Radarové systémy perimetrické ochrany

Tomáš Kutil

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tomáš Kutil**
Osobní číslo:	**A18352**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Radarové systémy perimetrické ochrany**
Téma práce anglicky:	**Radar Perimeter Protection Systems**

Zásady pro vypracování

1. Popište aktuálně používané systémy perimetrické ochrany objektů.
2. Vysvětlete použití inteligentních systémů pro zabezpečení perimetru.
3. Vypracujte rešerši současných radarových technologií pro zabezpečení perimetru.
4. Zpracujte standardy a legislativní požadavky na perimetrické systémy.
5. Porovnejte funkce a vlastnosti nejnovějších radarových technologií.
6. Navrhněte modelové situace, při kterých budou zřejmé výhody a nevýhody použití jednotlivých technologií v rámci stupně zabezpečení objektu.
7. Proveďte cenové ohodnocení jednotlivých systémů.
8. Odhadněte další vývoj těchto systémů.

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

Seznam doporučené literatury:

1. LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management I. Zlín: VeRBuM, 2011. ISBN 978-80-87500-05
2. LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management II. Zlín: VeRBuM, 2012. ISBN 978-80-87500-19-4
3. LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management III. Zlín: VeRBuM, 2013. ISBN 978-80-87500-35-4
4. VALOUCH, Jan. Projektování integrovaných systémů. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2015, 1 online zdroj (169 s.). ISBN 978–80–7454–557-3
5. VALOUCH, Jan. Projektování integrovaných systémů. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj (152 s.). ISBN 978-80-7454-296-1
6. HAMISH D.MEIKLE. Modern radar systems. Artech House Publischers. ISBN – 978-1596932425
7. LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management IV. Zlín: VeRBuM, 2014. ISBN 978-80-87500-57-6.

Vedoucí bakalářské práce: **Ing. Rudolf Drga, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **15. ledna 2021**
Termín odevzdání bakalářské práce: **19. května 2021**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

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

Ve Zlíně dne 15. ledna 2021

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

Tomáš Kutil. r.v.
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá perimetrickou ochranou a analýzou nejpoužívanějších systémů perimetrické ochrany pro různé stupně zabezpečení. V teoretické části práce se bude zabývat vysvětlením radarových technologií a systémem MDS (systém pro detekci pohybu). V praktické části se budu zabývat porovnáním nejnovějších systémů, jejich vlastností a zpracováním modelových situací, při kterých budou zřejmé výhody a nevýhody použití jednotlivých technologií. Závěrem se práce bude věnovat využití systému Lidar (laserový radar) pro ochranu okolí objektu.

Klíčová slova: Perimetrická ochrana, radarové systémy, Lidar

ABSTRACT

The bachelor thesis deals with perimeter protection and analysis of the most used systems of perimeter protection for various levels of security. The theoretical part of the task explains radar technologies and the Motion Detection System (MDS). The practical part of the thesis deals with the comparison of the latest systems, their properties, and processing of model situations which demonstrate obvious advantages and disadvantages of these individual technologies. Finally, the thesis focuses on the use of the Lidar system (laser radar system) to protect the surrounding area of the building.

Key words: perimeter protection, radar system, Lidar

V úvodu této bakalářské práce bych chtěl poděkovat svému vedoucímu Ing. Rudolf Drga, Ph.D. za odborné vedení, cenné rady a připomínky, které mi poskytoval během jejího zpracovávání. Dále chci poděkovat svým blízkým a rodině za podporu, které se mi dostávalo během mého studia.

OBSAH

ÚVOD

V dnešní době je neustále náročnější zajistit ochranu sebe, své rodiny i majetku, a to vzhledem k stále rostoucí kriminalitě. Proto se stále rozrůstá bezpečnostní trh, který se snaží stíhat důmyslnost pachatelů, předvídat jejich pokusy o vniknutí do nejrůznějších objektu a předejít jim. Jednou z opomíjených bezpečnostních prvků je ochrana perimetru. Toto téma jsem si vybral, abych prohloubil svoje znalosti moderních technologií právě pro ochranu perimetru. Perimetrická ochrana se dá definovat jako venkovní obvodová ochrana. Účelem tohoto způsobu ochrany je zajištění detekce vniknutí do střeženého prostoru nepovolanou osobou, následně ji v tomto prostoru sledovat, a to využitím aplikace technických, elektronických a kombinovaných elektronicky-mechanických systémů. Prvky perimetrické ochrany z důvodu nezbytnosti vysoké odolnosti proti klimatických podmínkám a vůči falešným poplachům nemají malou pořizovací cenu.

V 21. století kdy každý má svůj chytrý telefon, se i tyto vyspělé systémy dostaly do samotné perimetrické ochrany a to při využití ochrany pomocí radarových systémů. Tyto systémy využívají technologie digitálního formování paprsku a algoritmu inteligentní analýzy k určení místa výskytu a rychlosti potenciálního vetřelce.

V mé bakalářské práci se chci zaměřit na základní prvky perimetrické ochrany a poté rozvinout využití radarových systémů ve specifickém prostředí jako jsou budovy s vysokými riziky, například elektrárny, letiště anebo vojenské budovy.

V předposlední části se budu zabývat analýzou jednotlivých nejpoužívanějších systémů. Poslední kapitola bude zaměřena na ukázku nejnovějších trendů v oblasti technologie radarových systémů.

I. TEORETICKÁ ČÁST

1 PERIMETRICKÁ OCHRANA

Prvním úkolem v nastavení perimetrické ochrany musí být vyznačení samotného perimetru. Jedná se o specificky danou hranici, která je vždy vymezena bud plotem, hradbou, nebo jakoukoliv přírodní překážkou. Cílem perimetrické ochrany je zajistit ochranu dané oblasti, tedy objektu mezi hranicí a ním. Perimetrická ochrana nezapomíná ani na ochranu vstupu do hlídané oblasti. Využití perimetrické ochrany v rámci zabezpečení běžných objektů, jako jsou například rodinné domy, malé soukromé firmy, nebo zahrady se nevyplatí, a to z důvodu vyšších pořizovacích nákladů. Systémy ochrany perimetru se nejčastěji využívají u budov s vysokými riziky. Mezi tyto budovy patří například velmi rozšířené fotovoltaické elektrárny, různé vojenské budovy, letiště, elektrárny, či různé strategické budovy.

1.1 Vlastnosti perimetrické ochrany

Základem perimetrické ochrany je zajistit vnější ochranu objektu od určité hranice. Touto pomyslnou čarou je nejčastěji plot či zeď. Nutno také zajistit prostor mezi objektem a touto předem určenou hranicí, proto je u těchto systému potřeba spojit perimetrickou ochranu s mechanickými zábrannými systémy a nejlépe i s fyzickou ostrahou. Díky tomuto spojení můžeme říci, že perimetrická ochrana má tři základní vlastnosti a těmi jsou: odstrašení, odhalení a potřebné zpoždění pro zadržení narušitele pomocí fyzické ostrahy.

1.2 Rozdělení prvků perimetrické ochrany

Rozdělení prvků pro perimetrickou ochranu je podle jejich různých vlastností, nejčastěji dělíme detektory podle fyzikálního principu činnosti, vytvoříme tak tří základní skupiny:

Elektromechanické, elektromagnetické a elektroakustické prvky. Další možný způsob rozdělení je podle vyzařování signálu, a to na pasivní a aktivní systémy.

1.2.1 Elektromechanické detektory

Tento princip je jeden z nejstarších, ale také nejspolehlivějších. Spočívá v reakci detektorů fyzikální změnu. Touto změnou může být například sepnutí či rozepnutí, změny odporu, změny kapacity elektrického obvodu, přerušení samotného obvodu.
Do této skupiny patří:

- Tenzometrické detektory
- Optovláknové detektory
- Zemní diferenciální tlakové hadice

1.2.2 Elektromagnetické detektory

Využívají pro vyhodnocení narušení objektu změny v elektromagnetickém poli, které způsobí pachatel. Principem je přerušení paprsku, případně změna vyzařování.

Do této skupiny patří:

- Infračervené bariéry/závory
- Štěrbinové kabely
- Mikrovlnné bariéry

1.2.3 Elektroakustické detektory

Principem elektroakustických detektorů je změna akustické tlakové vlny, která se šíří na povrchu materiálu a případně v jeho okolí.

Do této skupiny patří:

- Mikrofonický kabel
- Geofony – zemní mikrofony

1.2.4 Pasivní detektory

Pasivní detektor využívá především fyzikálních změn, které nastanou při pohybu pachatele v detekčním prostoru. Nevyužívá žádné vyzařování energie potřebné pro účel detekce ve střeženém prostoru, jako je to u aktivních systémů. Velkou výhodou je tudíž nemožnost detekce systému pachatelem a nízká spotřeba elektrické energie.
Do této skupiny patří:

- Pasivní infračervené detektory
- Mikrofonní kabely
- Diferenciální tlakové detektory
- Vibrační detektory
- Plotové tenzometrická čidla
- Seismická čidla

- Vláknově optické systémy
- Systémy hlídání drátěnou osnovou

1.2.5 Aktivní detektory

Aktivní detektory využívají principu vyzařování elektromagnetického či akustického signálu do detekované oblasti. Díky tomuto vyzařování signálu reagují pak na fyzikální změny, které se uskuteční při narušení.

