délka koaxiálního kabelu je 300 m u SD rozlišení videa a u HD rozlišení 100 m. [31]

Další možností je pro přenos použít optický kabel jak na krátkou, tak i na dlouhou vzdálenost. U přenosu pomocí optického kabelu je výhodou, že není náchylný na elektromagnetické rušení, což umožní použít HD-SDI v širokopásmových technologiích. [31]

Tabulka 2. Jednotlivé standardy používané u SDI a jejich mezní přenosové vzdálenosti. [31]

Standard	Název	Vzdálenost s optickým kabelem (metry)
SMPTE 259M-C	SDI	300
SMPTE 292M	HD-SDI	100
SMPTE 372M	Dual-link HD-SDI	100
SMPTE 424M	3G-SDI	100

3.2.1.2 SDI formáty

- **SD-SDI** (Standard Definition) pro přenos využívá nejčastěji standard **SMPTE 259M-C** s datovým tokem 270Mbit/s a poměrem stran 4:3 nebo 16:9. Rozlišení u tohoto formátu je 576i (720x576pixelů). Tento formát patří již mezi starší, poprvé byl představen v roce 1989. [31]
- **ED-SDI** (Enhanced Definition) využívá pro přenos standard **SMTPE 334M,** který má datový tok 540Mbit/s, a dva typy podporovaného rozlišení 480p, kde poměr stran je 4:3 (640x480pixelů) a 576p s poměrem stran 4:3 (720x576pixelů). [31]
- **HD-SDI (**High Definition) tento formát patří k nejvíce využívaným u bezpečnostních kamerových systémů, pro přenos používá standard **SMPTE 292M**, který umožňuje dva rozdílné datové toky v závislosti na použité snímkové frekvenci u frekvencí 60 Hz, 50 Hz, 30 Hz, 25 Hz a 24 Hz je datový tok 1,485Gbit/s a u frekvencí 59.94 Hz, 29.97 Hz a 23.98 Hz je datový tok 1,485/1,001 Gbit/s tento rozdíl je dán z důvodu, že datový tok 1,485/1,001 Gbit/s více vyhovuje zpětné kompatibilitě s NTSC systémy (analogové video). [31]
- **Dual-link HD-SDI** tento formát využívá standard SMPTE 372M a v podstatě jde o zdvojení formátu HD-SDI, kdy je po dvou paralelních koaxiálních nebo optických kabelech možno přenést až 2.970 Gbit/s, nebo 2.970/1.001 Gbit/s v závislosti na snímkové frekvenci stejně jako HD-SDI. Tento formát umožňuje přenos videa v kvalitě 1080p60. [32]
- **3G-SDI** podobně jako formát **Dual-link HD-SDI** umožňuje přenos videa v kvalitě 1080p60. Velkou výhodou formátu **3G-SDI** je, že pro přenos využívá jen jeden koaxiální nebo optický kabel. Tento formát pracuje na standardu **SMPTE 424M**. [32]

- **6G-SDI** tento formát umožňuje přenos 6 Gbit/s a zobrazení videa v kvalitě 2160p30. Pro přenos je využit standard **SMPTE ST-2081**. [32]
- **12G-SDI** tento formát umožňuje přenos až 12 Gbit/s a zobrazení videa v kvalitě 2160p60. Pro přenos je využit standard **SMPTE ST-2082**. [32]
- **24G-SDI** tento formát umožňuje přenos až 24 Gbit/s a zobrazení videa v kvalitě 2160p120. Pro přenos je využit standard **SMPTE ST-2083**. [32]

3.2.2 HD-TVI technologie

HD-TVI (High Definition Transport Video Interface) je nová digitální technologie pro přenos obrazu ve vysokém rozlišení až 1080p (1920 × 1080 Pixelů) s rychlostí 12 snímků za sekundu nebo 1280 × 720p s rychlostí 25 snímků za sekundu. Tato technologie byla vyvinuta společností Techpoint v roce 2012 a v současné době představuje otevřenou technologii využívanou řadou výrobců. [33]

3.2.2.1 Přenos signálu u HD-TVI

Při přenosu je signál z digitálního převeden na analogový na nosné frekvenci 21MHz (720P) ⁄ 38MHz (1080P), což umožní přenos na delší vzdálenost než u technologie HD-SDI až do vzdálenosti 500 m současně tak sníží nároky na záznamová zařízení.

Přenos signálu může probíhat přes koaxiální kabel, RS-485 nebo i UTP kabel při použití pasivních videobalunů. Při použití UTP kabelu je možno přenášet signál až do vzdálenosti 200 m. [33]

3.2.3 HD-CVI technologie

HD-CVI (High Definition Composite Video Interface) standard představuje další z technologií, které u kamerového bezpečnostního systému využívají přenosu signálu pomocí koaxiálního kabelu. Mezi hlavní přednosti této technologie patří možnost přenosu videa v kvalitě 1080p (1920 x 1080) bez komprese na vzdálenost až 500 m, dále pak možnost přenosu zvukové stopy a ovládacích instrukcí pro kameru po stejném koaxiálním kabelu, po kterém je přenášen obraz z kamery. [34]

3.2.3.1 Přenos signálu u HD-CVI

Pro přenos je využíván koaxiální kabel a v porovnání s HD-SDI je možno tuto technologii použít na jakémkoliv koaxiálním kabelu, který byl dříve využíván pro standardní VDS. [34]

3.2.4 AHD technologie

AHD (Analog High Definition) je otevřenou technologií, kterou uvedla na trh společnost Nexchip. Tato technologie umožňuje přenos v kvalitě 1080p (1920 x 1080). AHD technologie odděluje pro přenos Y a C složku signálu a využívá vysokofrekvenční analogové filtry. Díky tomuto je obraz vysoce kvalitní i při zhoršených světelných podmínkách. [35]

3.2.4.1 Přenos signálu u AHD technologie

Při přenosu je signál z digitální podoby převeden do modulovaného analogového signálu což umožňuje přenést signál na výrazně delší vzdálenost než u klasické technologie VDS. Maximální délka u kvalitního koaxiálního kabelu je až 500 m a UTP kabelu s použitím video převodníků (videobaluny) 320m. [35]

3.2.5 Porovnání jednotlivých hybridních kamerových systémů

Tabulka 3. Srovnání jednotlivých hybridních kamerových systémů. [34, 35, 31, 33]

Hybridní kamerové systémy				
Parametry	**HD-CVI**	**AHD**	**HD-SDI**	**HD-TVI**
Maximální rozlišení (pixely)	**1080p** (1920 x 1080)	**1080p** (1920 x 1080)	**1080p** (1920 x 1080)	**1080p** (1920 x 1080)
Výstupní video kvalita	**Velmi dobrá** při kvalitním osvětlení, za šera ztrácí ostrost.	**Dobrá,** obrazu chybí ostrost a barvy nejsou přesné.	**Velmi dobrá,** ostré zobrazení HD obrazu s věrnými barvami	**Velmi dobrá,** ostré zobrazení HD obrazu s věrnými barvami
Maximální přenosová vzdálenost s koaxiálním kabelem (RG59)	**500 m(720p) 400 m(1082p)**	**500 m**	**100 m**	**500 m**
Maximální přenosová vzdálenost s kroucenou dvojlinkou (CAT5)	**200 m**	**100 m**	**100 m** (pro přenos je třeba využít A/D převodník)	**200 m**
DVR výstupní kompatibilita Analog	**Všechny analogové kamery**, omezení kanálů a konfigurace	**Všechny analogové** kamery, omezení kanálů a konfigurace	**Jen některé modely kamer** omezení kanálů a konfigurace	**Všechny analogové kamery** se všemi kanály a plnou konfigurací
DVR výstupní kompatibilita HD Analog	Kamera podporující HD-CVI na všech kanálech s plnou konfigurací	Kamera podporující AHD na všech kanálech s plnou konfigurací	Kamera podporující HD-SDI na všech kanálech s plnou konfigurací	Každá HD-TVI kamera na jakémkoliv kanále s plnou konfigurací
DVR výstupní kompatibilita IP	Podpora IP kamer na vybraném kanálu a při vybrané konfiguraci	IP kamery nejsou podporovány	IP kamery nejsou podporovány	Podpora IP kamer na 2 kanálech při libovolné konfiguraci
DVR Hybridní možnosti	**Omezená** nastavitelnost	**Omezená** nastavitelnost	**Omezená** nastavitelnost	**Neomezená** nastavitelnost
Kompatibilita formátů	Patentovaná technologie s jedním výrobcem Dahua	Otevřený standard s omezeným počtem výrobců	Otevřený standard s velkým množstvím výrobců	Otevřený standard s velkým množstvím výrobců

3.3 IP kamerový systém

S postupným růstem digitalizace se tento trend projevil i u bezpečnostních kamerových systémů, kdy vznikly IP (Internet Protocol) kamery. Tyto kamery v sobě mají zabudovaný webový video server, který zajišťuje digitalizaci, komprimaci a přenos pomocí počítačové sítě (LAN/Internet).

3.3.1 Standardy i IP kamerového systému

Při vzniku prvních IP kamerových systému docházelo k problémům se standardy a často chyběla vzájemná kompatibilita a interoperabilita mezi jednotlivými výrobci. Z tohoto důvodu byla v roce 2008 firmami Sony, Bosch a Axis založena platforma **ONVIF** (Open Network Video Interface Forum) pro vývoj a zavedení standardů v oblasti IP kamerových systémů. Jedná se otevřené sdružení, které má v současnosti více než 500 členů, kteří nabízejí více jak 3200 výrobků, jež splňují tento standard. [36]

Pro snadnější a efektivnější kontrolu shody mezi jednotlivými výrobky byly v roce 2012 zavedeny profily, které zajišťují to, že ve chvíli, kdy jsou zařízení a klient založeny na stejném profilu, jsou bez pochyb v souladu. V současné době je k dispozici 5 profilů. [36]

- **Profil S** adresuje společnou funkcionalitu IP video systémů. Je možno nastavit audio a video streamování mezi zařízením (kamerou) a klientem. Klient může nastavit video a audio datové streamy. Díky tomuto lze nastavit poplachové vstupy a reléové výstupy. [36]
- **Profil G** pracuje s konfigurací záznamu, jeho vyhledáním a přehráním. Profil G obsahuje podporu pro příjem zvuku v případě, že klient podporuje tyto funkce. [36]
- **Profil C** umožňuje integraci s fyzickými řídicími systémy přístupu do objektu, řeší interoperabilitu mezi těmito systémy a síťovými video systémy. Díky profilu C může klient přistupovat k informacím o branách a přístupových bodech v systému a konfigurovat řízení přístupů u jednotlivých bodů. [36]
- **Profil Q** se zaměřuje na jednoduchost nastavení v základním nastavení. Zařízení je po přidání do sítě automaticky detekováno a je možno provést jeho konfiguraci. Součástí profilu Q je i podpora TLS (Transport Layer Security) protokolu, který se stará o zabezpečení při komunikaci v síti a zabraňuje odposlechu a padělání dat. [36]
- **Profil A** pracuje s nastavením oprávnění ke vstupu. Díky tomuto profilu je možno vytvářet, přidělovat a odebírat oprávnění ke vstupu do objektu. Dále pak umožňuje integraci IP kamerového systému a přístupového systému. Tento profil umí pracovat s kalendářem a časem, díky čemuž je možné poměrně komplexní nastavení přístupu. [36]

ONVIF není jediný standard využívaný u standardizace IP kamerových systémů. Mezi další standardy patří například PSIA (Physical Security Interoperability Alliance), jehož

cílem je vytvořit *plug and play* IP rozhraní pracující jako USB rozhraní. Velkou výhodou standardu je velké množství zařízení, které tento standard pokrývá. Tento standard je využíván jen omezeným množstvím výrobců v současné době zhruba 50, což je jeho značnou nevýhodou.

3.3.2 Přenos signálu u IP kamerových systémů

Pro přenos signálu u IP kamerových systémů se vyžívá IP protokol, který umožňuje přenos digitálního signálu po standardní ethernet síti. Video signál je digitalizován již přímo v kameře pomocí webového video serveru a dále odeslán pomocí standardní sítě ethernet. Při větším množství IP kamer je s tím třeba počítat a mít uzpůsobenou ethernetovou síť, kdy propustnost by měla být minimálně 1Gb/sec. U velkých IP kamerových systémů je doporučováno budovat ethernetovou síť speciálně pro tyto účely. Některé kamery umožňují přenos video signálu pomocí bezdrátové sítě Wi-Fi, tento způsob ale není většinou příliš vhodný z důvodů možného rušení a nestability signálu. [37]

Výhodou IP kamerových systémů je možnost využití globální sítě Internet, kdy je možno sledovat živý obraz z kamery prakticky z jakéhokoliv místa na světě. Pro správné fungování je třeba mít kvalitní připojení do sítě Internet, na straně kamery je důležitý upload, který by měl být minimálně 1024 kb⁄sec. [37]

Nejčastěji používané typy kabeláže představují UTP (Unshielded Twisted Pair) a STP (Shielded Twisted Pair). Rozdíl mezi těmito dvěma typy kabeláže spočívá ve stínění u STP kabeláže, které snižuje míru vyzařování. Pro oba typy kabeláže se využívá standardní konektor 8P8C, který je častěji znám pod označením RJ-45. Při použití kabelu UTP nebo STP je možno napájet kameru pomocí POE (Power over Ethernet), kdy k samotné kameře není nutné přivádět napájení zvlášť, ale vše je obstaráno díky ethernetovému kabelu. Ethernetové kabely se dále dělí do kategorií a pro IP kamerové systémy je doporučeno využívat kategorii CAT6 s maximální vzdálenosti 55 m a kategorii CAT6a s maximální vzdáleností 100 m. Pro přenos na větší vzdálenost nebo v páteřních místech větších sítí je možno využít optických kabelů. [37]

Obrázek 21. Přenosová trasa u IP kamerového systému. [38]

3.3.3 Kompresní formáty u IP kamerových systémů

Z důvodu snadnějšího zpracování, přenesení a uskladnění dat je třeba data zkomprimovat. Při komprimaci je třeba zachovat co možná nejvyšší kvalitu videa a současně výrazně snížit množství dat. U IP kamer se nejčastěji používají kompresní formáty M-JPEG, MPEG-4 a H.264. [39]

- **M-JPEG** vychází z kompresního formátu JPEG (Joint Photographic Experts Group), který je používán pro kompresi barevných fotografií. M-JPEG (Motion Joint Photographic Experts Group) je jeho modifikací. Při přenosu jsou kódované a posílané celé jednotlivé snímky, mezi kterými není žádná časová závislost. Při přenosu nedochází k filtrování statických částí oblastí v obrazu. Tento kompresní formát má nejhorší kompresní poměr ze zde uvedených kompresních formátů. [39]
- **MPEG-4** (Moving Picture Expert Group) tato kompresní norma je určena pro přenos video a audio signálu. Výhodou tohoto standardu je, že při přenosu dochází k dvojité kompresi, a to jak nadbytečných prostorových dat podobně jako u formátu M-JPEG, tak i nadbytečným časových dat. Při časové komprimaci je využito podobnosti po sobě jdoucích snímků a je přenášen pouze rozdíl mezi nimi, díky tomuto je možno snížit datový tok na polovinu oproti M-JPEG. [39]
- **H.264** je kompresní formát vycházející z formátu MPEG-4. Tento kompresní formát má široké využití jak u IP kamer, tak i ve spotřební elektronice. Jeho kompresní poměr je až o polovinu lepší než u MPEG-4. [39]
- **H.265** nejnovější kompresní formát často označovaný zkratkou HEVC (High Efficiency Video Coding) představuje současnost a budoucnost kompresní formátů u digitálního videa. Tento kompresní formát umožňuje kódovat video s maximálním rozlišením 8192×4320 pixelů. Při porovnání komprese oproti kompresnímu formátu H.264 je kompresní poměr o polovinu lepší. [58]

Tabulka 4. Přibližné srovnání jednotlivých kompresních formátů při 25 snímcích za sekundu. [40]

Rozlišení	MJPEG	MPEG-4	H.264	H.265
640 x 480 (VGA)	7.78Mb/s	1.58Mb/s	0.57Mb/s	0.29Mb/s
1280 x 1024 (1.3MPix)	32.77Mb/s	6.76Mb/s	2.46Mb/s	1.46Mb/s
1920 x 1080 (Full HD)	51.81Mb/s	10.65Mb/s	3.89Mb/s	2,48Mb/s

3.4 Normy pro práci s kamerovými systémy

Při práci s kamerovými systémy je třeba postupovat na základě platných norem, které předepisují minimální požadavky a poskytují doporučení pro dohledové videosystémy VSS (Video Surveillance System), dosud zvané CCTV (Closed Circuit Television).