Do této skupiny patří:

- Infračervené závory a bariéry
- Štěrbinové kabely
- Mikrovlnný detektor
- Laserové závory
- Kombinované detektory a bariéry
- Kapacitní čidla

2 SYSTÉMY PERIMETRICKÉ OCHRANY

V této kapitole se zaměřím na ukázku jednotlivých, aktuálně používaných systémů perimetrické ochrany. Jedním z nedostatků venkovních systémů je náchylnost na falešné poplachy způsobené klimatickými změnami. Dalším velkým nebezpečím těchto systému je například pohyb listí, odloženého smetí, anebo pohyb různých částí stromu a keřů v blízkosti hlídaného prostoru. Také pohyb zvěře může spustit poplach. Proto je žádoucí tyto systémy doplnit dohledovým videosystémem neboli CCTV, a to z důvodu odhalení falešných poplachů způsobené vlivy venkovního prostředí.

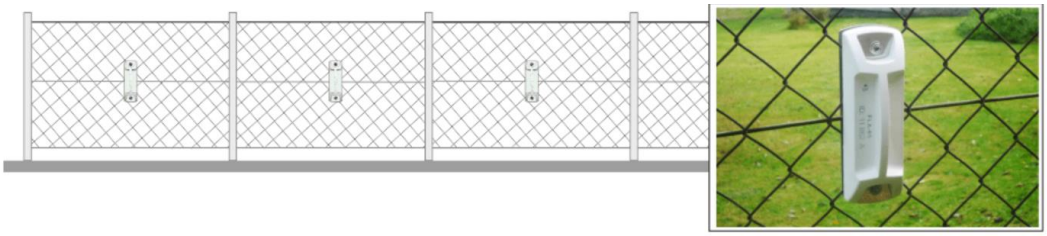
2.1 ELEKTROMECHANICKÉ DETEKTORY

2.1.1 Tenzometrické detektory

Tento typ detektoru se používá v takzvaném tenzometrickém plotovém systému. Systém využívá elektrický tenzometr v kombinaci s mechanickým zábranným systémem, například ostnatým či žiletkovým drátem. Princip detekce narušení perimetrického systému spočívá ve změně odporu, neboli samotný detektor vyhodnocuje tahovou diferenci. Tato změna diference může být důsledkem deformace, nebo přestřižení vrcholové ochrany, kterou způsobí pachatel. Při použití tohoto systému je kladen velký důraz na stabilitu dosavadního oplocení a vrcholové ochrany.

2.1.2 Vibrační detektory

Základem těchto systémů je pevné propojení detektoru s plotem. Detektor vyhodnocuje jakékoliv záchvěvy na plotě způsobené pokusem tento plot přelézt či vnitřní vyplň plotu přestříhnout. Tyto změny vyhodnocuje za pomoci akceleračního senzoru a elektronického gyroskopu. Výhodou je rozmístění jednotlivých vibračních detektorů na jednotlivá pole plotu pro přesnou lokaci narušitele. Tyto prvky pro ochranu perimetru se mohou používat na kovové, pletivové a plastové ploty a to vždy po jednotlivých úsecích maximálně do 150m. [1]



Obrázek 1 Vibrační detektor [1]

2.1.3 Optovláknové detektory

Tyto detektory vyhodnocují změnu mezi vysílačem světelného paprsku skrz zakopané optické vlákno a přijímačem. Změny, které zde mohou nastat, jsou při deformaci vlákna způsobeny jednotlivými otřesy a změnou tlaku. Pokud vyhodnocovací jednotka zaznamená změnu přijímaného paprsku oproti předchozímu, je následně zaznamenáno narušení perimetru.

2.1.4 Zemní diferenciální tlakové hadice

Zemní diferenciální tlakové hadice neboli hydraulické podzemní čidlo. Základem tohoto systému je použití dvou paralelně položených hadic napuštěných nemrznoucí kapalinou, a to ve vzdálenosti od sebe 1 až 2 metry. Tyto hadice kopírují terén a jsou uloženy pod povrchem země přibližně 25 až 35 cm do hloubky. Princip detekce narušitele spočívá v kompenzační metodě, která funguje na principu diferenciálního tlakového čidla. To slouží ke kontrole změn tlaku mezi jednotlivými hadicemi.

Obrázek 2 Zemní diferenciální tlakové hadice [2]

2.2 ELEKTROMAGNETICKÉ DETEKTORY

2.2.1 Infračervené závory/ zábrany

Infračervené závory slouží pro ochranu perimetru v místech, kde není problém s nerovností pozemku. Základem je vysílač a přijímač, mezi kterými probíhá infračervený paprsek. Pro minimalizaci falešných poplachů se používá více paprsků. Právě při přerušení více paprsků vstupem pachatele je vyhlášen poplach. Tyto systémy se vyrábějí v pulzních režimech s vnitřním vyhříváním, a to z důvodu nutnosti zamezit rosení jednotlivých přijímačů a vysílačů.

Obrázek 3 Infračervená závora [3]

2.2.2 Štěrbinové kabely

Základem štěrbinových kabelů je použití koaxiálního kabelu, tento kabel je vložen v páru pod povrch země. Jeden z této dvojice vytváří elektromagnetické vlnění, které indukuje okolo sebe elektromagnetické pole a druhý kabel vyhodnocuje změny, které nastanou v tomto elektromagnetickém poli. Při změně hodnot dojde k vyhlášení poplachu. Velkou výhodou těchto systémů je možnost kopírování terénů.

2.2.3 Mikrovlnný detektor

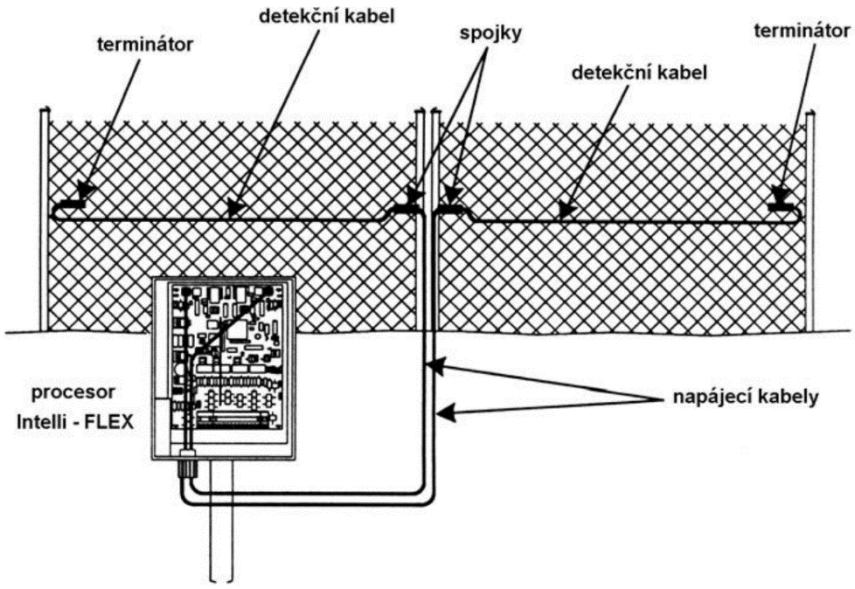
Mikrovlnné detektory fungují na principu Dopplerova jevu. Tento systém detekce je složen z vysílače, přijímače a vyhodnocovací elektroniky. Na jedné straně je generovaná vysílací frekvence a ta je následně zpracována. Pokud narušitel vstoupí do tohoto prostoru, je vyzařovací frekvence pozměněna a následně je vyhlášen poplach. Výhodou jsou minimální falešné poplachy způsobené povětrnostními podmínkami. Nevýhodou je krátké detekční pole.

Obrázek 4 Mikrovlnné bariéry [4]

2.3 ELEKTROAKUSTICKÉ DETEKTORY

2.3.1 Mikrofonní kabely

Principem mikrofonního kabelu je detekce mechanického namáhání mikrofonního kabelu. To může být způsobené jakýmkoliv otřesem, který způsobí například přelézání či stříhání plotu. Tyto záchvěvy se v mikrofonním kabelu převedou na elektrický signál, vyhodnocovací jednotka tento signál detekuje a vyhlásí případný poplach. Je nutné, aby tento kabel byl umístěn na pevný a kvalitní plot a byl s ním pevně spojen, a to z důvodu snížení počtu falešných poplachů.



Obrázek 5. Mikrofonní kabely [5]

Dílčí závěr

V této kapitole jsem specifikoval aktuálně používané systémy perimetrické ochrany objektů, jejich rozdělení podle fyzikálních vlastností a dále zda se jedná o pasivní či aktivní prvky. Podle pohledu na aktuální trh jsou nejčastěji využívané infračervené závory a mikrovlnné detektory. Tyto systémy jsou použity z důvodu cenové dostupnosti a absence potřeby terénních úprav hlídaného prostoru.

3 INTELIGENTNÍ SYSTÉMY

V této kapitole se budu zabývat inteligentními systémy pro zabezpečení perimetru. Tyto novodobé systémy můžeme využít jak pro ochranu celého perimetru, tak i pro ochranu jednotlivě určených vstupních popřípadě i výstupních bodů využitím *„elektronického systému kontroly vstupu (electronic assess control system) / systém kontroly vstupu (access control system), elektronického systému kontroly vstupu, poskytující oprávněným osobám nebo entitám, vstup do a/nebo opuštění zabezpečeného prostoru a zamítající vstup a/nebo odchod neoprávněným jedincům nebo entitám*.“ [6] Dále do inteligentní ochrany perimetru můžeme zařadit i jednotlivé bezpilotní prostředky.

3.1 Elektronické systémy kontroly vstupu

Elektronické systémy kontroly vstupu jsou vždy součástí režimové ochrany objektu. *„Režimová opatření stanoví oprávnění osob a dopravních prostředků pro vstup a vjezd do objektu.“* [7] Samotná kontrola vstupu a vjezdu do objektu spočívá v identifikaci uživatele/zaměstnance, a to pomocí jednotlivých čteček karet nebo RFID čipů. Bohužel takto prováděná identifikace osob při vstupu či vjezdu pro místa s vyššími požadavky na zabezpečení není dostatečná, a to z důvodu možnosti krádeže identifikačního zařízení. Proto se u těchto zařízení využívá modernější možnosti identifikace osob pomocí biometrických dat v kombinaci se základními prvky, jako jsou karty a čipy.

3.1.1 Identifikace pomocí karty

K identifikaci pomocí karty lze využít možnosti jak bezkontaktního tak i kontaktního snímání. V případě bezkontaktního systému stačí přiložit kartu do vzdálenosti několika centimetrů, v případě dražších systému i desítky centimetrů. Při přiblížení karty ke čtecímu zařízení dojde k načtení magnetického kódu na kartě a povolení vstupu. Pro identifikaci kontaktním způsobem musíme kartu zasunout do čtecího zařízení. V případě zvýšení bezpečnosti lze doplnit čtecí zařízení klávesnicí pro zadání PIN kódu, jako je tomu například u bankomatů. V tom případě proběhne dvojí identifikace pomocí karty a kódu. [8]

Obrázek 6 Identifikace pomocí karty [8]

3.1.2 Snímače biometrických dat

Důvodem využívání snímání biometrických rysů je jejich jedinečnost, i když se v dnešní době objevuje mnoho pokusů vytvořit odlitek prstu ze silikonu, či jiné variace obdobných pokusů. Je tu stále obrovská výhoda, že existuje mnoho možností jak bezpečnost zvýšit. *„Touto možností je například použití aplikace ezoterické identifikace, protože skryté znaky je mnohem obtížnější změnit, dokonce v některých případech i nemožné změnit."* [9]

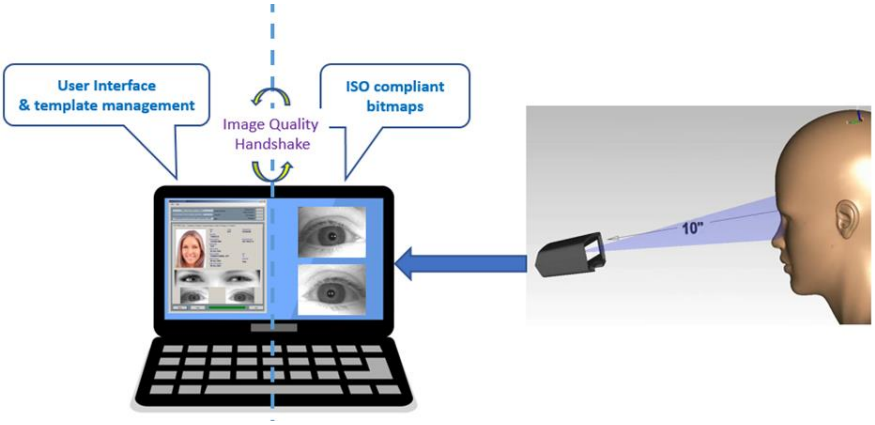
3.1.2.1 Snímání otisků prstů

V dnešní době jeden z nejznámějších a nejčastěji používaný systémů biometrického snímání dat. Je mnoho způsobů jak načíst data. Například jak je známo z chytrých telefonů, které používají pro kontrolu vstupu optický skener. Tento optický skener vychází z principu samotného skeneru, kdy se prst opticky naskenuje a dále se vytváří snímek. *„papilárních linií, který se následně zpracovává nebo kapacitní, kde je princip činnosti založen na využití rozdílu kapacit mezi deskou snímače a povrchem prstu."[10]*

Obrázek 7 Snímač otisků prstů [11]

3.1.2.2 Snímač oční duhovky

Snímače očních duhovek pro ochranu perimetru se téměř nepoužívají. Tyto systémy se převážně montují pro ochranu vnitřních vstupů do střežených místností. V dnešní době se můžeme setkat i s touto možností biometrické kontroly vstupu. Samotný sken oční duhovky je založen na naprosté unikátnosti oční duhovky. Oko, jako interní orgán, je prakticky nemožné duplikovat. A proto zabezpečení pomocí tohoto systému je velmi bezpečné.



Obrázek 8 Snímač oční duhovky [12]

Dílčí závěr

V této krátké části o chytrém zabezpečení vstupu jsem jen částečně naznačil tuto problematiku. K tomuto tématu se může ještě přidat snímač 3D geometrie obličeje, snímač krevního řečiště, detekce chůze a podobně.

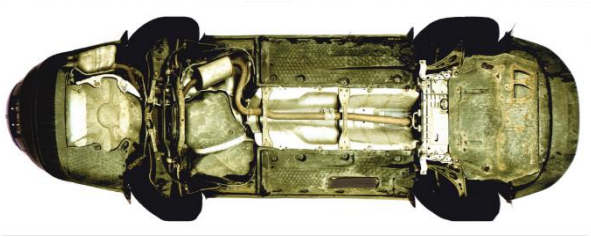
3.2 Chytrá identifikace automobilů a kontrola podvozků

Nedílnou součástí ochrany objektu je ochrana vjezdu do objektu. Jedná se o včasnou identifikace přijíždějících vozidel do objektu. Tuto problematickou úlohu nám zajišťují chytrá zařízení čtení registračních značek. Jedná se o specifikovaný software, který pomocí kamer přečte poznávací značku a zároveň dokáže rozeznat například typ a barvu auta. Tyto informace porovná v systému a vyhodnotí, zda vozidlo má oprávnění vjezdu do objektu.

Obrázek 9 Identifikace automobilů [13]

Další z novodobých systému pochází od společnosti Kerberos. Tato společnost vytvořila poloautomatické snímání podvozku projíždějícího vozidla přes retardér. Kerberos 2D vision poskytuje 2D model kontrolovaného podvozku vozidla, který ve chvíli naskenování začíná porovnávat s databází. Tento systém vytváří fotografie podvozku ve vysoké kvalitě, že dokáží rozpoznat i nepatrné změny. Systém lze využít, jak pro kontrolu vozidel, které přijíždějí či odjíždějí z hlídané oblastí, tak i pro kontrolu podvozku, kde předpokládáme, že by se mohl někdo skrývat, nebo by zde mohla být uložena jakákoliv potenciální hrozba. Samotné skenování a následná kontrola s databází a určování neshod s jinými 2D modely je natolik rychlá, že výrobce uvádí kontrolu až 10 vozidel za minutu. [13]

Obrázek 10 Skenování automobilu [14]



Obrázek 11 Naskenovaný podvozek automobilu [15]

3.3 Systém MDS

MDS neboli movement detection systém, v překladu systém pro detekci pohybu. Tento systém detekce pohybu se začal využívat především pro kontrolu přítomnosti osob či zvířat v zavazadlovém či jiném místě v automobilu, nákladním vozidle, nebo v jakémkoliv jiném dopravním prostředku. Tento inteligentní systém je založen na detekci pohybu skrytých osob uvnitř vozidla. Samotný systém se skládá z dvou částí, z řídící jednotky a detekčního senzoru, ty se připevní na kostru vozidla za pomoci magnetu. A dále se pomocí citlivých senzorů, měří jakékoli vibrace, kterou způsobí samotné tělo či osoba ve styku s nákladem nebo interiérem vozu. Řídící jednotka tuto vibraci vyhodnotí a následně informuje o přítomnosti osob uvnitř vozidla. „*Tato technologie je mnohem spolehlivější díky velmi citlivým senzorům než například měření koncentrací CO_2, nebo rentgenování nákladních prostor automobilů. Tyto metody jsou spolehlivé, ale bohužel se mnohdy dají obejít.*“[16] Velká výhoda je minimalizace falešně negativních kontrol z důvodu tak velké citlivosti, která dokáže rozpoznat i malé signály, jako například tlukot srdce. Další výhodou je velmi rychlá kontrola, která se pohybuje do dvou minut. Proto je tato technologie velmi využívaná pro stálou kontrolu vjezdu vozidel do objektu, jako jsou: přístavy, letiště, nápravná zařízení

a vojenská zařízení. Tato technologie je vytvořena rovněž pro mobilní stanoviště a využívá se v terén. Schopna během krátké doby začít prohlížet vozidla, která jsou podezřelá pro pašování osob například v oblastí hranic. [16]

Tento systém je i schopen detekovat pomocí zemního senzoru seizmické vibrace, které můžou způsobovat pohyby zemských desek, a díky tomu může varovat proti zemětřesení.

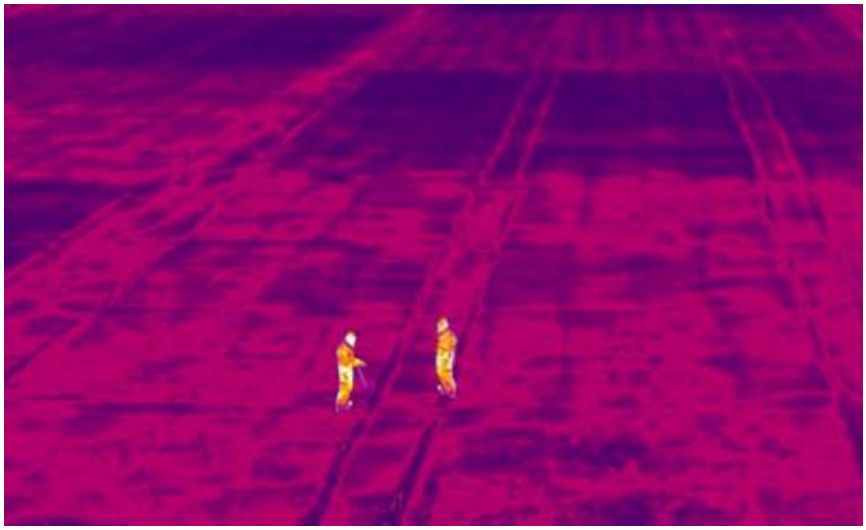
Obrázek 12 Systém MDS [16]

3.4 Kamerový systém

Kamerové systémy se nejčastěji používají v kombinaci s jednotlivými perimetrickými systémy. Díky speciálním systémům, které dokáží vyhodnocovat jakýkoliv pohyb ve snímané oblasti, je můžeme použít i samostatně. Další obrovskou výhodou je, že se nejedná o vyhodnocení jakéhokoliv pohybu, ale dokáži detekovat pohyb osob nebo překonání hradby. Samozřejmě samotné kamery nevyhodnocují, zda se jedná o pohyb nebo ne, to obstarávají jednotlivé specializované vyhodnocovací jednotky. Tyto systémy dokáží pracovat 24 hodin denně při použití infra přisvícení. Dalším vylepšení tohoto systému je použití termokamer.