V současné době je v České republice v platnosti soubor evropských norem IEC 62676. Tento soubor norem vydala technická komise IEC/TC 79, která společně s mnoha dalšími spolupracujícími organizacemi tyto normy vytvořila. Soubor norem IEC 62676 je možno dále dělit do čtyř samostatných částí: [41]

- Systémové požadavky 1,2.
- Video přenosové protokoly 1,2,3.
- Analogové a digitální video rozhraní.
- Pokyny pro aplikace.

3.4.1 ČSN EN 62676-1-1

ČSN EN 62676-1-1 Dohledové videosystémy pro použití v bezpečnostních aplikacích Část 1-1: Systémové požadavky-Obecně

Tato česká norma má stejný status jako evropská norma EN 62676-1-1:2014 a její oficiální překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. [42]

Norma ČSN EN 62676-1 předepisuje minimální požadavky a doporučení pro dohledové videosystémy používané pro bezpečnostní aplikace. Dále pak udává základní funkční požadavky, které je třeba sjednat mezi zákazníkem a dodavatelem v rámci provozních poža-

davků. Součástí normy je vysvětlení termínů a definic používaných u dohledových video systémů. [42]

Tato norma převážně řeší tato témata: snímání obrazu, vzájemná propojení, zpracování obrazu, rozhraní k jiným systémům, stupně zabezpečení, funkční požadavky, zpracování obrazu, ukládání dat, správa systému, kvalita obrazu, třídy prostředí, dokumentace systému. [42]

3.4.2 ČSN EN 62676-1-2

ČSN EN 62676-1-2 Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-2: Systémové požadavky-Výkonové požadavky na video přenos

Druhá část normy ČSN EN 62676-1 zabývající se videosystémy. Tato část normy se zabývá přenosem videa a převážně řeší tato témata: výkonové požadavky, synchronizaci času na síti, požadavky na streamované video, požadavky na návrh IP video přenosových sítí, požadavky na video online přenosy, požadavky na ovládání datového toku, požadavky na rozpoznání a popis zařízení, požadavky na popis událostí v síti, požadavky na správu síťových zařízení. [43]

3.4.3 ČSN EN 62676-2-1

ČSN EN 62676-2-1 Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 2-1: Video přenosové protokoly - Obecné požadavky

První část normy ČSN EN 62676-2 se věnuje síťovému rozhraní pro zařízení v dohledových aplikacích, dále pak specifikuje síťový protokol pro plnou interoperabilitu video zařízení, kdy jsou nad základní vrstvou definovány protokoly pro dosažení plné interoperability video zařízení a dosažení těchto funkcí: streamování videa, řízení streamů, zpracování událostí, vyhledání, popis vlastností, správa zařízení, řízení PTZ funkcí, pomocné a další funkce. [41]

3.4.4 ČSN EN 62676-2-2

ČSN EN 62676-2-2 Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 2-2: Video přenosové protokoly – Implementace vzájemné spolupráce IP systémů založených na využití HTTP a REST

Druhá část normy ČSN EN 62676-2 není dostupná v českém jazyce. Tato norma specifikuje kompatibilní protokol založený na IP video protokolu, který je založen na protokolu

HTTP a REST. Video zařízení jsou dnes již běžně vybavena webovými servery, které umožňují reagovat na požadavek HTTP a v odpovědi na tento požadavek mohou obsahovat XML soubor s dalšími informacemi. REST umožňuje vytvářet služby, jež umožňují jednotný přístup ke všem informacím jednotným způsobem.[44]

3.4.5 ČSN EN 62676-2-3

ČSN EN 62676-2-3 Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 2-3: Video přenosové protokoly – Implementace vzájemné spolupráce IP systémů založených na síťových (web) službách

Třetí část normy ČSN EN 62676-2 není dostupná v českém jazyce. Tato část normy definuje postupy pro komunikaci mezi síťovými video klienty a video vysílači založenými na webových protokolech. Tento nový set specifikací umožňuje vytvořit síťový video systém se zařízeními a přijímači od různých výrobců při použití známého a dobře definovaného uživatelského rozhraní. Toto rozhraní pokrývá obvyklé funkce, jako je správa zařízení, přenos v reálném čase videa i zvuku, zpracování událostí, Pan (pohyb do leva a doprava), Tilt (pohyb nahoru a dolů), přiblížení obrazu, video analýza, hledání nahrávky a její přehrání. [45]

3.4.6 ČSN EN 62676-3

ČSN EN 62676-3 Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 3: Analogové a digitální video rozhraní

Tato norma není dostupná v českém jazyce. Norma ČSN EN 62676-3 specifikuje fyzické, elektronické a programové specifikace pro analogové a digitální video rozhraní u VSS. Video rozhraní slouží jak pro připojení a přenos video signálu, tak i pro přenos audio signálu a kontrolních signálů. Díky standardizaci video rozhraní lze propojit odlišné komponenty, jako jsou zařízení pro zachycení obrazu, zařízení pro zpracování obrazu a další. Tato se stahuje výhradně na kamerové systémy a definuje pouze minimální požadavky pro analogové a digitální video rozhraní. [41]

3.4.7 ČSN EN 62676-4

ČSN EN 62676-3 Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 4: Pokyny pro aplikace

Norma ČSN EN 62676-4 poskytuje doporučení a požadavky pro výběr, plánování, instalaci, přejímku, údržbu a zkoušení dohledových videosystémů zahrnující snímající prvky, propojení a zařízení pro zpracování obrazu při použití v bezpečnostních aplikacích. Díky této normě vzniká pracovní rámec, který napomáhá zákazníkům, instalačním firmám a koncovým uživatelům stanovit jejich požadavky. Tato norma pak dále umožňuje vytvořit objektivní vyhodnocení vlastností VSS. [41]

3.4.8 Další platné české normy pro dohledové systémy

Kromě souboru norem ČSN EN 62676 v současné době, v České republice platí normy:

- **ČSN EN 50132-5-3** Poplachové systémy - CCTV dohledové systémy pro použití v bezpečnostních aplikacích - Část 5-3: Video přenosy - Analogový a digitální video přenos [41]
- **ČSN EN 50132-7 ed. 2** Poplachové systémy - CCTV dohledové systémy pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace. Tato norma bude zrušena 13. dubna 2018. [41]

3.5 Dílčí závěr

Tato kapitola představuje kamerové systémy používané při ochraně perimetru. Cílem je seznámit čtenáře s technologiemi, které jsou používaný u kamerových systémů při ochraně perimetru, staršími analogovými a novějšími IP kamerami.

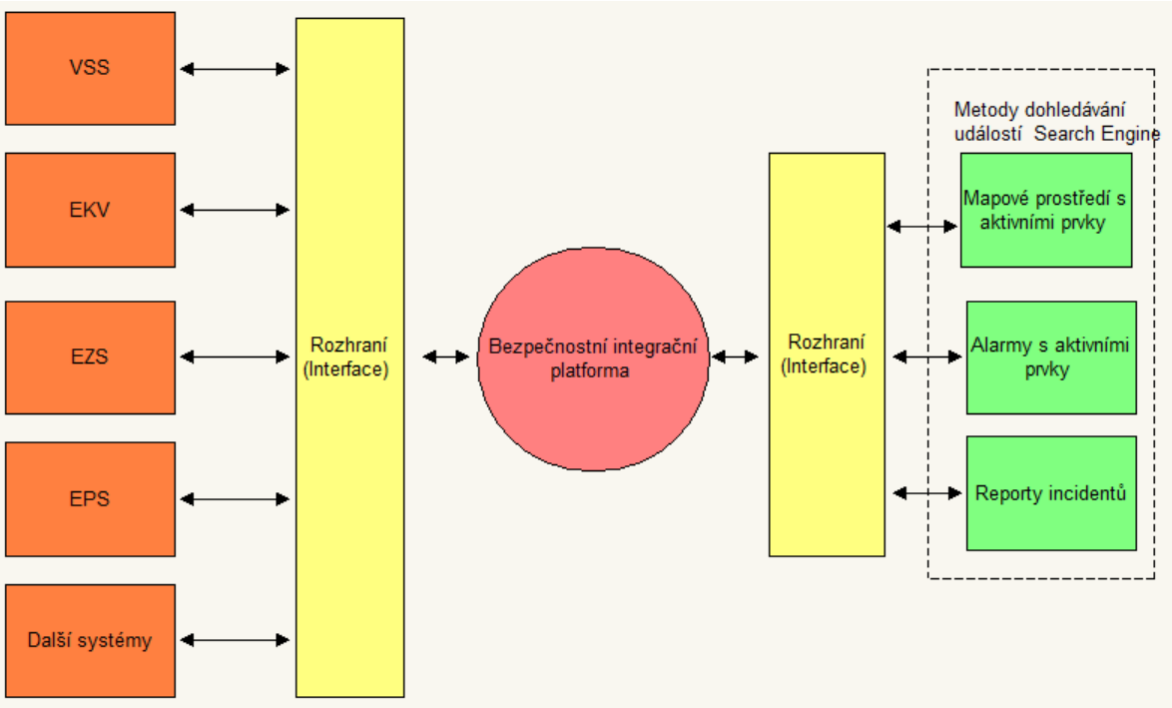
Obecně lze říci, že analogové kamery jsou na ústupu a jsou stále více nahrazovány IP kamerami. Mezi těmito dvěma technologiemi se nacházejí takzvané hybridní kamerové systémy, které stále používají analogový přenos signálu, ale kvalitou obrazu se vyrovnají modernějším IP kamerám. Tato kapitola se věnuje i těmto hybridním technologiím jejich výrobcům a standardům, jež používají.

Součástí této kapitoly je přehled norem používaných u kamerových systémů popisující systémové požadavky, video přenosové protokoly, analogové a digitální video rozhraní a pokyny pro aplikace u kamerových systémů.

4 INTEGRACE BEZPEČNOSTNÍCH SYSTÉMŮ OCHRANY PERIMETRU

Pro maximální využití všech systémů, které jsou použity při ochraně perimetru, je dobré tyto systémy vzájemně propojit, tím vytvořit bezpečnostní integrační platformu (BIP), často taky označovanou jako integrovaný poplachový systém (IPS). Což je systém, mající jedno nebo více společných zařízení a alespoň jedním z nich je poplachová aplikace. [46]

Bezpečnostní integrační platforma shromažďuje data z jednotlivých integrovaných bezpečnostních systémů, zobrazuje je v jednotném výstupu, umožňuje provozní ovládání integrovaných bezpečnostních systémů, vyhodnocení jednotlivých bezpečnostních událostí a incidentů. Prostředí umožňuje selektivní přístup, kdy je jednotlivým uživatelům přiděleno různé oprávnění pro přístup a správu bezpečnostních systémů. Dále pak BIP zaručuje vysokou úroveň před neoprávněným vstupem. Část dat zpracovaných v integrační platformě se automaticky propisuje zpět do jednotlivých bezpečnostních systémů. [46]



Obrázek 22. Blokové schéma bezpečnostní integrační platformy.

4.1 Důvody pro zavedení BIP

- Zvýšení bezpečnosti areálu díky jednotné přehledné integrační platformě.
- Možnost optimalizace manuálových a zautomatizovaných operací.
- Vyšší efektivita práce ostrahy díky jednotnému uživatelsky orientovanému prostředí.
- Možná vzájemná verifikace poplachů.
- Zjednodušená administrace.
- Jednotná a komplexní dokumentace.
- Podpora interaktivních map.

4.2 Interoperabilita

V posledních letech je na výrobce vytvářen tlak, aby byla data z jednotlivých prvků nebo i celých systémů snadno zpracovatelná a možná zpracovávat z různých integračních platforem. Díky používání zavedených standardů dochází v oblasti integrace k výraznému posunu.

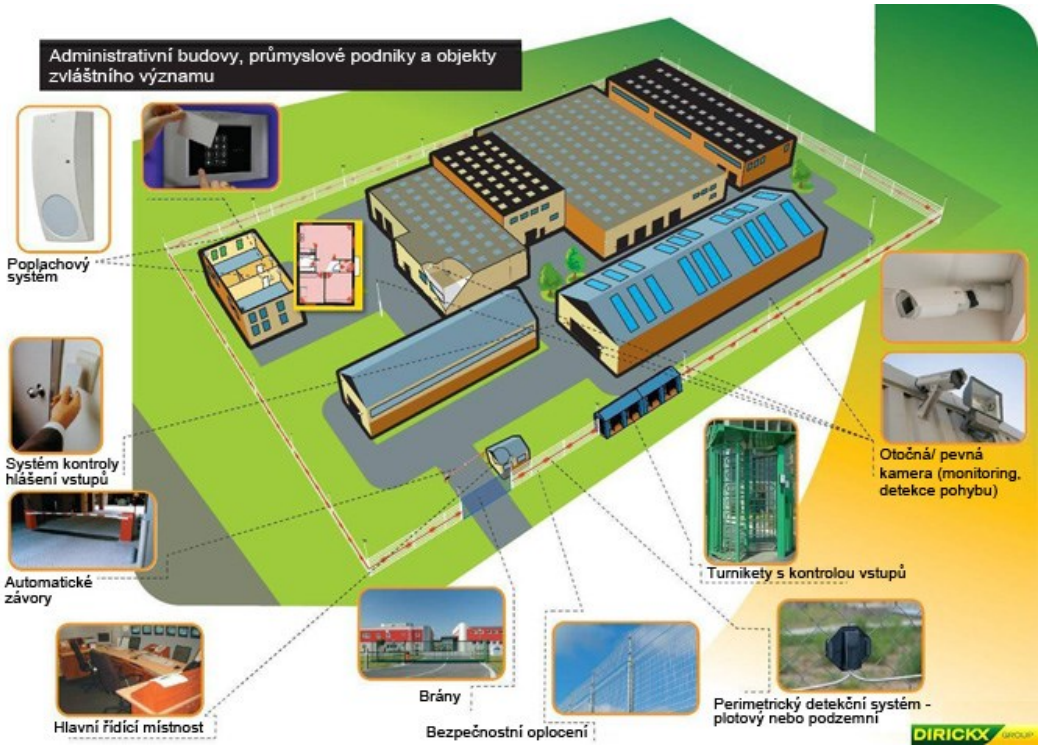
Při praktickém řešení je třeba vyřešit dvě základní otázky: jakým způsobem a do jaké hloubky systému se pomocí integrace lze dostat. U jednotlivých systémů je třeba sledovat, zda je řídící systémová jednotka vybavena pro standardizovaným komunikačním rozhraním. V současné době je možno propojit drtivou většinu systémů a umožnit určitý stupeň komunikace. Dalším stupněm při integraci jednotlivých systémů je Plug-and-Play, kdy již není nutné nastavovat komunikaci, ale po připojení dochází k automatické výměně informací mezi jednotlivými prvky a jejich synchronizaci. [47]

4.3 Jednotlivé funkční celky v BIP

- **I&HAS/HAS** – řada norem ČSN EN 50131 (Intrusion and hold-up systems/Hold-up systems) poplachové zabezpečovací a tísňové systémy.
- **ACS/EACS** – řada norem ČSN EN 50133 a ČSN EN 60839 (Access control systems/Electronic access control systems) systémy kontroly vstupů pro použití v bezpečnostních aplikacích, elektronické systémy kontroly vstupu.
- **CCTV/VSS** – řada norem ČSN EN 50132 a ČSN EN 62676 (Closed circuit television/Video surveillance systems) CCTV dohledové systémy pro použití v bezpeč-

nostních aplikacích, dohledové videosystémy pro použití v bezpečnostních aplikacích.