- **Temokamery**

Termokamery fungují na principu termografie, což je zobrazovací metoda, která zviditelňuje infračervené spektrum. Jedná se o detekci jakéhokoliv tepla, které vyzařuje člověk či zvíře. Tyto systémy nepotřebují přísvit ani nic podobného. Vidí za jakéhokoliv počasí, a to díky rozeznání i nepatrného tepla.



Obrázek 13 Termokamery [17]

3.5 Bezpilotní systémy

Využitím bezpilotních zařízení se nám otevírají úplně nové možnosti zajištění bezpečnosti perimetru hlídané oblasti. Bezpilotní zařízení fungují na jednoduchém principu. Jedná se o velmi kvalitní prostředky, které využívají předem naprogramované monitorování oblasti, popřípadě jsou řízeny na dálku z operačního stanoviště. Díky různým pohybovým senzorům, termokamerám a jednotlivým technologickým nástavbám pro denní i noční průzkum dokáží odhalit osoby pohybující se v blízkosti hlídaného pásma.

3.5.1 MDARS

MDARS je produkt od společnosti General Dynamics Robotic Systems. Tato společnost se již dlouhou dobu zabývá výrobou bezpilotních vozidel. Obrovskou výhodou tohoto stroje je samostatné detekování překážek na cestě, následné vyhodnocení a vyhnutí se této překážce. Další unikátností je možnost detekování poškozené hradby, ohradníku, či plotu chráněného

objektu a tuto informaci předat okamžitě operátorovi. Tento typ vozidel se například využívá na ochranu jaderného testovacího komplexu v Nevadě. Pro využívání těchto zařízení ve velkých komplexech je přínosem možnost i ozbrojené verze, pričemž použití zbraní je stále na operačním stanovišti.[18]

Obrázek 14 Bezpilotní vozidlo MDARS [18]

3.5.2 GUARDIUM

Guardium je produkt společností G-NIUS.T Toto bezpilotní vozidlo bylo vyvinuto do hlídkové a ochranné práce pro nebezpečnou oblast v pásmu Gazy. V této oblasti hlídá hranice a blízké okolí, a to za pomoci velkého množství inteligentních technologií, jako jsou například infračervené kamery, různé typy senzorů, radary a dokonce detektory požáru přímo ve vozidle. [19]

Obrázek 15 Bezpilotní vozidlo Guardium [19]

Dílčí závěr

V této kapitole jsem specifikoval inteligentní systém používaný pro zabezpečení perimetrické ochrany. Jak na možnost ochrany pro vstup a vjezd do objektu, tak i ochrany samotného perimetru. Pro specifickou ochranu se používají bezpilotní letouny, ale jejich využijí, není primárně cíleno pro tento úkol.

4 RADAROVÉ SYSTÉMY

V této kapitole se zaměřím na radary z pohledu jejich principu a využitelnosti. Dále se budu věnovat jejich rozdělení podle funkce a použitelnosti v jednotlivých oborech.

4.1 Princip základních radarových systémů

Radar, převzatý výraz z anglického slova radio detecting and ranging, které se překládá jako radiové rozpoznávání a zaměřování. Již tento překlad vyjadřuje princip vzniku těchto systémů. Jejich základní vlastností bylo určování, detekování polohy nepřátelských jednotek, vyhledávání cílů a získávání mnoho dalších informacích o cílech.

Radar je elektronické zařízení, které spočívá v detekci cíle. Pro tento účel využívá výkonný vysílač, který generuje vysokofrekvenční oscilace. Radarová anténa vysílá pomocí pulzů. Anténa nejen vysílá, ale i přijímá jednotlivé signály, které se odrážejí od cílů. Díky její vysoké citlivosti dokáže přijmout jednotlivé ozvěny a poté je převést z vysokofrekvenčního signálu neboli echma na videosignál. Bohužel díky velkému množství novodobých systémů, které sami vyzařují jednotlivé vysokofrekvenční signály, je musí anténa oddělovat od těchto nežádoucích rušivých signálů. Mezi nejdůležitější prvky radarů patří generátor vysokofrekvenčních signálů a anténa, která vysílá a následně i přijímá vysokofrekvenční vlnění. Další velmi důležitou součástkou je přijímač, který zpracuje signál a přepošle jej na zobrazovací zařízení, nejčastěji monitor. Základem radaru je vyhodnocovací jednotka, která měří čas mezi vysláním, odrazem a zachycením odrazu. Na základě této hodnoty za pomoci Dopplerova jevu vypočítá vzdálenost jednotlivých objektů kolem sebe nebo v určeném směru. [20]

4.2 Rozdělení radaru podle jejich funkce

Radary rozdělujeme na aktivní, mezi které patří primární a sekundární a na pasivní.

- Primární typ radaru vysílá elektromagnetické vlnění, které letí až k cíli a od něj se odráží a vrací se zpět k anténě. Díky tomuto způsobu lze z výsledků odečíst například polohu a rychlost cíle atd. Velkou výhodou tohoto systému je že nevyžaduje komunikaci s cílem, ke kterému bylo vysláno vlnění. [20]
- Sekundární typ radaru vyžaduje oproti předchozímu způsobu, komunikaci s cílem, ke kterému bylo vlnění vysláno. Principem tohoto radaru je vyslání

vysokofrekvenčního elektromagnetického signálu. Tento signál dorazí k cíli a zařízení umístěné na palubě reaguje na vyslanou zprávu. *„Zařízení odpovídá pod svým kódem, který má přidělený“* [20] Danou odpověď zachytne anténa a následně jí dekóduje a zobrazí na zobrazovací jednotce. [20]

- Pasivní typ radaru, jedná se o pasivní radiolokátor, který nic nevysílá - jen se zaměřuje na sledování jakékoliv komunikace daného objektu. Nejčastěji se používá tento typ pro sledování letadel. Jedná se o sledování jakéhokoliv elektromagnetického rušení, toto rušení například může vydávat motor nebo jakákoliv elektronika v letadle. [21]

4.3 Využívání radarových systémů

Od doby 2. světové války se tyto systémy velmi rozmohly. V dnešní době se ve velkém množství používány pro navigaci a řízení leteckého či lodního provozu, vyhledávání cílů, mapování anebo v oblasti meteorologie. Mezi hlavní oblasti aplikace radarového systému patří:

- Letecká, vodní a pozemní doprava, pro tuto oblast se využívají jak pasivní tak aktivní typy radarů. Výhodou použití radarů je jednoduchá navigace a určování polohy i při zhoršeném počasí, nebo v noci.
- Využití radarů v dopravy, je také již velmi rozšířené. Nejčastěji se s tím setkáme při hlídání rychlosti, ale rovněž plynulosti dopravy. S touto možností se setkáme například u semaforu, kdy podle hustoty dopravy stojících aut na červené se řídí semafory.
- Jedna z dalších velmi často využívaných sfér je meteorologie. Zde se využívají radary pro zjišťování polohy mraků, které sebou mohou nést dešťové kapky či sněhové vločky.

Je mnoho dalších odvětví kde se používají radarové systémy. Jejich specifický princip nám může pomoct jak pro kosmický výzkum, v astronomii, tak i pro geodézii a kartografii a samozřejmě pro ochranu perimetru. [20]

5 RADAROVÉ SYSTÉMY PRO OCHRANU PERIMETRU

Využití bezpečnostních radarů pro ochranu perimetru se začalo využívat před několika lety. Výhodou využití těchto systému je jejich flexibilní použití v jakýkoliv podmínkách. Pro ochranu perimetru se může využívat mnoho specifických systémů, jak bylo zmíněno v předchozích kapitolách, ale většina z nich je náchylná na náročné povětrnostní podmínky, kopcovitost terénu anebo zalesněnost. Radary mají právě tu výhodu, že dokáží pracovat a to velmi spolehlivě i v těchto podmínkách. Velká část z nich dokonce využívá kombinaci detekce narušitele v rozsáhlé oblasti s připojenými kamerami nebo i termokamerami, které danou oblast začnou nahrávat pro snadnější identifikaci a potvrzení narušitele v oblasti.

5.1 Hikvonsion

Tato firma funguje na celosvětovém trhu již několik let. Mezi jejich produkty patří Security radar řady DS-PR*-**. Tato řada je primárně instalovaná do míst, jako jsou přístavy, různá skladiště, letiště a také i do továren. Pro snadnější specifikaci vlastností rozeberu radar typu DS-PRP100. Pomocí digitální technologie tvarování paprsku a algoritmu inteligentní analýzy dokáže tento typ ukázat přesnou polohu, směr, trasu pohybu a rychlost potenciálních narušitelů. Bezpečnostní radar DS-PRP 100 může nabídnout přesnou detekci v širokém úhlu 100° a do vzdálenosti 100m. Dokáže sledovat naráz až 32 různých cílů a svůj zorný uhel si dokáže rozdělit až do 16-ti zón, ve kterých detekuje. Další velkou výhodou je jeho komunikace s PTZ kamerou, při detekci narušitele konkrétní zóny informuje kamery a automaticky je zaměří na přesnou oblast pro tento účel. Dokáže propojit, detekovat a sledovat za pomoci kamer až 4 různé cíle. Má volitelné režimy, u kterých se může nastavovat různá citlivost. Samozřejmě se jedná o přístroj, který se nachází ve venkovním prostředí, tudíž musí mít velký teplotní rozsah, ve kterém může fungovat a jako základ se považuje i odolnost vůči vniknutí prachu a alarm proti neoprávněné manipulaci. [22]

Obrázek 16 Radar DS-PRP100 [22]

5.2 AVESTECH AG

Švýcarksá firma Avestech Tyto Solutions se věnuje ve velké míře zabezpečení perimetrické ochrany v kombinaci radarových systému s ostatními prvky a to nejčastěji s PTZ kamerami.

5.2.1 Zabezpečení obvodu

Výrobek Perimeter security je určen pro ochranu jakékoliv hranice či plotové linii. Je schopný detekce změny mezi dvěma pevnými body a to do vzdálenosti 500m. Díky využívání bezpečnostního radaru (a ne například infrazávor) se rapidně zvedá přesnost místa kde byl detekován narušitel a velmi snižuje míra falešných poplachů. Radarovým systémům nevadí jakákoliv změna počasí. Díky snadnému propojení s PTZ kamerami, je vždy při detekci narušitele automaticky zaměřena kamera na danou oblast. [23]

Obrázek 17 Koridorový radar [23]

5.2.2 Scan-360

V předchozím bodě jsem ukázal ochranu samotného obvodu, ale v dnešní době je již zapotřebí sledovat hrozby dřív než se k nám přiblíží. Proto společnost Avestech vytvořila Scan-360. Tento systém využívá 24GHz radarovou technologii k detekci a sledování cílů v definované oblasti. Skenovaná oblast se nachází v rozsahu do 200m na každou stranu a 360°. Při detekci v jeho vyznačeném pásmu začne ovládat CCTV kameru PTZ, pro jednoduší sledování i za pomoci obrazu narušitele a tyto informace předávána ARC. A pokračuje ve své dosavadní činnosti, skenování hlídané oblasti a detekování případného dalšího narušitele. Další velkou výhodou jsou programovatelné detekční zoný, v těchto zónách lze nastavit citlivost a například i dobu setrvání. Pokud například každou hodinu bude projíždět okolo pozemku hlídkový vůz a nebude se zde zastavovat, radar to vyhodnotí

a nevyhlásí poplach. Veškeré zpracování probíhá v rámci samotného zařízení a to dále komunikuje s okolím. [23]

Obrázek 18 Radar typu Scan-360 Upraveno[23]

5.2.3 Scan-Integrated

Scan-integrated je plně integrovaný produkt, který spojuje dvě důležité složky pro ochranu perimetru. Těmito složkami je obraz a scan. Jedná se o spojení radar scan-360 s kamerou 360Vision Technology Predator. Pokud se tato kombinace umístí na vysoko ležící bod, dokáže detekovat případného pachatele v oblasti a to v rozsahu 400m na každou stranu. Při detekci osoby nebo vozu, se kamera automaticky otočí a přiblíží se na danou oblast. Radar neustále skenuje a hledá případné další hrozby, zatímco kamera se soustředí přímo na hrozbu. V okamžik nalezení hrozby se vytváří videoklip, který se automaticky streamuje na ARC a případně externímu uživateli. Tento mechanizmus nemá žádné mrtvé úhly. [23]

Obrázek 19 Radar typu Scan-Integrated [23]

5.3 ReGUARD

RETIA je společnost, která vytvořila víceúčelový 3D radar s fázovou anténní řadou a to hned pro více režimů snímání - celokruhový režim anebo sektorový režim. Jedná se o velmi vyspělý typ radaru s možností detekování jak pozemních jednotek tak i vzdušných a to vše až na vzdálenost 18km - při šířce perimetru 22km v uhlu 56° (v nejvzdálenějším bodě až do výšky 3km).*„Jedná se výhradně o polovodičovou technologii zajišťující vysokou spolehlivost systému včetně redundance dílů. Díky monopulsnímu zpracování v azimutu i elevaci se jedná o velmi přesné vyhodnocení souřadnic. Velkou výhodou je pokročilé signálové a datové zpracování pro potlačení nezájmových objektů (včetně ptactva a automobilů)“* [24] Nepochybně se jedná o velmi důmyslný přístroj, který má velké přednosti v detekování všech cílů, které se dostanou do hlídaného perimetru a velkou vzdálenost a díky tomu umožnuje dostatek času na reakci. V případě potřeby ochrany rozsáhlého prostoru můžeme využít celokruhového režimu a zajistit tak bezpečnost za pomoci jen jednoho přístroje. Radar nám umožnuje více konfigurací kam umístit tento radar, lze ho využít pro přenosná, statická i mobilní místa. [24]

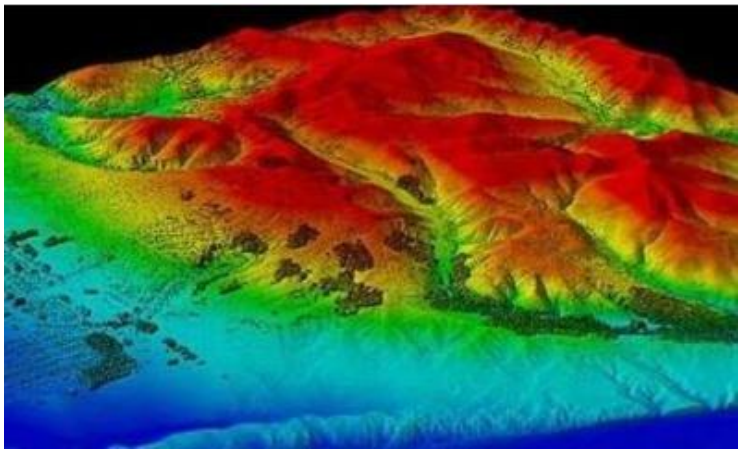
Obrázek 20 Radar ReGUARD [24]

6 LIDAR

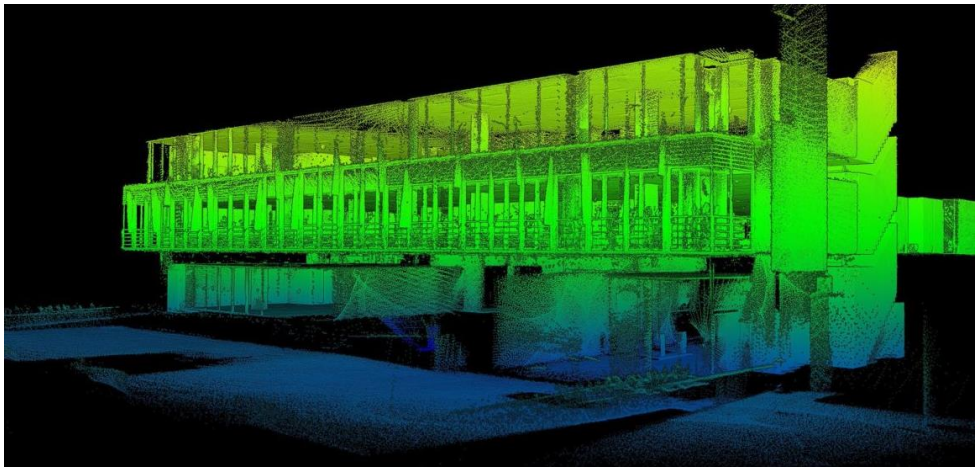
Pro některé je to novinka na trhu, ale pravda je opakem. Zmínky o tomto systému pocházejí již z roku 1963. Interpretace systému Lidar je převzata z „Light Detection And Ranging“ či „Laser Imaging, Detection And Ranging“ („laserové zobrazování, detekce a měření“). V dnešní době se ve skutečnosti se jedná o složeninu slov „**li**ght“ („světlo“) a „ra**dar**“. [25]

Základním principem této technologie oproti radaru, který používá pro detekci elektromagnetické vlnění - Lidar využívá světlo v jeho viditelném spektru a zároveň i infračervené či ultrafialové záření. Jedná se o stejný princip jako u radaru- jen rozdíl je, že nosičem v tomto případě je laser. „*Lidar je druh radaru pracujícího v optickém pásmu. Podobně jako v principu mikrovlnného radaru, používá elektromagnetickou vlnu v optickém kmitočtovém pásmu nejprve k přenosu detekčního signálu do cíle a poté porovnává přijímaný signál s vyslaným signálem, aby získal polohu (vzdálenost, azimut a výška), stav pohybu (rychlost, postoj) a další informace o cíli a realizují detekci, sledování a rozpoznání cíle.“*[26] Obrovskou výhodou Lidaru je jeho technologie s rozlišitelností překážek s přesností zhruba 3 cm na 100 m. Naopak nevýhodou je počasí. A to konkrétně déšť či sníh. Pokud laserový paprsek narazí na kapku vody, ta jej dokáže vychýlit. Ta se potom nemusí vrátit ve správném uhlu.