- **SAS** – řada norem ČSN EN 50134 (Social alarm systems) systémy přivolání pomoci.
- **ATS/ATSN** – řada norem ČSN EN 50136 (Alarm transmission systems/Alarm transmission service network) poplachové přenosové systémy a zařízení.
- **FPS/FDAS** – řada norem ČSN EN 54 (Fire protection system/Fire detection and fire alarm system) elektrická požární signalizace.
- **ARC/MARC** – řada norem ČSN EN 50518 (Alarm receiving centre/Monitoring alarm receiving centre) dohledová a poplachová přijímací centra.
- **CCF** – ČSN CLC/TS 50398 – (Central Control Facility) poplachové systémy, kombinované a integrované systémy.



Obrázek 23. Bezpečnostní integrační platforma. [53]

4.4 Norma ČSN CLC/ 50398

ČSN CLC/TS 50398 Poplachové systémy – Kombinované a integrované systémy - Všeobecné požadavky

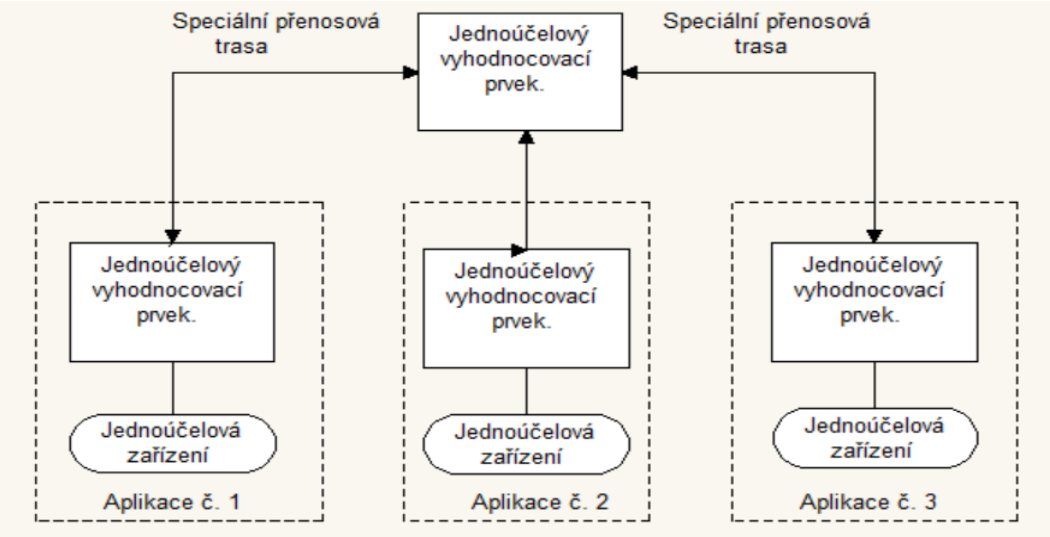
Tato norma uvádí všeobecné požadavky na typy struktur kombinovaných a integrovaných poplachových systémů. Norma má zajistit integraci jedné nebo více aplikací do jednoho

integrovaného systému. Norma obsahuje informace o prvotním návrhu systému, plánování, instalaci, předání, provozu a údržbě kombinovaného integrovaného systému. [41]

Dále norma specifikuje požadavky na poplachové systémy, které jsou kombinovány, nebo integrovány s jinými systémy, které mohou, být poplachovými systémy. Součástí této normy je definice pravidel integrace s cílem zdůraznit význam jednotlivých aplikačních poplachových norem a objasnit případné rozpory. [41]

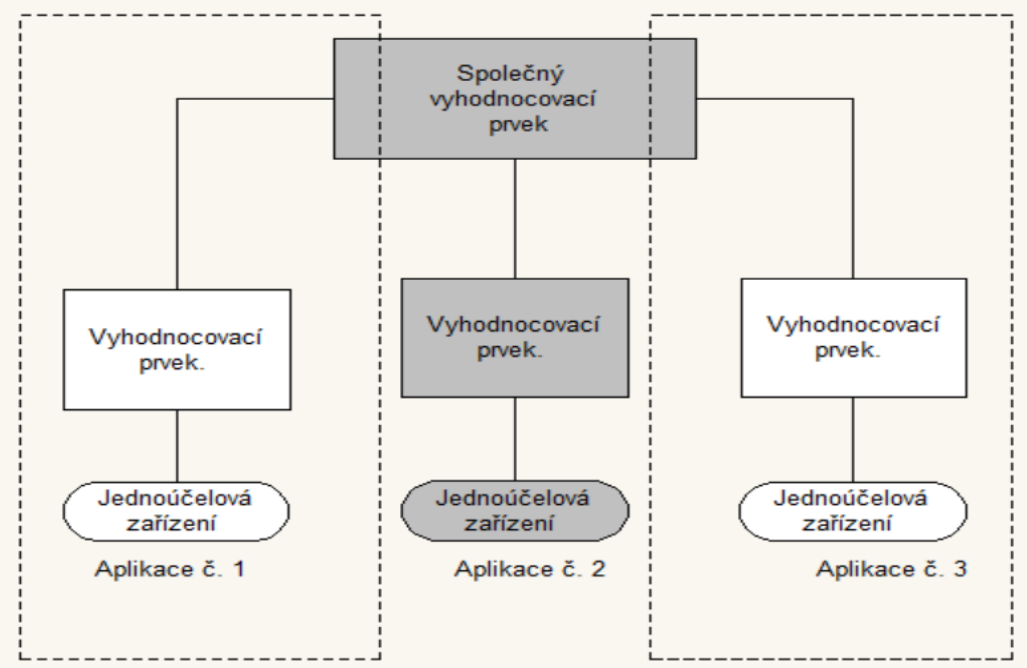
4.4.1 Typy konfigurace integrovaných poplachových systémů

- Konfigurace typu 1 je kombinací dvou nebo více jednoúčelových systémů, které jsou připojeny ke společnému doplňkovému zařízení. Při typu konfigurace 1 nesmí žádné provozní zařízení negativně ovlivňovat další jednoúčelový systém. [48]



Obrázek 24. Příklad konfigurace typu 1, ústřední ovládací zařízení (CCF) třídy 1(čárkované čáry ukazují ty části každé aplikace, které splňují jejich aplikační normy, pokud existují). [48]

- Konfigurace typu 2 je kombinací dvou nebo více jednoúčelových systémů, kdy všechny systémy využívají normou vyžadované zařízení společné nejméně pro jednu aplikaci. Konfigurace typu 2 se dále dělí na Typ 2A a Typ 2B. Rozdíl mezi těmito dvěma typy je dán v tom, že konfigurace 2A nesmí být integritou jakéhokoliv normou vyžadovaného poplachového zařízení v jakékoliv aplikaci být nepříznivě ovlivněna žádnou poruchou v jiné aplikaci. U typu 2B může být integrita ovlivněna jedinou poruchou v jiné aplikaci. [48]



Obrázek 25. Příklad konfigurace typu 2 (čárkované čáry a šedá pole ukazují ty části každé aplikace, které splňují své aplikační normy, pokud existují. [48]

4.4.2 Systémové požadavky

Integrovaný poplachový systém musí být projektován tak, aby žádná jeho aplikace v normálním stavu (včetně stavu poplachového) nepříznivě neovlivňovala jinou aplikaci. V rámci kombinovaných a integrovaných systémů mohou být povelové signály přenášeny z jedné aplikace do druhé nebo z ústředního ovládacího zařízení (CCF) do dalších částí aplikace. Využití povelových signálů může být výhodné pro organizaci správy velkých budov nebo celých areálů, ale může také snižovat úroveň zabezpečení, je-li nesprávně použito. [48]

- Přístupové úrovně jednotlivých aplikací musí odpovídat příslušné normě a vyžadovanými úrovněmi pro každou aplikaci a nesmí umožnit neoprávněný přístup k jakékoliv jiné aplikaci. [48]
- **Společné ovládací zařízení** musí být jasné a jednoznačné. Pokud je jedním manuálním zařízením ovládáno více aplikací, tyto aplikace musí být jasně identifikovány, že jsou tímto zařízením ovlivněny. [49]
- **Společné signalizační zařízení** může být doplňkové nebo normou vyžadované. Vždy je třeba signalizovat na základě priorit tak, aby byla nejkritičtější informace

viditelná za předpokládané úrovně osvětlení. Je doporučené použít vícestupňové priority poplachů:

- **Priorita 1** poplachové signály vztahující se k ochraně života při požárním poplachu nebo napadení.
- **Priorita 2** poplachové signály při ochraně majetku nebo při nedovoleném vniknutí do objektu.
- **Priorita 3** poplachové signály z ostatních poplachových systémů.
- **Priorita 4** poruchové signály ze systémů ochrany života a majetku.
- **Priorita 5** poruchové signály z ostatních poplachových systémů.
- **Priorita 6** informace z nepoplachových systémů.

Pokud normy určují specifické barvy pro signalizaci, tak musejí být tyto barvy dodrženy, v případě rozporu mezi jednotlivými normami se je třeba řídit požadavky EN 60073. V případě akustické signalizace je třeba vycházet z daných podmínek a logického uvažování. [48]

- **Integrita normou vyžadovaných prvků pro zpracování poplachů:** u některých aplikací je aplikační normou vyžadováno monitorování programu tak, aby bylo detekováno a signalizováno selhání monitorovací sekvence. [48]
- **Dělení poplachového softwaru:** je doporučeno oddělit software jednotlivých poplachových aplikací. Možný vliv softwaru jedné aplikace na jiné aplikace by měl být popsán ve zvláštním dokumentu. [48]
- **Centrální ovládací zařízení** se dále dělí do tříd. Třída 1 určuje, že centrální ovládací zařízení smí být použito pouze k zobrazení informací v prostorách, kde na systém dohlíží obsluha. Třída 2 určuje, jak lze v souladu s normami použít centrální zobrazovací zařízení nejen zobrazení na centrálním zařízení, ale i ovládací prvky, pokud jsou součástí. [48]
- **Propojení:** pokud jsou k zařízením splňujícím požadavky norem připojena zařízení, která nesplňují jednu nebo více norem musí být splněny následující požadavky[48]:
  - Pracuje pouze s povely, které povolují aplikační normy.
  - Neidentifikované signály nemají nepříznivý vliv.
  - Úmyslné zasahování nemá nepříznivý vliv nebo musí splňovat požadavky příslušných aplikačních norem.

4.5 Dílčí závěr

Tato kapitola pojednává o integraci bezpečnostních systémů a vytvoření bezpečnostní integrační platformy, která jednotlivé bezpečnostní i nebezpečnostní systémy spravuje. Hlavními důvody pro zavedení BIP jsou zvýšení bezpečnosti areálu, možnost automatizovat jednotlivé operace v systému, jednotné uživatelské rozhraní a podpora map. Celkově bezpečnostní integrační platforma představuje vrcholný zastřešující systém, který umožňuje efektivní správu bezpečnostních a jiných systémů. Mezi nevýhody bezpečnostní integrační platformy patři velká náročnost na jednotlivé systémy s důrazem na interoperabilitu. Tato kapitola se věnuje jednotlivým funkčním celkům, které mohou být použity v bezpečnostní integrační platformě, a jejich ukotvení v příslušných normách.

Součástí této kapitoly je detailnější popis normy ČSN CLC/TS 50398, jež popisuje všeobecné požadavky pro kombinované a integrované systémy.

II. PRAKTICKÁ ČÁST

5 KOMPARACE TECHNICKÉHO STAVU OCHRANY PERIMETRU V PRŮMYSLOVÉM OBJEKTU

V praktické části se diplomová práce zabývá možnostmi integrace kamerového dohledového systému ATEAS s integrační platformou C4 pro potřeby velké výrobní společnosti. Cílem je vytvořit funkční integrační propojení mezi těmito systémy, které dále spravují detektory ochrany perimetru Peridect od firmy Sieza a kamery od výrobců Hikvision a Axis.

5.1 Observace zabezpečovaného perimetru

Pro ověření funkčnosti propojení bezpečnostních systémů byly v zabezpečovaném průmyslovém objektu vybrány dvě vzorové plotové zóny vybavené detektory Peridect. Pro snadnější odlišení v dalších částech této práce jsou označeny jako zóna A a zóna B.

5.1.1 Zóna A

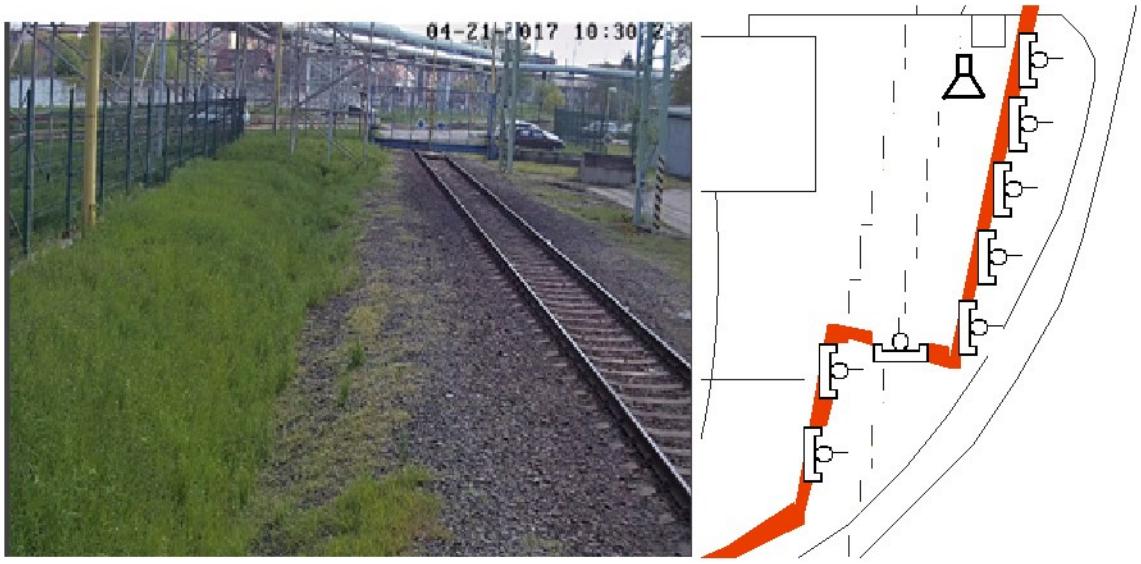
Zóna A se nachází na jihozápadní straně objektu a ochrana perimetru je zde zajištěna pomocí plotových detektorů Peridect, které jsou umístěny na bezpečnostním, svařovaném, zvlněném pletivu. Tuto část perimetru snímá několik kamer, ale jako hlavní kamera pro integraci s ostatními systémy byla zvolena kamera IP kamera AXIS Q6114 E. Tato dome IP kamera umožňuje díky svému umístění a možnosti otáčení sledovat celý perimetr zóny A.