Lidar jak je všestranný laser, který se využívá v mnoha odvětvích. Mezi ně patří ALS (Airborne Laser Scanning) – letecké laserové skenování. Tento způsob se používá na skenování, mapování povrchu země, měření atmosférických jevů a to za pomoci jakéhokoliv létajícího prostředku. TLS (Terrestrial Laser Scanning) – pozemní laserové skenování. Skenování z určitého statického bodu. Skenování okolí, budov a podobně. V těchto případech se dá velmi snadno po zmapování terénu nebo budovy vytvořit 3D model.MLS (Mobile Laser Scanning) - mobilní laserové skenování. V dnešní době se tento způsobe stále rozšiřuje a jsou s ním vybavena velká část nových automobilu a jiných dopravních prostředků. Využívá se především na skenování oblasti před či za dopravním prostředkem. A jako další ho můžeme využít jako laserový lokátor. [26] [27]



Obrázek 21 Skenování povrchu pomocí laserového radaru [28]



Obrázek 22 Skenování budovy pomocí laserového radaru [29]

6.1 Laserový lokátor

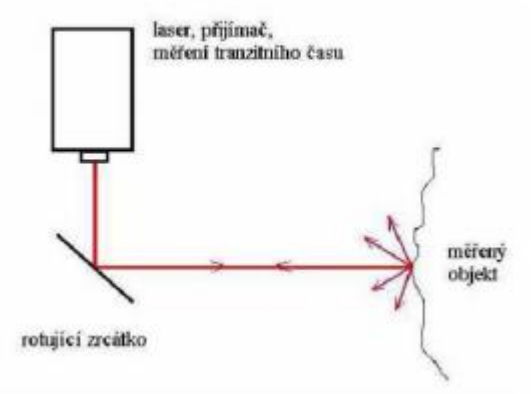
Laserový lokátor se používá pro přesné určení polohy objektu, a proto se dá využít i pro přesnou detekci narušitele v hlídaném prostoru. Systém funguje na neustálém skenování jeho okolí pomocí nejméně dvou rotujících laserových zaměřovačů. Ty neustále vysílají modulované paprsky a detekční jednotka poté vyhodnocuje paprsky, které se vrátí zpět. Tímto způsobem se vytvoří takzvaně 3D mapa okolí a při jakékoliv změně v této oblasti se tato nuance začne vyhodnocovat detekčním algoritmem. Pokud ten vyhodnotí, že se jedná o narušitele, pošle informaci na ARC a vyhlásí poplach. S touto informací předává přesnou polohu, rychlost a další parametry pro snadnější lokaci. Mezi přední výrobce těchto laserových lokátorů se řadí Hesai, Leica, Ouster, a Velodyne.

6.2 Metoda skenování

Je založena na vyslání paprsku k objektu, od jeho povrchu se odrazí a vrací se zpět. Tímto způsobem se naskenuje celá oblast a určí se přesná lokace jednotlivých překážek. [30]

6.2.1 Metoda time od flight (TOF)

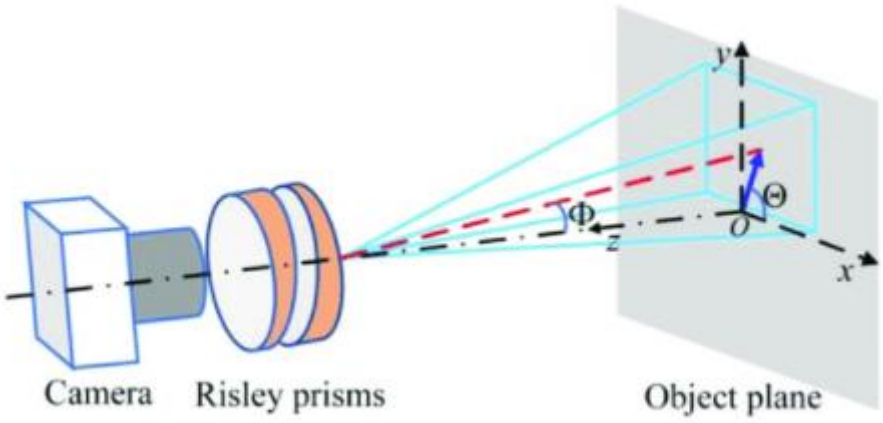
„Tato metoda spočívá v měření délek. Vysíláním laserového impulsu směrem na měřený objekt. Vzdálenost mezi vysílačem a povrchem objektu je spočítána z času, který uběhne mezi vysláním a přijetím signálu. Princip TOF je zobrazen na obrázku. Tato metoda je více vhodná pro skenování středních a větších délek a také objektů.“[31]



Obrázek 23 Metoda TOF [31]

6.2.2 Metoda Risley Prisms

Oproti metodě TOF - Risleyoúv způsob laserového skenování obsahuje dvojici klínových hranolů. Tyto hranoly složí k nepřetržitému průchodu a lomu optického paprsku za pomoci středně velké clony v širokém úhlovém rozsahu. Princip Risley Prisms je zobrazen na obrázku. Tato metoda zvyšuje rozlišení obrazu a to až na hranici optické difrakce optického systému pro zobrazovací systémy, jejichž rozlišení je omezeno velikostí pixelu. Jedná se o nástroj pro vysoce přenou detekci objektu. [32]



Obrázek 24 Metoda Risley Prisms [33]

6.3 Hesai

Firma Hesai se primárně zaměřuje na výrobu laserových radarů řady Pandar. Mezi jejich základní prvky patří PANDAR40P, tento výrobek pracuje s vlnovou délkou 905nm a jedná se o typ „spinning“, to znamená, že je to senzor se zrcadly co se otáčí o 360°. Horizontální zorné pole 360° s rozlišením 0,2° a vertikální zorným polem 40° s rozlišením 0,33° a to vše s maximálním dohledem 200m. Tento typ má také 40 různých laserových kanálů, tento parametr hovoří o množství paprsků, které skenují. To má vliv na různou rozpoznávací schopnost, zaměření a lepší rozlišování zpětného obrazu. [34]

Obrázek 25 PANDAR40P [34]

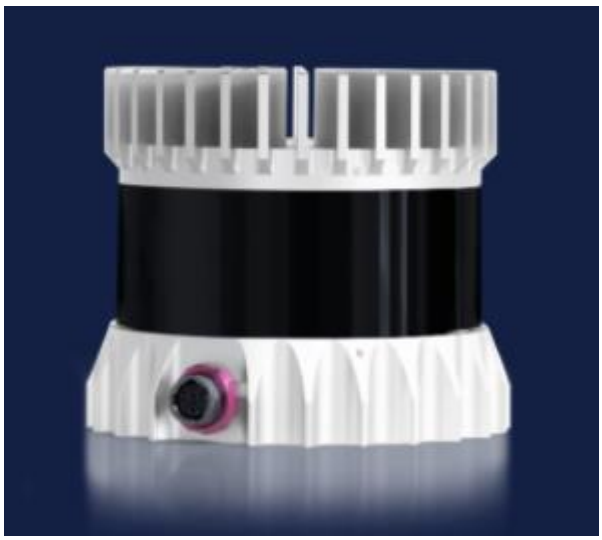
6.4 Leica

Firma Leica se zaměřila na nedostaky její konkurence a vytvořila výrobek označený BLK247. Ten má oproti předchozímu typu výhodu v jeho zorném poli. Zde se jedná o horizontální uhel zorného pole 360° a pro vertikální se jedná o 300°, bohužel zde ale byla rapidně snížena vzdálenost pro maximální dosah a to na pouhých 30m. BLK má kontinuální rozložení skenování paprsku a pracuje s vlnovou délkou 830nm. [34]

Obrázek 26 BLK247 [34]

6.5 Ouster

Společnost Ouster představila své výrobky řady OS1-**, u kterých se snažila zvýšit počet laserových kanálu. Například pro OS1-128 je to 128 kanálů, výrobek pracuje s vlnovou délkou 850nm. Jedná se o typ „spinning“, s horizontálním zorným polem 360° a s rozlišením 0,18°, vertikální zorné pole 45° rozlišení 0,35 a vše do maximálního dosahu 120m. [34]



Obrázek 27 OS1-128 [34]

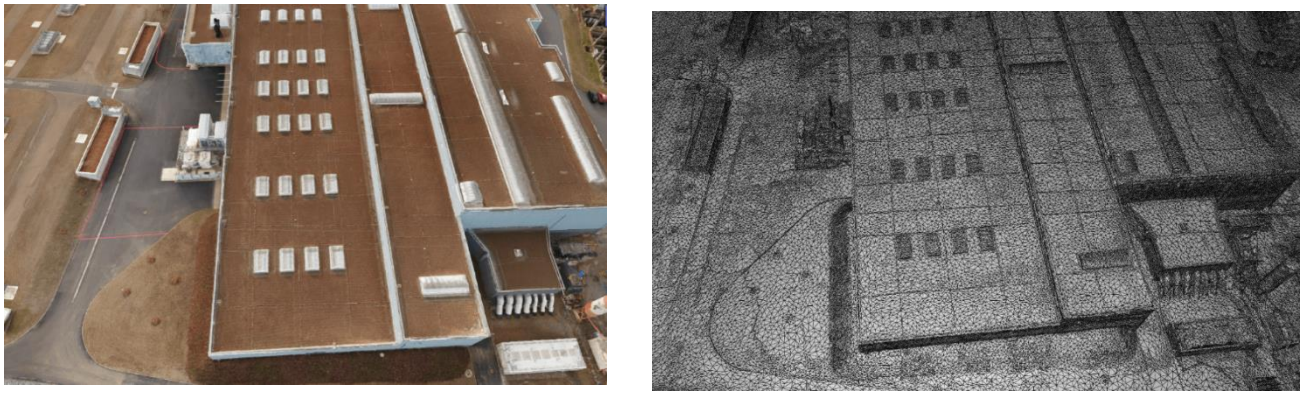
7 POMOCNÉ SOFTWARY

7.1 ACCUR8VISION

Již jsem představil mnoho systémů, které dokážou detekovat narušitele - jak v obvodu hlídané oblasti, tak i uvnitř. Některé systémy dokážou i říct v jaké zóně se daná osoba nachází a nasměrovat kameru pro vizualizaci místa. Základ software accur8vision spočívá ve 3D modelování objektu.. Výhodou je především pro operátory, kteří budou danou oblast střežit, a to z důvodu možnosti přesného identifikování místa, kde došlo k narušení a následného přesného sledování pohybu narušitele v reálném prostředí. Nejprve je zapotřebí vytvořit 3D mapování. S tímto nám pomůže například dron, který danou oblast naskenuje, a poté použijeme technologie fotogrammetrie. Tato technologie spočívá v rekonstrukci jednotlivých tvarů, měření velikostí a zaměřování přesné polohy zachycené na fotografii pořízené dronem. Díky těmto technologií máme vytvořený 3D model s reálnými prvky a překážkami.