Obrázek 26. Rohový výřez z mapy areálu zobrazující zónu A a plotové detektory, které jsou umístěny na bezpečnostním oplocení.

Obrázek 27. Obrazy kamery AXIS Q6114 E při pohledu na zónu A.

5.1.2 Zóna B

Zóna B se nachází na severní straně objektu tato zóna je zabezpečena pomocí plotových detektorů Peridect umístěných na bezpečnostním oplocení. Tuto část perimetru snímá IP kamera HIKVISION – DS-2CD4A35FWD.



Obrázek 28. Zóna B obraz kamery HIKVISION – DS-2CD4A35FWD a výřez z mapy areálu s naznačeným umístěním detektorů a kamery.

5.2 Obvodový detekční systém Peridect

Perimetrická ochrana objektu je zajištěna jak bezpečnostním oplocením, tak detekčním systémem Preridect, který je nainstalován na bezpečnostním oplocení. Tento systém je založen na detekci vibrací, které vznikají při pokusu o překonání (přelezení, prostříhání, nadzvednutí) oplocení. Instalace je provedena tak, že je na jeden plotový dílec připevněn jeden detektor. Každý detektor obsahuje piezoelektrický element doplněný o mikroprocesor, který se stará o zpracování signálu.

Firma Sieza, která je výrobcem detekčního systému Peridect, navrhuje tento systém tak, aby bylo možno použít několik typů detektorů přímo od tohoto výrobce a současně systém rozšířit o další detektory od jiných výrobců.

5.2.1 Součásti systému Peridect

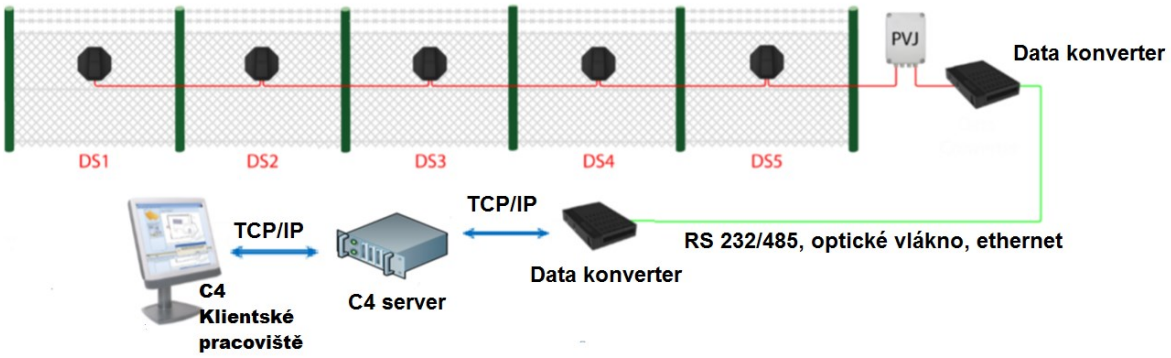
- **Peridect vyhodnocovací jednotka – PVJ** představuje mozek systému Peridect, tato jednotka umožňuje ovládat až 246 plotových detekčních senzorů, 8 vstupně výstupních modulů, 10 programovatelných výstupů, 8 dvojitě vyvážených vstupů. Peridect vyhodnocovací jednotka je s dalšími systémy propojena pomocí sériové linky RS-232.
- **Peridect detekční senzor – PDS** detekční jednotka založená na piezoelektrickém měniči. Tento senzor generuje až 400 vzorků za sekundu, které zpracovává pomocí mikroprocesoru a do systému předává v digitální podobě. Systém umožňuje individuální nastavení každého detektoru. Detektory jsou vyráběny v několika provedeních (klasické, antivandal, skryté).

Tento systém je certifikován pro zabezpečení objektu do stupně zabezpečení 4 (vysoké riziko) a je testován v teplotním rozsahu od -55 °C až do +85 °C. Z hlediska působení vnějších vlivů podle normy ČSN 33 2000-5-51 ed. 3 jde o typ prostředí vnitřní prostředí normální, venkovní zvlášť nebezpečné.

Obrázek 29. Peridect detektor [48]

5.2.2 Integrace systému Peridect se systémem C4

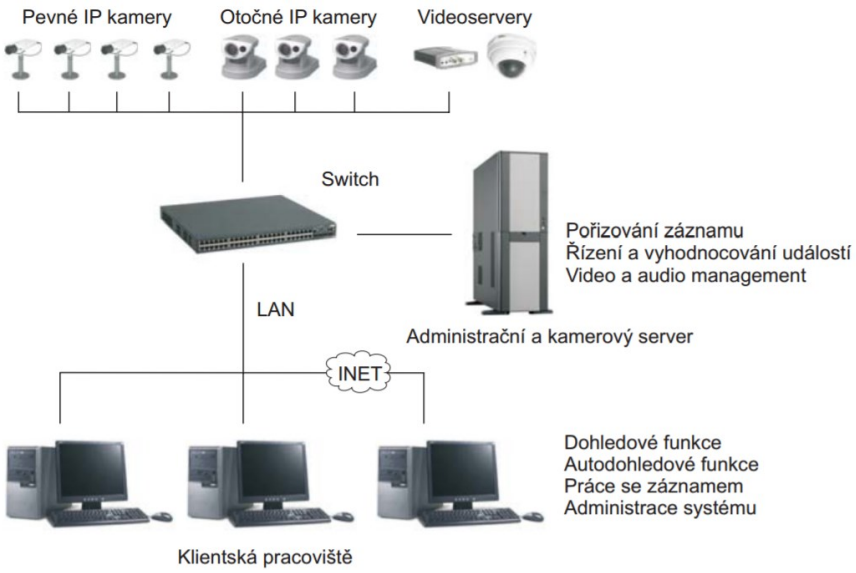
Při integraci systému Peridect s integrační platformou C4 je využito Peridect vyhodnocovací jednotky, která umožňuje komunikaci pomocí sériové sběrnice RS-232. Dále jsou pak data přenesena do data konvektoru, který zajistí přenos dat pomocí RS-232/485, optického kabelu nebo ethernetu. Data jsou dále zpracována v C4 serveru a zobrazena na klientské stanici. Celý systém Peridect lze ovládat ze systému C4.



Obrázek 30. Topologie připojení systému Peridect a systému C4. (DS - detekční senzor PVJ – vyhodnocovací jednotka). [48]

5.3 ATEAS Security PROFESSIONAL

Pro správu IP kamer je v průmyslovém objektu použit software Ateas ve verzi profesionál. Tento systém je postaven na bázi klient server a umožňuje správu až 64 kamer. Veškeré operace, jako je záznam obrazu a jeho zpracování, probíhají na serveru. K tomuto serveru může být připojen libovolný počet klientských stanic pro zobrazení obrazu. V zabezpečovaném průmyslovém objektu je nasazena verze profesionál, která umožňuje integraci tohoto systému se systémem C4. [50]

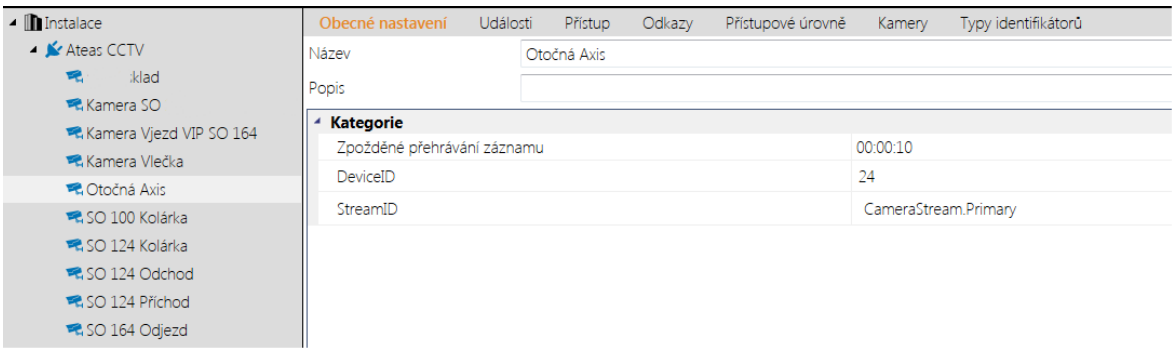


Obrázek 31. Schéma ATEAS Security. [50]

5.4 Integrace systému ATEAS se systémem C4

Pro integraci systému ATEAS se systémem C4 je třeba nainstalovat na server C4 příslušný ATEAS ovladač. Pro vzájemnou komunikaci mezi servery ATEAS a C4 je použit protokol TCP/IP a port 8504, který je otevřen na serveru ATEAS.

Po úspěšné instalaci ovladače a propojení systémů je možné do systému C4 přidat kamery a to v menu zařízení.



Obrázek 32. Strom zařízení v systému C4 po propojení systémem ATEAS.

5.4.1 IP kamery spravované systémem ATEAS

V rámci průmyslového objektu je využito více typů IP kamer, které jsou spravovány softwarem ATEAS. Pro ověření možnosti integrace kamer s integrační systémem C4 byly vybrány kamery IP kamera AXIS Q6114 E a IP kamera HIKVISION – DS-2CD4A35FWD.

5.4.1.1 IP kamera AXIS Q6114 E

Kamera od předního výrobce IP kamer, která umožňuje snímat obraz v kvalitě HDTV 720p s 30 násobným optickým přiblížením. Tato dome IP kamera je vhodná pro ochranu rozlehlých oblastí, jako jsou letiště nebo průmyslové objekty. Kamera je dále vybavena slotem na paměťové karty a otřesovým detektorem, který upozorní na případný pokus o vandalizmus nebo jiné poškozování kamery. Připojení kamery a její napájení je zajištěno pomocí síťového kabelu. Tato kamera může pracovat při teplotách od -50°C do +50°C a relativní vlhkosti 100%. [**Chyba! Nenalezen zdroj odkazů.**]

Obrázek 33. AXIS Q6114 E [51]

5.4.1.2 IP kamera HIKVISION – DS-2CD4A35FWD

Statická kamera od čínského výrobce umožňuje snímat obraz v HD kvalitě 2048 x 1536 a 45 snímků za sekundu. Tato kamera je vhodná pro snímání plotů, bran a dalších statických objektů. Díky vysokému stupni IP 67 krytí je ji možno použít ve venkovním prostředí. Napájení a přenos dat probíhá přes síťový kabel. [52]

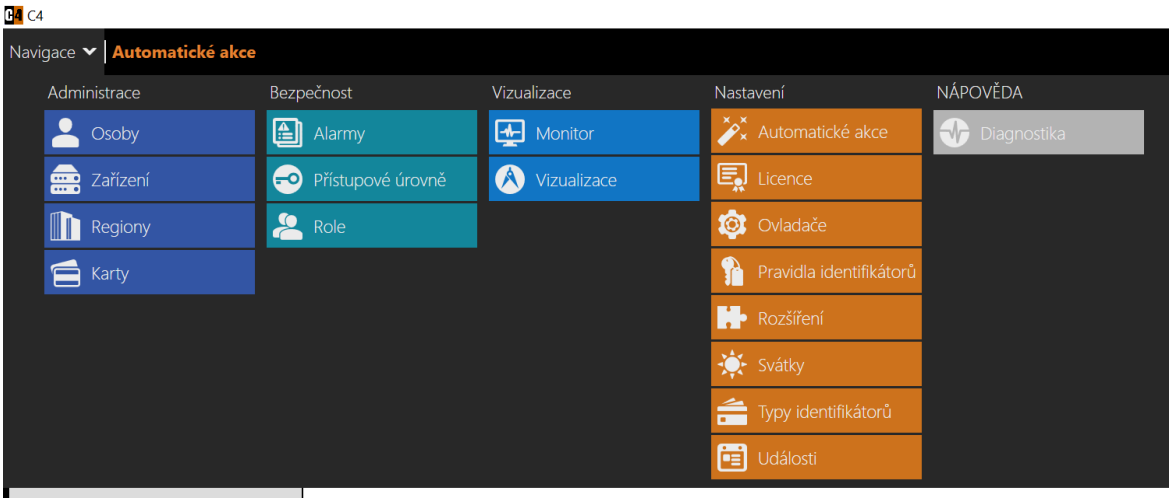
Obrázek 34. HIKVISION – DS-2CD4A35FWD [52]

5.5 Systém C4

Integrační bezpečnostní systém C4 poskytuje centralizované víceuživatelské rozhraní pro správu budov. Tento systém je postaven na otevřené architektuře, která umožňuje snadné přizpůsobení jednotlivým objektům a požadavkům zákazníků. Výrobcem tohoto softwaru je společnost Gamanet, která na svých webových stránkách www.c4portal.com uvádí seznam podporovaných zařízení pro tento systém. [55]

Tento systém slouží jako vrcholná integrační platforma v zabezpečovaném průmyslovém objektu a umožňuje spolupráci jednotlivých bezpečnostních systémů. Systém C4 uživatelům poskytuje tyto možnosti:

- Centrální správu bezpečnostních zařízení.
- Vizualizaci a monitoring zařízení.
- Automatizaci bezpečnostních procesů.
- Analýzu a vyhodnocení bezpečnostních informací.
- Centrální databázi osob a identifikátorů.
- Podpora krizového managementu.



Obrázek 35. Systém C4 Menu po instalaci ve verzi 2016.

5.6 Dílčí závěr

Tato kapitola seznamuje se zabezpečovaným průmyslovým objektem a jednotlivými zónami perimetru, které jsou použity pro ověření integrace bezpečnostních systémů. Dalším cílem této kapitoly je poskytnout přehled o použitých bezpečnostních systémech a jejich vzájemném propojení.

6 KOMPARATIVNÍ STUDIE STŘEŽENÍ PERIMETRU

Cílem této kapitoly je komparovat současné systémy zabezpečení perimetru popsané v předešlé kapitole s dalšími bezpečnostními systémy dostupnými na trhu. Nejprve je představen systém AXIS Perimeter Defender, který funguje na principu video analýzy.

Ve druhé polovině této kapitoly jsou představeny integrační platformy, které jsou komparovány se současným systémem C4. Pro porovnání jsou zvoleny integrační platformy s uživatelským rozhraním v českém jazyce.