A8V systém umí vytvořit různé zóny a těmito úseky vymezit různou členitost hlídané oblasti. Například vstupní cestu může úplně vynechat z hlídání a u zadního vchodu nastavit zpožďovací zónu. Také lze nastavovat u hlídaných zón i čas. Například přes den nechat hlídání jen zahrady a v noci hlídání celého perimetru. Pro jednotlivé zóny lze také nastavit různou citlivost na vnější falešné poplachy, kterými může být například hranice pozemku, za kterou se pohybují ve velké frekvenci automobily, které vytvářejí častou změnu v detekované oblasti. Falešné poplachy mohou vytvářet i malá zvířátka, proto lze u tohoto systému nastavit detekování objektu o různé velikosti a eliminovat tyto falešné poplachy. Případný narušitel vstupující do sledované zóny je díky fixnímu laserovému radiolokátoru identifikován. Díky identifikaci narušitele v hlídané oblasti je tato skutečnost přenesena na ARC. Operátor zaznamená poplachovou událost a díky 3D modelu nyní vidí přesnou polohu, pohyb a trajektorii vstupujícího objektu. Díky velmi chytrým programátorům a vývojářům tohoto prostředí, systém umožňuje dělat testy ve virtuálním prostředí. [34]*,, Díky tomu je možné procházet mapu pomocí virtuálního vetřelce, který simuluje skutečný pohyb vetřelců a tím ověřuje přesnost nastavení systému"*[34]

Samozřejmě se tyto prvky mohou i kombinovat s různými typy kamer. Toto vytvoření 3D modelu lze využít i pro vložení jednotlivých bezpečnostních prvků a to jak pro vyzkoušení jejich vhodného umístění, tak i ukázky zajištění/pokrytí celé oblasti.

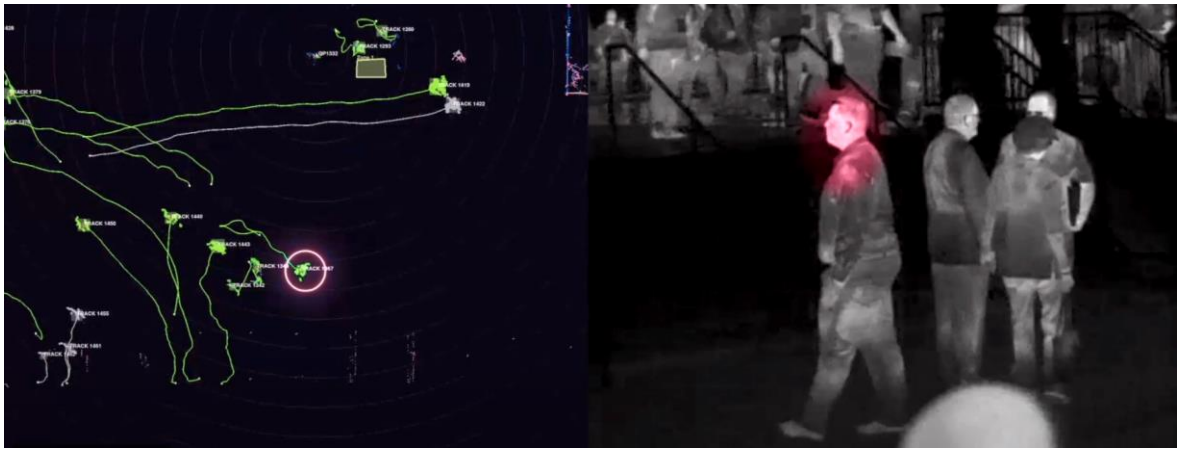


Obrázek 28 Skenování objektu [34]

7.2 QUANERGY

Společnost Quanergy vytvořila platformu, která spojuje nejmodernější laserové lokátory se softwarem QORTEX. Použití produktů této firmy se především využívá pro ochranu veřejných prostor, jako jsou například parky, nákupní střediska a další místa s větší koncentrací lidí. Toto spojení umožnuje boj proti zákeřné virové nemoci Covid-19 a to tak, že zachycená data samotným senzorem se následně analyzují pomocí integrovaného softwaru. Inteligentní systém umožnuje vytvoření oblastí, ve který se hlídá sociální distance. Lidar dokáže zjistit přesnou polohu, rychlost a směr osoby v hlídané oblasti, následně software tyto údaje porovná s dalšími detekovanými osobami a v případě nalezení shlukování osob v těsné blízkosti vytvoří hlášení pro operátora a ten následně postupuje podle předem nastavených pravidel. Velkou výhodou laserové radiolokátoru je jeho umění detekování postavy. Díky těmto vlastnostem software dokáže rozeznat a vyhodnotit matku s dítětem oproti shluku osob. Pokud se tento systém propojí i s termokamerou - dokáže vyhodnocovat zvýšenou teplotu osob v hlídané oblasti. Tento způsob boje proti Covid-19 má budoucnost. . [35]

Obrázek 29 Detekce shlukování osob[35]

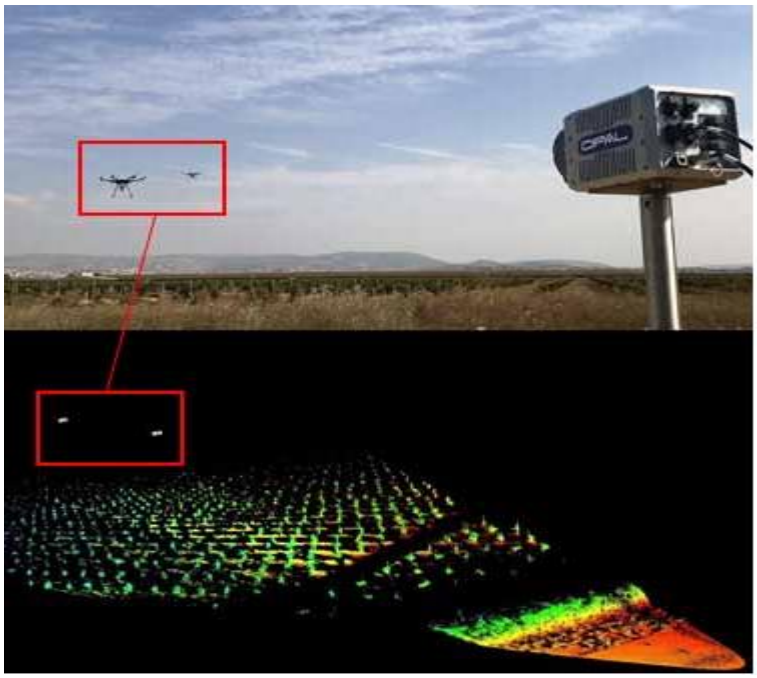


Obrázek 30 Detekce zvýšené teploty osoby.[35]

7.3 OPAL BY LUMIBIRD

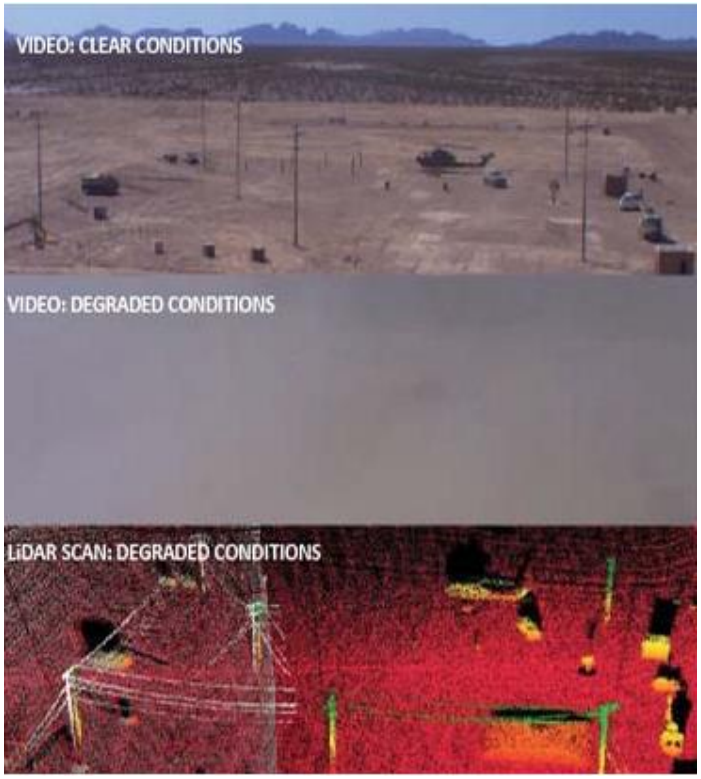
OPAL BY LUMIBIRD je společnost, která se zaměřila na takzvanou šedou zónu laserových lokátoru. A tou je detekování malých cílů s velkou přesností na malé i velké vzdálenosti. Těmito malými cíli se myslí především drony, anebo jiné bezpilotní letouny. Tento způsob sledování letišť, průmyslových zón a dalších oblastí se zákazem vstupu se v dnešní době velmi rozmohl. Pro detekování dronů se používají jednotlivé výrobky z řady OPAL-P****Tento systém poskytuje výjimečnou kombinaci detekčních technologiích a inteligentní 3D zpracování v reálném čase, má velký detekční rozsah, hustotu a rychlost

získávání dat. Díky právě velké hustotě získaných dat a schopnosti odstranění pozadí snímané oblasti je umožněno detekování právě i malých plastových dronů na velké vzdálenosti. Systém dokáže sledovat velké množství cílů najednou, a tudíž ho nepřekvapí ani pokus vniknutí do oblasti za pomoci velkého množství dronů či narušitelů.[36]