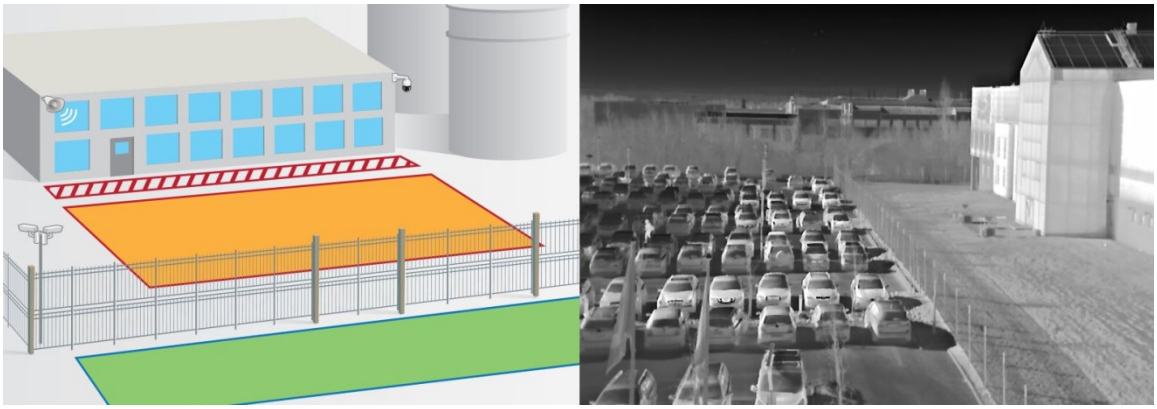
6.1 AXIS Perimeter Defender

Společnost AXIS Communications je na trhu se zabezpečovací technikou dobře známa díky svým bezpečnostním kamerám, které nesporně prokazují své kvality. Tato společnost představila vlastní řešení ochrany perimetru založené na video analýze, kdy není již pro zachycení pachatele potřeba použít žádný z typů PZTS detektorů, ale samotná kamera je schopna rozpoznat pohyb v obraze a reagovat v případě narušení chráněné zóny.

6.1.1 Způsob fungování systému Axis Perimeter Defender

Axis Perimeter Defender pracuje na principu pokročilé video analýzy, která probíhá přímo v IP kameře, což umožňuje připojit do systému prakticky neomezené množství IP kamer, případně postupně navyšovat počet kamer bez nutnosti výměny hardwaru. Celý tento systém může být kontrolován z jednoho uživatelského rozhraní, nebo fungovat na serveru s možností více uživatelských rozhraní. Veškerý přenos v síti probíhá pomocí TCP/IP protokolu. [54]

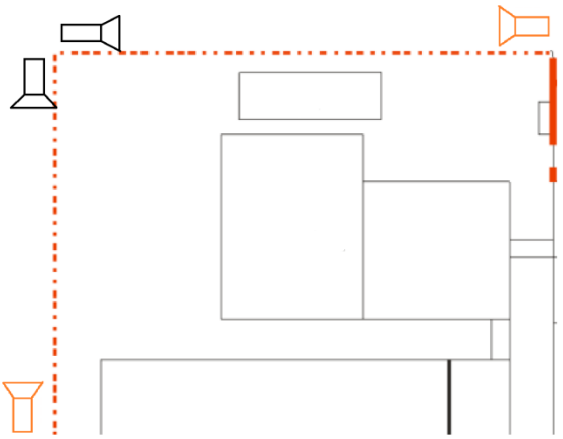
Tento bezpečnostní systém je nejčastěji použit společně s kamerami umístěnými přímo na plotové konstrukci nebo v těsné blízkosti bezpečnostního oplocení tak, aby bylo možno vytvořit více zón, které může kamera sledovat. Na každé z těchto zón může být jiný typ poplachu. Takovéto rozdělení do střežených zón umožní objevit případného pachatele ještě před pokusem o překonání oplocení. Systém bývá často doplňován o reflektory a venkovní reproduktory, které umožňují komunikaci s osobou, jež narušila zónu. U tohoto systému zabezpečení perimetru jsou často využívány IP termální kamery, které jsou vhodné pro denní i noční provoz. [54]



Obrázek 36. Detekce pomocí zón a obraz z AXIS IP termální kamery. [54]

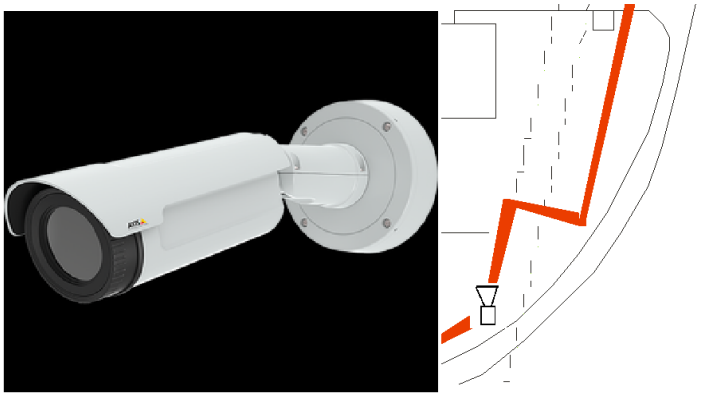
6.1.2 Zabezpečení průmyslového objektu pomocí AXIS Perimeter Defender

Pro zabezpečení průmyslového objektu pomocí tohoto systému by bylo třeba do zóny A, jak ji definuje kapitola 5.1.1, umístit dvě další kamery od výrobce AXIS tak, aby byla celá plotová část pod stálým dohledem. Tyto kamery by bylo možné umístit do rohové části, oplocení nebo na jeho krajní části, viz Obrázek 38.



Obrázek 37. Možné rozmístění kamer při použití AXIS Perimeter Defender, jednotlivé varianty jsou odlišeny barvami.

Pro zabezpečení zóny B by bylo třeba zónu doplnit o jednu AXIS termální kameru, která by mohla doplnit kameru HIKVISION – DS-2CD4A35FWD. Umístění termální kamery by bylo na bezpečnostním oplocení naproti kameře HIKVISION, aby bylo docíleno pokrytí celého perimetru zóny B.



Obrázek 38. Termální kamera AXIS Q1942-E [54]

a její umístění v zóně B.

6.1.3 Termální kamery

S bezpečnostním systémem AXIS Perimeter Defender mohou spolupracovat všechny kamery vybavené otevřenou platformou ACAP (Axis Camera Application Platform), která umožňuje používat analytické a bezpečnostní aplikace. [54]

Pro případ komparativní studie při použití bezpečnostního systému AXIS Perimeter Defender pro zabezpečení průmyslového objektu byly jako kamery zvoleny termální kamery AXIS Q1942-E, které jsou výrobcem doporučovány. [54]

Termální kamery mohou spolehlivě pracovat 24 hodin denně díky tomu, že jsou méně citlivé na venkovní osvětlení, klimatické podmínky (mlha, kouř…). Mezi další výhody termálních kamer patří možnost sledovat teplotu a upozornit na případné přehřívání či vznikající požár. [54]

Obrázek 39. Porovnání klasické kamery a termální při zhoršených světelných podmínkách. [54]

6.1.4 Termální kamera AXIS Q1941-E

Tato kamera nabízí rozlišení 384x288, které umožňuje detekovat, rozpoznat a identifikovat lidskou postavu a osobní vozidlo dle použité ohniskové vzdálenosti a obrazového úhlu, viz Tabulka 5.

Tabulka 5. Rozsahy detekce termální kamery AXIS Q1941-E. [54]

Rozsahy detekce termální kamery AXIS Q1942-E				
	Ohnisková vzdálenost [mm]	**Obrazový úhel horizontální**	**Detekce lidská postava (1,8 x 0,5m) [m]**	**Detekce vozidlo (4x 1,5m) [m]**
Detekce (1,5 pixelu na cíl)	7	55°	200	613
	13	28°	393	1205
	35	10,7°	1028	3153
	60	6,2°	1774	5441
Rozpoznání (6 pixelů na cíl)	7	55°	50	153
	13	28°	98	301
	35	10,7°	257	788
	60	6,2°	444	1360
Identifikace (12 pixelů na cíl)	7	55°	25	77
	13	28°	49	151
	35	10,7°	129	394
	60	6,2°	222	680

6.1.5 Cenová kalkulace

V této cenové kalkulaci nejsou zahrnuty náklady na montáž systému, které nelze přesně vyčíslit bez konzultace s dodavatelem těchto technologií. Ceny u jednotlivých položek odpovídají cenně uváděné v době zpracování této práce a jsou uváděny bez DPH.

Samotný systém je zpoplatněn pomocí licencí, které se přiřazují k jednotlivým kamerám tak, že jedna licence umožňuje fungování jedné kamery v systému. Společnost AXIS má ve své nabídce dvě možnosti pro nákup těchto licencí, kdy je možné koupit jednu licenci nebo deset licencí najednou. Celková cena za pořízení tří termálních kamer a licencí k nim je 238 722 Kč.

Tabulka 6. Cenová kalkulace pro systém AXIS Perimeter Defender.

Cenová kalkulace pro systém AXIS Perimeter Defender				
Jednotlivé položky	Cena za jednu položku [Kč]	Množství položek	Celková cena [Kč]	Poskytovatel
Termální kamera AXIS Q1942-E	72 274	3	216 822	TZK s.r.o.
1 licence (0333-606)	7 300	3	21 900	Surveillance-Video
10 licencí (0333-607)	73 000	není použito	není použito	Surveillance-Video

6.1.5.1 Výhody systému AXIS Perimeter Defender

- Snadná aplikace na většinu kamer od výrobce AXIS.
- Možnost zaznamenat pokus o napadení ještě před samotným pokusem o zdolání systémů MZS.
- Práce s detekčními zónami, možnost automatické výzvy k opuštění perimetru.
- Komunikace s mobilními aplikacemi.
- Zpracování dat probíhá přímo v kameře.
- Propojení klasických a termálních kamer.

6.1.5.2 Nevýhody

- Pouze bezpečnostní systém, částečně doplnitelný o přístupové systémy.
- Omezené možnosti integrace do dalších systémů.
- Bez možnosti českého jazyka.
- Cena AXIS kamer je při porovnání s konkurencí vyšší.
- Nutná podpora Axis Camera Application Platform bez možnosti přidat kamery od jiných výrobců.
- Velké množství použitých kamer, u kterých je třeba řešit přenos dat, záznam dat, ochrana osobních údajů.

6.1.6 Dílčí závěr

AXIS Perimeter Defender představuje zajímavé řešení ochrany perimetru, které plně spoléhá na kamery jak běžné IP kamery, tak i na IP termální kamery. Nespornou výhodou tohoto systému je, že z běžných IP AXIS kamer dokáže velmi rychle vytvořit systém k ochraně perimetru bez nutnosti použití PZTS systému.

Mezi mínusy tohoto systému patří snížená interoperabilita systému s dalšími bezpečnostními i nebezpečnostními systémy, chybějící česká lokace systému a nemožnost použít kamery od jiných výrobců.

Dle mého názoru by tento systém mohl představovat zajímavé řešení pro ochranu některých částí perimetru (vjezdové brány, místa bez oplocení, automatické vykazování lidí z nebezpečných prostor), ale pro celý perimetr zabezpečovaného průmyslového objektu by nepředstavoval velký přínos.

6.2 Integrační platformy

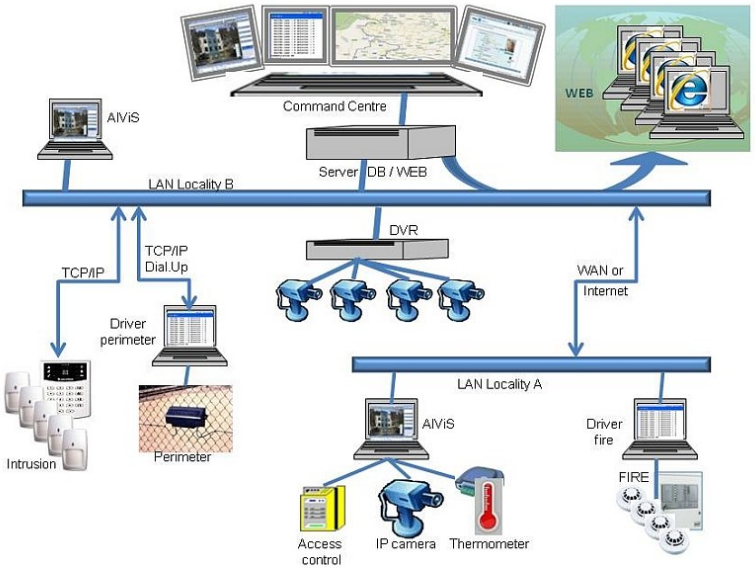
Na trhu v České a Slovenské republice je velký počet různých integračních platforem (systémů) a je velmi obtížné zvolit pro konkrétní nasazení tu správnou. Mezi nejznámější integrační platformy patří: Alvis, MrGuard, AS200, C4, ECC, Eliwin, Integra, MCT-S, LATIS SQL. Tyto integrační platformy jsou často upravovány přímo pro konkrétní projekt, a proto je velice důležitá při jejich zavádění podpora od výrobce.

Z těchto nejznámějších integračních platforem byly zvoleny dvě a dále porovnány se současnou integrační platformou C4. Výběr proběhl na základě dostupných informací o těchto integračních platformách.

6.2.1 AlViS Alarm Visualization System

Grafický systém pro integraci, řízení a monitorování technologií budov od výrobce Spirit a.s. patří k velice často užívaným integračním systémům v České a Slovenské republice. Tento systém můžeme najít například na Pražském hradě, ve Fakultní nemocnici v Motole nebo v jaderných elektrárnách Mochovce a Bohunice. AlViS systém přímo podporuje připojení více než 100 různých zařízení od více než 40 výrobců. Pro připojení dalších systémů, které nejsou přímo podporovány systémem Alvis je důležité, aby tyto systémy podporovaly některý z otevřených komunikačních protokolů (OPC, Modbus, Espa, DDE, Ascii). [56]

Architektura systému AlViS je modulární s možností kombinovat architekturu klient/server. Výhodou tohoto systému je možnost přístupu přes webový prohlížeč Internet Explorer. Ovladače systému komunikují s grafickým klientem pomocí síťového rozhraní TCP/IP přes síť Internet a v lokáních sítích využívají protokol DDE (Dynamic Data Exchange). [56]



Obrázek 40. Systém AlViS [56]

Samotný systém AlViS pracuje ve dvou režimech v režimu vývoj a monitorování. V režimu *vývoj*, který je určen pro návrh systému. V tomto režimu je možné do systému přidávat plány objektů (nakreslené nebo v rastrové podobě), využít skriptovací jazyk a používat další funkce pro správu systému. V režimu *monitorování* jsou aktivní vstupně-výstupní linky a je zobrazen stav jednotlivých zařízení v systému.[56]

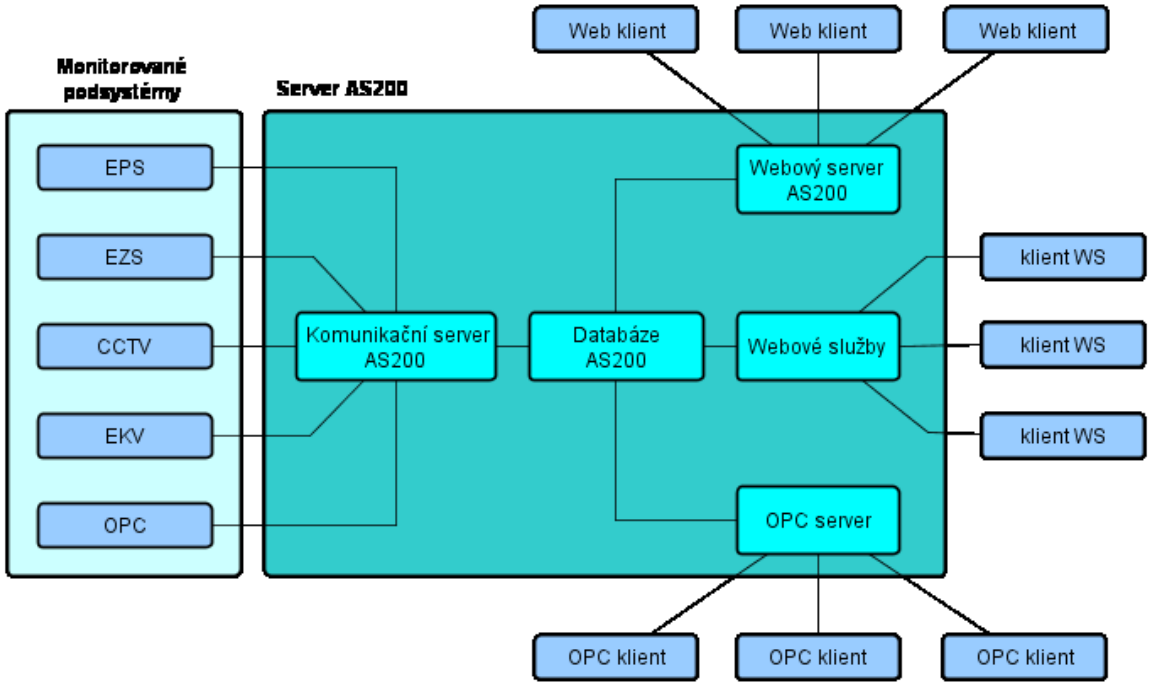
6.2.1.1 Porovnání systému AlViS se systémem C4

Systém AlViS představuje komplexní systém, jenž umožňuje stejně jako systém C4 správu poplachových systémů, systémů požární ochrany, přístupových systémů a kamerových systémů. Kromě těchto zmíněných systémů systém AlViS dokáže více pracovat s automatizací budov (topení, ventilace, výtahy, osvětlení). Mezi výhody systému AlViS patří možnost přístupu do systému pomocí webového prohlížeče. Hlavní nevýhodou tohoto systému AlViS oproti systému C4 je složitější správa systému, což je dáno jeho komplexností.

6.2.2 Systém AS200

Tento systém je vyvíjen společností A2D s.r.o., která se od roku 1992 zabývá bezpečnostními systémy. Systém umožňuje vizualizaci areálu s možností přesné lokace jednotlivých prvků v systémech. Pro lepší spolupráci s bezpečnostní službou je možné tisknout výjezdové karty s podrobnými informacemi o poplachu. [57]

Systém AS200 v současné době plně spolupracuje s 15 výrobci bezpečnostních systémů a více než čtyřiceti těmito výrobci vyráběnými systémy. Tento systém je založen na modularitě jednotlivých systémů a jejich ústředen, díky čemuž je možné současně provozovat starší analogové systémy a novější digitální. Mezi přednosti systému AS200 patří OPC (Open Platform Communications), díky tomu je možné pracovat s automatizací budov. [57]



Obrázek 41. Schéma zapojení systému AS200 klient/server. [57]

6.2.2.1 Porovnání systému AS200 se systémem C4

Výhodou systému AS200 je podpora OPC (Open Platform Communications), která umožňuje automatizaci budovy a jiných procesů při správě objektu. Mezi další výhody patří možnost práce se systémem přes webové služby.

Výhody systému C4 oproti systému AS200 jsou: podpora více zařízení, lepší podpora a aktualizace pro zákazníka, snadnější ovládaní systému, přehlednější mapové podklady, srozumitelnější a modernější uživatelské rozhraní.

6.3 Dílčí závěr

Tato kapitola porovnává současné systémy zabezpečení perimetru v zabezpečovaném průmyslovém objektu s dalšími systémy zabezpečení, které jsou aktuálně na trhu. Toto porovnání se soustředí výhradně na systémy poplachové a zabezpečovací, kamerové a integrační, do tohoto porovnání nejsou zahrnuty mechanické zábranné systémy z toho důvodu, že současné bezpečnostní oplocení splňuje požadavky pro ochranu objektu tohoto typu.

Obecnému popisu PZTS detektorů používaných při ochraně perimetru se věnuje druhá kapitola v teoretické části, a proto byl pro srovnání se současným zabezpečením zvolen systém AXIS Perimeter Defender fungující na základě pokročilé video analýzy. Tento systém byl doplněn o termální kamery od stejného výrobce.

Tato kapitola se dále věnuje srovnání integračních platforem, které jsou dostupné na českém a slovenském trhu. Tyto platformy jsou srovnávány s integrační platformou C4, která je v současné době nasazena při integraci v průmyslovém objektu. Z tohoto srovnání vyplynulo několik doporučení pro zavádění integračních platforem, která jsou: používat již prověřená integrační řešení, pro propojení systémů používat otevřené formáty, zajistit si podporu od výrobců jednotlivých systémů, pokud možno budovat integrační platformu i se všemi bezpečnostními systémy jako celek, ne po částech.

Dle mého názoru je současný způsob a stupeň zabezpečení v zabezpečovaném průmyslovém objektu na dobré úrovni a po propojení kamerového systému s plotovým detekčním systémem bude tato úroveň ještě navýšena. Integrační platforma C4 patří mezi přední řešení tohoto typu na českém a slovenském trhu a ve srovnání s dalšími integračními systémy je vhodnou variantou pro ochranu perimetru. Mezi nevýhody systému C4 patří slabá podpora automatizace budov.

7 APLIKACE KAMEROVÉHO DOHLEDOVÉHO SYSTÉMU PRO AUTOMATICKÉ STŘEŽENÍ PERIMETRU

7.1 Integrace systému Peridect se systémem C4

Cílem této integrace je získat plnohodnotná data z plotového detekčního systému Peridect v integrační platformě C4. Díky této integraci získá uživatel možnost sledovat střeženou oblast v reálném čase na mapových podkladech včetně aktuálního stavu jednotlivých prvků. Systém C4 podporuje následující funkce systému Peridect: nahrání souborů, podpora časového pásma, potlačení poplachů, vzdálenou správu zařízení, možnost dynamických příkazů.

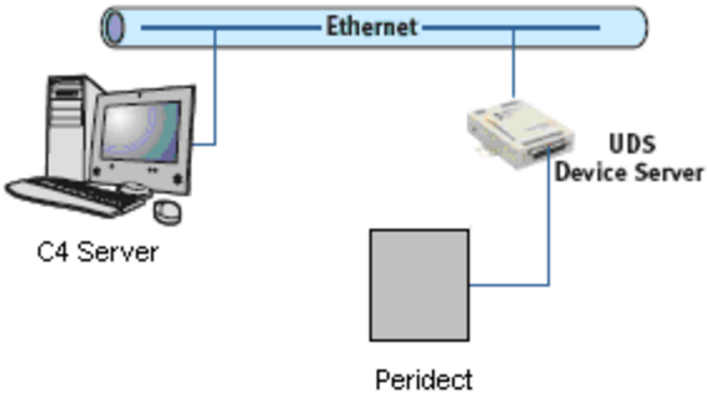
7.1.1 Instalace systému C4

Nejprve je třeba nainstalovat systém C4, ten funguje jako klasická aplikace typu klient-server a je detailně popsán v instalačním manuálu, který je součástí instalačního souboru. Po samotné instalaci na serveru je třeba oživit licenci a nahrát aktuální ovladač, který je dostupný po přihlášení na stránkách: https://www.c4portal.com.

Samotnou instalaci klientské verze lze provést ze serverové verze tak, že do adresového řádku prohlížeče je zadána IP adresa serveru v tomto formátu http://xxx.xxx.xxx.xxx/c4iis/client“, po tomto kroku se zobrazí stránka, ze které lze spustit instalaci aplikace C4 Klient. [55]

7.1.2 Připojení systému Peridect k systému C4

Systém Peridect komunikuje prostřednictvím sériového rozhraní RS 232, z tohoto důvodu musí být použito převodníku z RS 232 na TCP/IP. Pro přenos dat po převodu na TCP/IP lze použít standardních síťových zařízení (router, switch, eternet kabel a další). Přenos dat je prováděn tak, že je každou sekundu do systému Peridect odeslán jeden packet. V případě, kdy systém neobdrží odpověď na tři po sobě jdoucí žádosti, vyhodnotí tento stav jako poruchu spojení a zahájí proces inicializace připojení. [55]

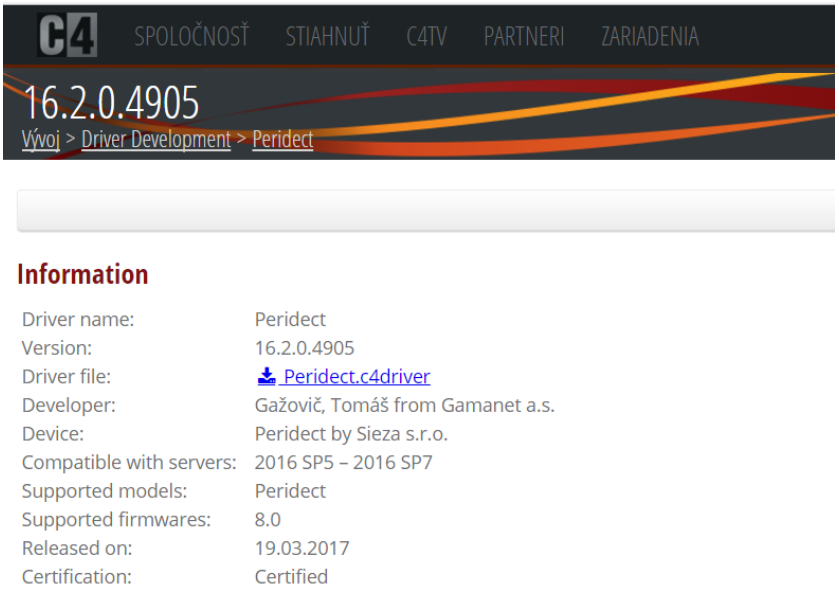


Obrázek 42. Komunikace systémů C4 a Peridect pomocí sítě Ethernet. [55]

7.1.3 Instalace ovladače systému Peridect

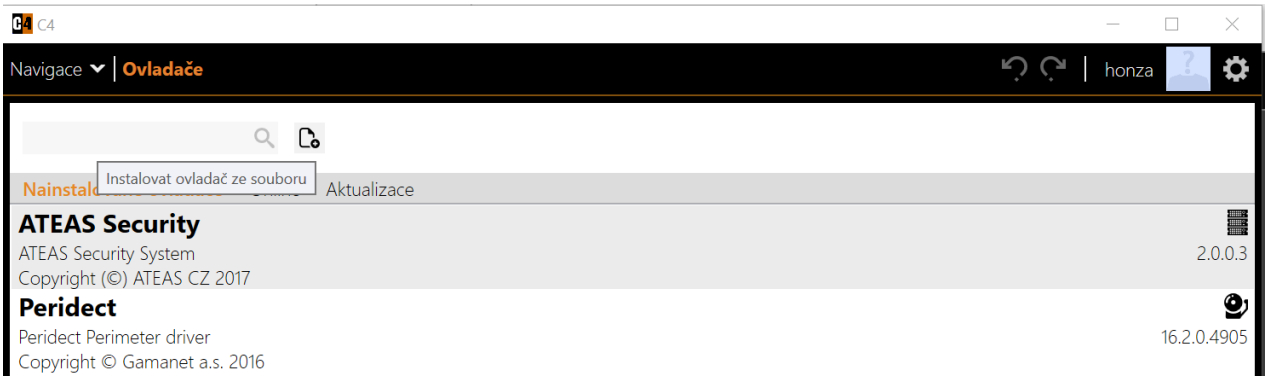
Při instalaci ovladače pro správu systému Peridect je potřeba následovat několik základních kroků:

- Stažení ovladače ze stránek *www.c4portal.com*, kde lze po přihlášení v záložce zariadenia najít veškerá podporovaná zařízení. Ovladače je možné stahovat i instalovat přímo v systému C4 v menu *Navigace-Nastavení-Ovladače-Online*.



Obrázek 43. Stažení ovladače systému Peridect. [55]

- Instalaci ovladače je možno provést v menu: *Navigace-Nastavení-Ovladače*. V tomto menu je možno spravovat jednotlivé nainstalované ovladače (vyhledávat, aktualizovat, instalovat online).



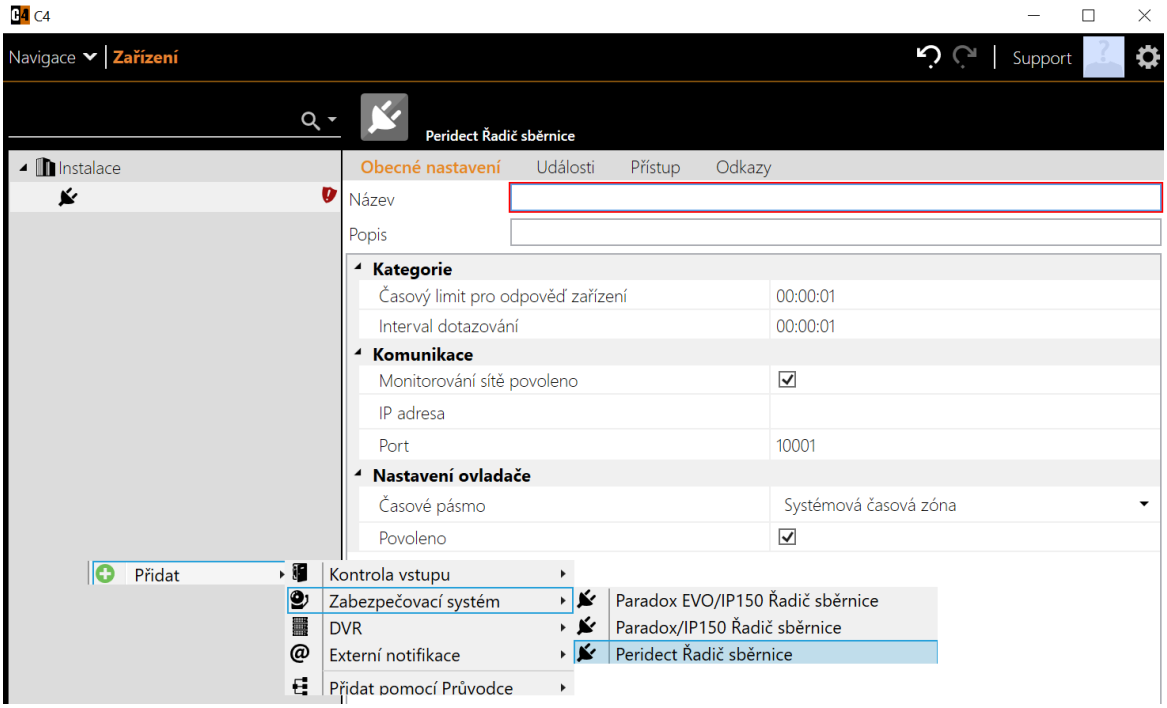
Obrázek 44. Zpráva ovladačů v systému C4.

7.1.4 Přidání systému Peridect do stromu zařízení v systému C4

Po úspěšné instalaci ovladače systému Peridect je třeba přidat tento systém do stromu zařízení v systému C4. Strom zařízení poskytuje uživateli rychlou orientaci o připojených systémech a zařízeních. Obecně systém C4 podporuje dva způsoby přidávání zařízení do stromu zařízení automaticky a manuální. U systému Peridect je třeba tento systém přidat manuálně, protože automatické přidání nepodporuje.