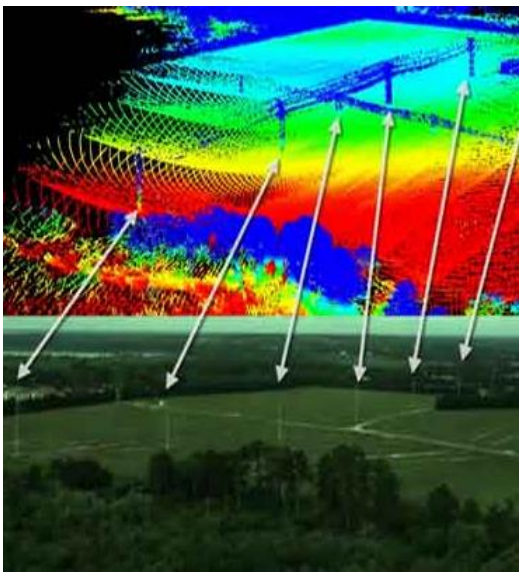
Obrázek 31 Detekování dronů [36]

Všechny produkty jsou navrženy, tak že spolupracují se softwarem 3DRi. Jedná se o software pro extrakci užitečných informací ze 3D skenerů v reálném čase. Například o identifikaci a rozpoznávání známých objektů, jejich typu, rychlosti a směru pohybu, všechny tyto vlastnosti jsou řešeny v reálném čase. Opal se dále může využívat jako senzor pro snadnější práci pilotům při vzletu či přistání během nepříznivých podmínek. Využití spočívá v přesné detekci jakékoliv překážky na vzletové ploše a pomoci s autonomním přistáním. [36]



Obrázek 32 OPAL-P1000 v praxi. [36]

Další nepřehlédnutelnou vlastností je využití dosahu pro zajištění bezproblémového letu. Detekce například vysokého napětí, lesní porostů a podobně vše na vzdálenost 1km může zajistit zvýšení bezpečnosti při používání bezpilotních leteckých systémů. [36]



Obrázek 33 Navigace pro letouny. [36]

Dílčí závěr

V této kapitole jsem ukázal velké množství dnes používaných radarových technologií, které se používají pro perimetrickou ochranu. Dobře víme, že samotné detekování narušitele pro ochranu nestačí, proto je zapotřebí k těmto detekčním přístrojům přidat ještě oči. Pokud se ale podíváme na všechny tyto prostředky a měli bychom je mezi sebou porovnat ohledně jejich vlastností a funkčnosti na jednotlivých objektech, mohli bychom je pak rozdělit do jednotlivých skupin. Do základní skupiny bych zařadil takzvané pásmové neboli segmentové detektory. Tento typ detektoru se používá pro ochranu jednotlivých pásem, vymezených úseků, či jednotlivých koridorů. Velkou výhodou je jejich detekční vzdálenost pohybují se až v stovkách metrů, na druhou stranu díky tomu mohou zabírat jen vymezený úsek. Jako u většiny těchto systému, je oproti například infrazávorám, umožněna přesná lokalizace narušitele. Do další skupiny zařadíme radary 36O°, zde se jedná o velký skok kupředu. Již můžeme hlídat, kromě prostoru před hranicí či plotové linii i vnitřní prostor. Těchto typů radarů je velké množství, z nichž všechny skenují celou oblast okolo sebe bez mrtvých úhlů. Téměř všechny systémy jsou doplněny o oči za pomoci připojení jednotlivých kamer. V této skupině by měly být kamery nejlépe úzce spojeny s radarem a umožňují operátorovy okamžité přenesení obrazu na ARC.

Do další kategorie řadíme laserové lokátory, tyto fungují v podobném duchu jako radarové systémy, ale jako nosič se využívá laser. Největší výhodou této technologie je její přesnost. Dokáží určit stejně jako v předchozích kategoriích rychlost a polohu, navíc přináší detaily jako je postava, výška, a to v detailu s přesností 3cm na 100m. Následně je můžeme ještě rozdělit mezi úzce profilové, které dokáží snímat jen úzkou část hlídané oblasti a jejich dokonalejší bratry, kteří pokryjí celý prostor. Také se mezi sebou dělí podle množství paprsků, kterými skenují oblast. Nesmíme, ale zapomenou na poslední kategorii, ve které se nám ukrývají pomocné SW. Tyto nástavby k laserovým lokátorům posouvají detekování, sledování narušitele do úplně jiné dimenze. Využitím přesnosti Lidaru a SW, vytvoříme 3D model na monitoru operátora v ARC, který sleduje reálnou situaci v přímém přenosu a dokáže podle ní navigovat případnou fyzickou ostrahu nacházející se v oblasti.

II. PRAKTICKÁ ČÁST

8 ANALÝZA STANDARDŮ A LEGISLATIVNÍCH POŽADAVKŮ NA PERIMETRICKÉ SYSTÉMY

V této kapitole se zabývám legislativními požadavky, které určují právní úpravy obecně závazné v oblasti ochrany osob a majetku. Legislativu doplňují technické normy, které specifikují technické parametry celého systému, i jednotlivých komponentů v oblasti perimetrických systémů. Velkým milníkem pro určení práv a povinností právnické a fyzické osoby v oblasti ochrany osob a majetku je zákon o civilních bezpečnostní službách, který je nyní v návrhu a rozděluje jednotlivé bezpečnostní činnosti do kategorii a dále je specifikuje.

Zákon č. 1/1993 Sb., Ústava České republiky

Ústava *„Česká republika je svrchovaný, jednotný a demokratický právní stát založený na úctě k právům a svobodám člověka a občana“* [37]

Zákon č. 2/1993 Sb., Listina základních práv a svobod

„Listina základních práv a svobod je dokument se silou ústavního zákona, zaručující lidská práva a základní svobody, hospodářské, sociální a kulturní práva národnostních a etnických menšin.“[38]

Zákon č. 163/2020 Sb. Občanský zákoník, ve znění pozdějších předpisů, a další související zákony

Občanský zákoník z pohledu problematiky této bakalářské práce řeší zejména

: • § 126 ochranu vlastnických práv

• § 11 ochranu fyzické osoby jako takové

• § 6, 415, 417 a 418 odvrácení neoprávněného zásahu do práv, majetku a škody na zdraví [39]

Zákon č. 40/2009 Sb., Trestní zákon, ve znění dalších předpisů

Účelem trestního zákona je: „C*hránit zájmy společnosti a ústavní zřízení České republiky, práva a zájmy fyzických a právnických osob“* [40]

Krajní nouze *„Čin jinak trestný, kterým někdo odvrací nebezpečí přímo hrozící zájmu chráněnému trestním zákonem, není trestným činem. Nejde o krajní nouzi, jestliže bylo možno toto nebezpečí za daných okolností odvrátit jinak anebo způsobený následek je zřejmě*

stejně závažný nebo ještě závažnější než ten, který hrozil, anebo byl ten, komu nebezpečí hrozilo, povinen je snášet.“ [40]

Nutná obrana „*Čin jinak trestný, kterým někdo odvrací přímo hrozící nebo trvající útok na zájem chráněný trestním zákonem, není trestným činem. Nejde o nutnou obranu, byla-li obrana zcela zjevně nepřiměřená způsobu útoku.“* [40]

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

Účel tohoto zákona nám hovoří: „*Účelem trestního řádu je upravit postup orgánů činných v trestním řízení tak, aby trestné činy byly náležitě zjištěny a jejich pachatelé podle zákona spravedlivě potrestáni. Řízení přitom musí působit k upevňování zákonnosti, k předcházení a zamezování trestné činnosti, k výchově občanů v duchu důsledného zachovávání zákonů a pravidel občanského soužití i čestného plnění povinností ke státu a společnosti.*

Pomáhat k dosažení účelu trestního řízení je právem a podle ustanovení tohoto zákona i povinností občanů.“ Dále nám trestní řád ukládá že: *„osobní svobodu osoby, přistižené při trestném činu nebo bezprostředně po něm, smí omezit kdokoli, je-li to nezbytné k zjištění její totožnosti, k zabránění útěku této osoby nebo k zajištění důkazů. Je povinen tuto osobu neprodleně předat policejnímu orgánu.“* [41]

Zákon č. 101/2000 Sb., o ochraně osobních údajů a Zákon č. 110/2019 Sb. o zpracování osobních údajů

Řeší problematiku nakládání s osobními údaji ve smyslu jejich ochrany před případným zneužitím, včetně uchovávání, zpracovávání osobních údajů a souhlasu dotčené osoby [42]

8.1 Technické normy

Technické normy považujeme za dokument, který určuje měřítko pro stanovení základních parametrů pro standardy. Tyto normy, ale nejsou závazné, považují se za doporučení.

Tabulka 1 Normy v oblasti poplachových systémů [43]

Číslo normy	Název normy
ČSN