Postup při manuální detekci je následující:

1. V hlavním menu, které se otevře, po kliknutí na ikonu *Navigace*, je třeba zvolit *Zařízení.*
2. Na stránce se zařízeními je třeba kliknout pravým tlačítkem na myši do sloupečku *Instalace* a zvolit *Přidat-Zabezpečovací systém* a vybrat *Peridect Řadič sběrnice.*
3. Následně je třeba vyplnit informace, jako je IP adresa název prvku v systému.
4. Po úspěšném přidání systému Peridect do systému C4 je možné spustit datovou komunikaci mezi těmito systémy tak, že je na daný systém kliknuto pravým tlačítkem myši a je zvolen příkaz *Start* pro zahájení komunikace.
5. Po přidání systému Peridect do systému C4 a otestování vzájemné komunikace je třeba do systému C4 přidat Peridect zabezpečovací ústřednu tak, že je třeba pravým tlačítkem myši kliknout na *Peridect Řadič sběrnice* v levém sloupci *Instalace* (v menu *Zařízení*) a z nabídky zvolit *Přidat-Peridect Zabezpečovací ústředna.*
6. Po přidání *Peridect Zabezpečovací ústředny* by se tato ústředna měla objevit ve sloupci *Instalace* pod položkou *Peridect Řadič sběrnice*. Nyní je již možné k této ústředně připojovat jednotlivé detektory, a to opět pravým kliknutím myši tentokrát na položku *Peridect Zabezpečovací ústředna-Přidat*.

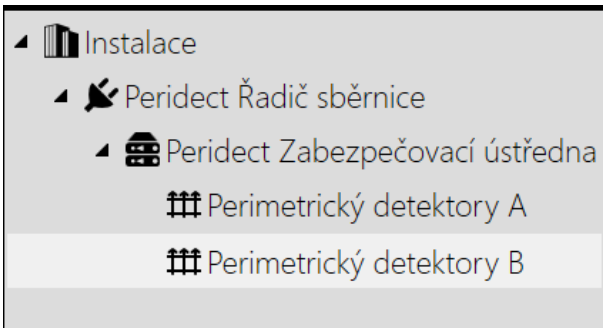


Obrázek 45. Přidání systému Peridect do stromu zařízení v systému C4.

7.1.5 Seskupování detektorů Peridect

Z důvodu praktičnosti při použití většího množství stejných detektorů je možné v systému C4 tyto detektory seskupovat do celků, jež se nazývají Multisenzory. Při použití systému Peridect je možné na jednu vyhodnocovací jednotku připojit až 246 detektorů. Každý z detektorů má své vlastní jedinečné číslo v rámci vyhodnocovací jednotky 1 až 246, díky tomuto jedinečnému číslu je možné detektory seskupovat do skupin.

Při seskupování detektorů je třeba postupovat následovně: pravé kliknutí myší na *Peridect Zabezpečovací ústředna-Přidat-Perimetrický detektor* dále už stačí uvést název daného seskupení a číslo prvního a posledního detektoru v dané skupině.



Obrázek 46. Strom zařízení v systému C4.

7.2 Integrace systému ATEAS se systémem C4

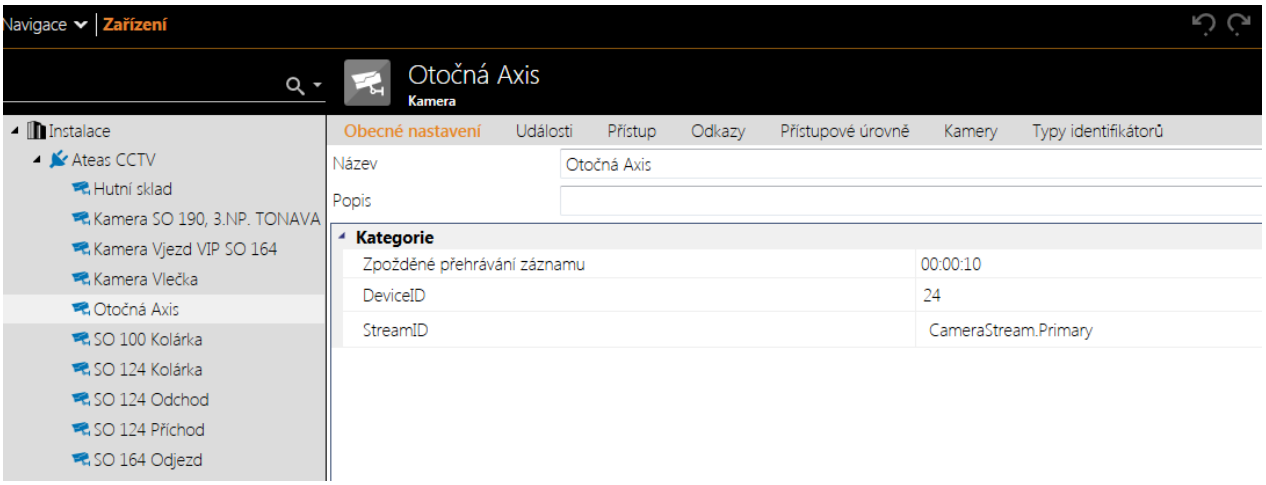
Systém ATEAS je možno integrovat se systémem C4 ve verzích professional a unlimited. Získání ovladače a jeho nainstalování je stejné jako u systému Peridect, popsáno v kapitole 7.1. Krom tohoto ovladače je třeba do systému C4 nainstalovat ATEAS Media Package pro zobrazení videa přímo v systému C4.

Komunikace mezi systémy probíhá pomocí TCP/IP protokolu a pro úspěšné propojení těchto systémů je nutné, aby na straně serveru ATEAS byl otevřen port 8504, toto je možné nastavit menu *Administrace-Externí uzel-Kanály*.

7.2.1 Funkce ovladače ATEAS

Systém C4 umožňuje integraci těchto funkcí ze systému ATEAS:

- Podpora otevřené platformy ONVIF a IP kamer, které tuto platformu podporují.
- Podpora nejčastěji používaných formátů videa MJPEG, MPEG4 a H264.
- Možnost živého přehrávání videa ve vysoké kvalitě.
- Možnost změny rychlosti přehrávaného videa.



Obrázek 47. Strom zařízení v systému C4 po integraci se systémem ATEAS.

7.2.2 Nastavení Presetů v systému ATEAS

U dome IP kamer je možné předefinovat nastavení snímání určitého prostoru. Toto nastavení se v systému ATEAS nazývá presety. Pro provázání kamery s jednotlivými plotovými detektory je třeba nastavit presety tak, aby kamera zabírala bezpečnostní oplocení po částech a pro každou tuto část byl definován preset s jedinečným číslem. Tyto presety jsou

následně spárovány s plotovými detektory Peridect. Nastavení presetů v systému ATEAS je možno provést v pravém horním rohu.

Obrázek 48. Presety v systému ATEAS

7.3 Propojení systému Peridect se systémem ATEAS v systému C4 při ochraně perimetru

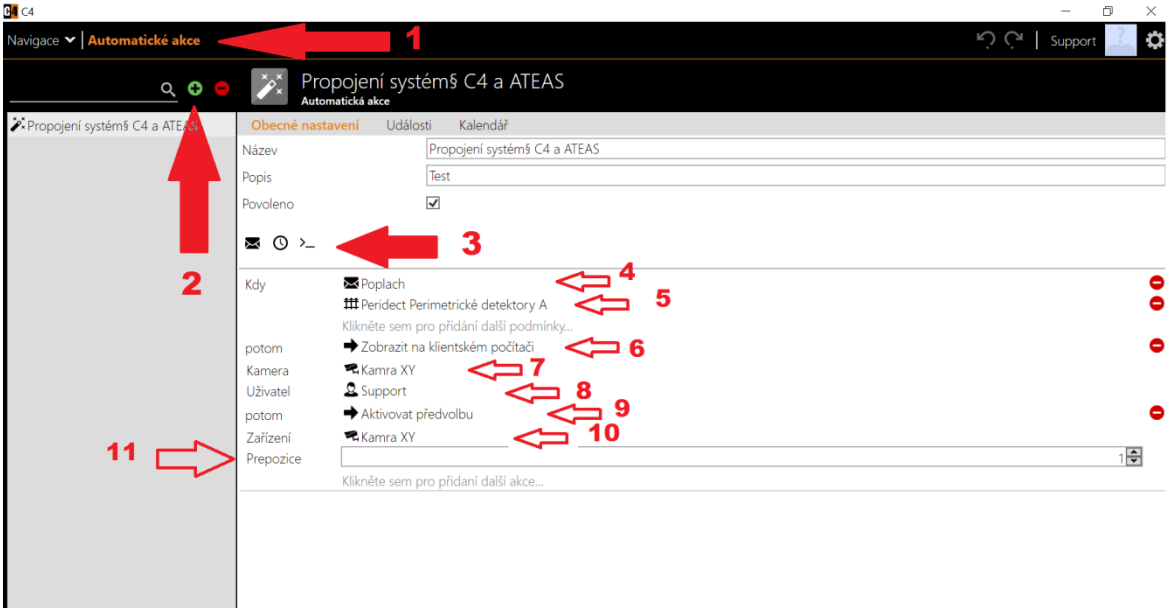
Po úspěšném zavedení systémů ATEAS a Peridect do systému C4 je možné tyto systémy propojit tak, aby bylo při narušení bezpečnostního oplocení bylo inkriminované místo automaticky zabráno kamerou k prověření poplachu.

Tento způsob propojení je možno nadefinovat v menu *Automatické akce,* které slouží k definování logických vazeb mezi jednotlivými systémy a zařízeními spravovanými v systému C4.

1. V menu *Navigace* je třeba zvolit položku *Automatické akce.*
2. V okně *Automatické akce* je nutné kliknout na zelené plus čímž je vytvořena nová automatická akce. Dále je pak potřeba, vyplnit název a případně popis akce.
3. V dalším kroku je nutné vytvořit podmínku na základě události přijaté v systému C4. Tuto podmínku lze zvolit ze seznamu po kliknutí na černou obálku s názvem *Přidat automatickou akci spuštěnou událostí* se otevře *C4 – Repozitáře.*
4. Ze *C4 – Repozitáře* v seznamu *Události* je nutné vybrat *Poplach.* Toto nastavení určí, jakým způsobem bude s případnou událostí.
5. V dalším bodě se zvolí, které detektory nebo Multisenzory budou spouštět poplach. Pod položkou poplach se nachází další pole s označením *Klikněte sem pro přidání další podmínky.* Po klinutí do tohoto pole se znovu otevře *C4 – Repozitáře* tento-

krát je třeba v seznamu *Zařízení* je zvolit, který detektor po případě Multidetektor bude spouštět poplach.

6. Dalším krokem je určit, jakým způsobem bude pracováno s případným poplachem, zda bude zobrazen na klientském počítači, odeslán pomocí SMS a nebo jinak zpracován. V modelovém případě je zvoleno *Zobrazit na klientském počítači.* Toto nastavení je v *C4 – Repozitáře* v seznamu *Akce.*
7. Dále je možno přidat kameru opět z *C4 Repozitáře, která je v seznamu Zařízení* řazena pod systémem ATEAS.
8. Nyní je třeba zvolit uživatele, kterému bude tato informace o poplachu předána. Výběr je proveden opět z *C4 – Repozitáře* a seznamu *Osob.*
9. Nyní je potřeba nastavit otočení kamery do místa poplachu. Nastavení tohoto je pomocí *Akce Aktivovat předvolbu.*
10. V položce *Zařízení* je třeba opět zvolit kameru, která má reagovat na poplach.
11. Posledním krokem nastavení je zadání čísla *Prepozice.* Zde je třeba zadat číslo presetu nastaveného v systému ATEAS.



Obrázek 49. Propojení systému Peridect se systémem ATEAS v systému C4 při ochraně perimetru.

Systém C4 umožňuje vytvářet automatické akce pomocí skriptů. Díky tomuto je možné rychle vytvářet, kopírovat a upravovat jednotlivé automatické akce. Výhodou skriptů je možnost tvorby složitějších nastavení, než je možno tvořit v běžném menu. Skripty je možné tvořit a upravovat pomocí tlačítka **>_.**

```
WHEN ( EVENT IS Alarm )
AND ( DEVICE IS '51be07de-ebe2-44fa-95b9-813051fab099' )
ACTION ShowLiveStreamOnUser
{
    Camera = '1d4d0712-4162-4976-9ead-55a80d4cab7e',
    User = '8361eb78-d08e-435f-9065-bf2aeac85816'
}
ACTION ActivatePreset
{
    Device = '1d4d0712-4162-4976-9ead-55a80d4cab7e',
    Preset = 1
}
```

Obrázek 50. Pomocí skriptu propojení systémů C4 a ATEAS.

7.4 Dílčí závěr

Závěrečná kapitola popisuje integraci bezpečnostních systémů ATEAS a Peridect v integračním systému C4.Tato integrace byla prováděna pro potřeby velké výrobní společnosti, která tyto systém používá pro ochranu perimetru. Správnost nastavení byla ověřována u společnosti Gamanet výrobce systému C4. Při vlastní integraci byl objeven problém ve spojení mezi systémy C4 a Ateas u dome IP kamery AXIS Q6114 E. Tyto systémy by podle jejich výrobců měly být schopny spolupráce na vyžadované úrovni což se při reálném testování nepodařilo ověřit. Tento problém byl nahlášen společnosti Gamanet, která ve spolupráci s firmou ATEAS pracuje na jeho odstranění.

ZÁVĚR

Cílem této diplomové práce bylo zabývat se systémy ochrany perimetru a jejich vzájemnou integrací. V teoretické části se práce věnuje jednotlivým bezpečnostním systémů, které jsou v současné době používány pro ochranu perimetru. Teoretická část práce je zaměřena na integraci bezpečnostních systémů pro potřeby velké výrobní společnosti.

První tři kapitoly teoretické části jsou věnovány trendům v bezpečnostních systémech při ochraně perimetru. Výčet těchto systémů je zahájen popisem tradičních mechanických zábranných systémů, které slouží k zastavení pachatele a jeho zpomalení. Mechanické zábranné systémy se dále dělí na umělé oplocení, vstupy, vjezdy a doplňkové zábrany. Dalším představeným systémem ochrany perimetru je poplachový zabezpečovací a tísňový systém, jenž slouží k detekci pokusu o narušení perimetru a jeho lokaci. Pro detekci pachatele se nejběžněji používají: infračervené bariery, mikrovlnné bariery, plotové detekční prostředky, systémy se zemními detekčními prostředky, laserové detektory a venkovní PIR detektory. Posledním systémem ochrany perimetru představeným v rámci první kapitoly jsou kamerové systémy. V rámci kamerových systémů jsou popsány tři hlavní kategorie těchto systémů, a to starší analogové, novější IP kamery a hybridní kamerové systémy, které fungují na pomezí těchto systémů. Součástí této kapitoly je i popis norem, které se zabývají jednotlivými bezpečnostními systémy.

Teoretická část je zakončena čtvrtou kapitolou, jež je věnována integraci bezpečnostních systémů. Tato kapitola popisuje důvody pro zavedení bezpečnostní integrační platformy a způsob fungování integrovaného systému. I tato kapitola se odkazuje na normy, a to převážně na ČSN CLC/50398.

Pátá kapitola je první kapitolou praktické části. Kapitola detailněji seznamuje s ochranou perimetru ve velké výrobní společnosti. Jsou představeny jednotlivé systémy ochrany perimetru detekční systém Peridect, systém pro správu IP kamer ATEAS a integrační systém C4.

Šestá kapitola porovnává zabezpečení perimetru a jednotlivé systémy s dalšími systémy ochrany perimetru dostupnými na trhu. V této kapitole je představen systém AXIS Perimeter Defender fungující na principu pokročilé video analýzy v kombinaci s termálními kamerami. Dále je zde systém C4 porovnán s dalšími integračními platformami dostupnými na trhu. Těmito platformami jsou AlViS Alarm Visualization System a systém AS200.

Sedmá a poslední kapitola diplomové práce je věnována integraci systému Peridect se systémem ATEAS pomocí integrační platformy C4. Součástí této kapitoly je detailní popis zavedení a propojení těchto systémů. Při realizaci tohoto propojení pro potřeby velké výrobní společnosti byl objeven problém ve vzájemné komunikaci těchto systémů a z tohoto důvodu nemohlo být propojení realizováno. Na odstranění tohoto problému v současné době pracuje společnost Gamanet, která je výrobce systému C4. Po odstranění tohoto problému by již použité bezpečnostní systémy měly spolupracovat.

SEZNAM POUŽITÉ LITERATURY

[1] IVANKA, Ján, 2014. Mechanické zábranné systémy. Zlín. Univerzita Tomáše Bati ve Zlíně Fakulta aplikované informatiky.

[2] ČSN EN 1627 (74 6001) Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace: Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012. Česká technická norma.

[3] Norma průlomové odolnosti výplní stavebních otvorů a jejich uzávěrů. AD Security [online]. 2013 [cit. 2017-01-02]. Dostupné z: http://www.adsecurity.cz/katalog/index.php?static_TB=2

[4] KRATOCHVÍ, Jiří. MODERNÍ EVROPSKÝ STANDARD ZABEZPEČENÍ: Pokyny ke stanovení úrovně zabezpečení objektů a provozoven proti krádežím vloupáním podle evropských norem. Gorazdova 24, 128 01 Praha 2, Praha 2013: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ) v edici Sborníky technické harmonizace ÚNMZ., 2013.

[5] POPLASTOVANÉ PLETIVO 200 CM SE ZAPL. DRÁTEM. E-pletivo [online]. [cit. 2017-01-02]. Dostupné z: http://www.e-pletivo.cz/

[6] Ochrana osob a majetku [online]. 32 [cit. 2017-01-02]. Dostupné z: http://www.slu.cz/math/cz/knihovna/ucebni-texty/Ochrana-osob-a-majetku/Bezpecnostni-system-na-ochranu-majetku.pdf/view

[7] Kosedag. Perimeter protection: International Exhibition for Perimeter Protection, Fencing and Building Security [online]. [cit. 2017-01-03]. Dostupné z: https://www.perimeter-protection.de/de/ausstellerprodukte/pp16/aussteller-20263591/kosedag-fence

[8] Eploty.cz [online]. [cit. 2017-01-04]. Dostupné z: http://test.heras.cz/detail-kovove-mrizove-ploty-kovove-mrizove-ploty-mrizove-oploceni-plot-heracles.html?_ID=13122010134156&rozbaleno=

[9] STAVBA OPLOCENÍ: Žiletkový drát + pyramida [online]. Hradec Králové: p. Majer, 2011 [cit. 2017-01-11]. Dostupné z: http://stavbaoploceni.webnode.cz/products/ziletkovy-drat-pyramida/

[10] Atlas Fence: Exceeding Expectations… [online]. 6852 Manlius Center Road • East Syracuse, New York 13057: Atlas Fence, 2017 [cit. 2017-01-11]. Dostupné z: http://atlasfence.com/cgi-bin/htmlos.cgi/atlasfence/index.html

[11] Zaun: Zaun Limited – Metal Fencing Manufacturers [online]. United Kingdom, 2016 [cit. 2017-01-12]. Dostupné z: http://www.zaun.co.uk/sectors/high-security-fencing/

[12] BranyPosuvne.cz: Kovové branky [online]. [cit. 2017-01-12]. Dostupné z: http://branyposuvne.cz/katalog/kovove-branky

[13] Brany.net: posuvné brány a teleskopické vrata [online]. Horoměřice: Mantra & WordPress., 2016 [cit. 2017-01-12]. Dostupné z: http://brany.net/teleskopicka-brana/brany/otocne-kridlove-brany

[14] KB - BLOK systém, s.r.o: Dokonalý stavební systém [online]. Postoloprty, 2016 [cit. 2017-01-12]. Dostupné z: http://www.kb-blok.cz/srv/www/cs/detail/doplnky/K11/vrata-a-branky/K1105/28-atypweb03/vrata-posuvna-samonosna-atyp.x

[15] Almma [online]. Praha 10, 101 00: Xcreative s. r. o, 2016 [cit. 2017-01-12]. Dostupné z: http://www.almma.cz/produkty/

[16] Axel Tiede [online]. Düsseldorf - Abfahrt Erkelenz-Süd, 2016 [cit. 2017-01-12]. Dostupné z: http://www.axel-tiede.de/produkte-und-leistungen/drehkreuze/dk-3-motorisch.html

[17] ID-karta: Identifikační systémy [online]. Opava, 2017 [cit. 2017-01-12]. Dostupné z: http://www.id-karta.cz/images/products/image/tur-BAR.jpg

[18] Turnstar Systems [online]. Johannesburg, 2016 [cit. 2017-01-12]. Dostupné z: http://www.archiexpo.com/prod/turnstar-systems/product-64391-1091731.html

[19] Nové zastavovací pásy [online]. Praha, 2015 [cit. 2017-01-12]. Dostupné z: http://praha.idnes.cz/foto.aspx?r=praha-zpravy&c=A150403_124952_praha-zpravy_kol&foto=KOL5a51eb_DSC05796.jpg

[20] Alamy Stock Photos: Security Fence Spiked [online], 2016. [cit. 2017-01-12]. Dostupné z: http://www.alamy.com/stock-photo/security-fence-spiked.html

[21] Under fence barrier: shutterstock [online], 2016. Mexico border fence [cit. 2017-01-12]. Dostupné z: https://www.shutterstock.com/cs/pic-12230011/stock-photo-

end-of-us-mexico-border-fence-under-construction-in-arizona-desert-us-to-the-left-mexico-to-the-right.html?src=a44ejmsob8renfGi-zeEwA-3-10

[22] PZTS - Poplachový zabezpečovací a tísňový systém: Co je to poplachový zabezpečovací a tísňový systém? Security Guide [online]. 3[cit. 2017-01-12]. Dostupné z: https://www.securityguide.cz/security/viewArticle/pzts

[23] ČSN EN 50131-1 ED. 2. Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky. 2 vydání Nahrazuje dokumenty EN 50131-1. Praha 1: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2007.

[24] Cias: Protective barrier [online]. Miláno, 2016 [cit. 2017-01-15]. Dostupné z: http://www.cias.it/

[25] Technicontrol: Peripheral and Perimeter Protection [online]. OLHÃO: Technologia e inovacao, 2016 [cit. 2017-01-16]. Dostupné z: http://www.tecnicontrol.pt/en/wiki/item.html?id=53-peripheral-and-perimeter-protection

[26] Sorhea [online]. Vaulx-en-Velin France: Pierre Papier Pixel, 2015 [cit. 2017-01-22]. Dostupné z: http://www.sorhea.com/qui-sommes-nous/notre-metier/

[27] HALOUZKA, Kamil. Fyzická bezpečnost: Perimetrické zabezpečovací systémy. Brno, 2014. Projekt: Vzdělávání pro bezpečnostní systém státu. Univerzita obrany.

[28] IP kamerový systém vs. CCTV. Ipsecure.cz: Řešení IP kamerového zabezpečení [online]. Praha 4 - Michle, 2012 [cit. 2017-02-16]. Dostupné z: http://www.ipsecure.cz/clanky/rady-a-tipy/ip-kamerovy-system-vs-cctv/

[29] Ochrana perimetru: Co je to perimetrická ochrana? Proč ji využít? Securityguide [online]. 2016 [cit. 2017-02-16]. Dostupné z: https://www.securityguide.cz/security/viewArticle/ochrana-perimetru

[30] HD-SDI kamerové systémy. Escad Trade [online]. Praha 10: PERUS, 2016 [cit. 2017-02-20]. Dostupné z: http://www.escadtrade.cz/1-hd-sdi-kamerove-systemy.html

[31] SDI a ti druzí, aneb na čem frčí profíci. TVFREAK [online]. oXy Online, 2011 [cit. 2017-02-20]. Dostupné z: http://www.tvfreak.cz/sdi-a-ti-druzi-aneb-na-cem-frci-profici/4521-2

[32] HUDSON, John, 2016. UHD-SDI Standards Overview. SEMTECH. Semtech Corporation – Gennum Products Group.

[33] HD-TVI cameras: new technology for analog HD solution. Unifore [online]. Hong Kong, 2016 [cit. 2017-02-26]. Dostupné z: http://www.hkvstar.com/technology-news/hd-tvi-cameras-new-technology-for-analog-hd-solution.html

[34] What is HD-CVI? SecurityCameraKing [online]. Florida Boca Raton, FL 33432: SecurityCameraKing, 2016 [cit. 2017-02-26]. Dostupné z: https://www.securitycameraking.com/what-is-hd-cvi.html

[35] What is AHD CCTV. CCTV Camera Pros [online]. Florida USA, 2016 [cit. 2017-02-27]. Dostupné z: http://videos.cctvcamerapros.com/surveillance-systems/what-is-ahd-cctv.html

[36] ONVIF [online]. San Ramon, CA 94583: Stan Moyer, 2016 [cit. 2017-02-28]. Dostupné z: https://www.onvif.org/contact/

[37] NILSSON, Fredrik. Intelligent network video: understanding modern video surveillance systems. Boca Raton: CRC Press, c2009. ISBN 14-200-6156-9.

[38] Jak instalovat kamerový systém (IP). Nejkam [online]. Benešov u Prahy, 2016 [cit. 2017-03-02]. Dostupné z: https://www.nejkam.cz/jak-instalovat-kamerovy-system-ip/

[39] IP kamerové systémy. ESCAD trade [online]. Praha 10: Perus, 2009 [cit. 2017-03-06]. Dostupné z: http://www.escadtrade.cz/webove-ip-kamery.html

[40] Komprimační formáty a přenosová rychlost. STASANET.cz: bezpečnostní technologie [online]. Praha 9: oXy [cit. 2017-03-08]. Dostupné z: https://www.stasanet.cz/Komprimacni-formaty-a-prenosova-rychlost/

[41] Úřad pro technickou normalizaci, metrologii a státní zkušebnictví [online]. Praha 1, 1993 [cit. 2017-03-08]. Dostupné z: http://www.unmz.cz

[42] ČSN EN 62676-1-1. Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-2: Systémové požadavky - Výkonové požadavky na video přenos. 1. Praha: ÚNMZ, 2014.

[43] ČSN EN 62676-1-2. Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-2: Systémové požadavky - Výkonové požadavky na video přenos. 1. Praha: ÚNMZ, 2014.

[44] ČSN EN 62676-2-2. Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 2-2: Video přenosové protokoly - Implementace vzájemné spolupráce IP systémů založených na využití HTTP a REST. 1. Brusel: Cenelec, 2014.

[45] ČSN EN 62676-2-3. Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 2-3: Video přenosové protokoly - Implementace vzájemné spolupráce IP systémů založené na síťových (web) službách. 1. Brusel: Cenelec, 2014.

[46] Zajištění zvýšení bezpečnosti na letišti Václava Havla Praha. In: Úřad vlády České republiky [online]. Praha [cit. 2017-03-13]. Dostupné z: https://www.vlada.cz/assets/urad-vlady/poskytovani-informaci/poskytnute-informace-na-zadost/Priloha_6_Material_2.pdf

[47] Monitorovací a řídicí systémy – integrační platforma IPS (1. část) Zdroj: http://elektro.tzb-info.cz/poplachove-a-zabezpecovaci-systemy/14144-monitorovaci-a-ridici-systemy-integracni-platforma-ips-1-cast#english_synopsis. TZB-info [online]. Praha: Topinfo s.r.o, 2016 [cit. 2017-03-13]. Dostupné z: http://elektro.tzb-info.cz/poplachove-a-zabezpecovaci-systemy/14144-monitorovaci-a-ridici-systemy-integracni-platforma-ips-1-cast#english_synopsis

[48] ČSN CLC/TS 50398. Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky. 1. Praha: UNMZ, 2009.

[49] Sieza [online]. Praha, 2017 [cit. 2017-03-23]. Dostupné z: http://sieza.com/

[50] Ateas [online]. Praha: ATEAS CZ, 2017 [cit. 2017-03-27]. Dostupné z: http://www.ateas.net/en/

[51] AXIS Q6114-E PTZ Network Camera. AXIS [online]. Švédsko, Lund: Axis Communications [cit. 2017-03-27]. Dostupné z: https://www.axis.com/cz/cs/products/axis-q6114-e/

[52] HIKVISION [online]. Čína, 2016 [cit. 2017-03-27]. Dostupné z: http://www.hikvision.com/en/index.html?jmode=j1&country=Czech%20Republic

[53] Dirickx: Bezpečnostní systémy pro ochranu vašeho objektu [online]. Brno, 2016 [cit. 2017-04-26]. Dostupné z: http://www.dirickx.cz/bezpecnostni-systemy

[54] AXIS Perimeter Defender: High-security, scalable perimeter protection [online]. [cit. 2017-05-03]. Dostupné z: https://www.axis.com/cz/cs/products/axis-perimeter-defender/how-it-works

[55] C4:Čo je C4 [online]. Bratislava [cit. 2017-05-06]. Dostupné z: https://www.c4portal.com/Home.aspx

[56] AlViS: Alarm Visualization System [online]. Bratislava [cit. 2017-05-06]. Dostupné z: http://www.alvis.sk/index.php

[57] A2D s.r.o.: nadstavbové systémy EPS/EZS [online]. Liberec, 2017 [cit. 2017-05-08]. Dostupné z: http://www.a2d.cz/web/cze/AS200.php

[58] WU, Kaicheng, J.W. GU, X.L. CHEN a E.H. LIU. Research of Video Steganalysis Algorithm Based on H265 Protocol. MATEC Web of Conferences. 2015, 25, 03003-. DOI: 10.1051/matecconf/20152503003. ISSN 2261-236x. Dostupné také z: http://www.matec-conferences.org/10.1051/matecconf/20152503003

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACAP	Axis Camera Application Platform.
AHD	Analog High Definition
BIP	Bezpečnostní integrační platforma
BNC	Bayonet Neill Concelman
CCF	Central Control Facility
CCTV	Closed Circuit Television
CVI	Composite Video Interface
DPH	Daň z přidané hodnoty
DVR	Digital Video Recorder
EKV	Elektronická kontrola vstupů
FTS	Flexible Steel Topping
HD	High Definition
HEVC	High Efficiency Video Coding
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IPS	Integrovaný poplachový systém
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
M-JPEG	Motion Joint Photographic Experts Group
MPEG-4	Moving Picture Expert Group
MZS	Mechanické zábranné systémy
NTSC	National Television System(s) Committee

ONVIF	Open Network Video Interface Forum
OPC	Open Platform Communications
PAL	Phase Alternating Line
PIR	Pasiv Infra Red
POE	Power over Ethernet
PSIA	Physical Security Interoperability Alliance
PZTS	Poplachový zabezpečovací a tísňový systém
SDI	Serial Digital Interface
SMPTE	Society of Motion Picture and Television Engineers
STP	Shielded Twisted Pair
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TVI	Transport Video Interface
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VDS	Video Dohledový Systém
VGA	Video Graphics Array
VSS	Video Surveillance System
XML	eXtensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK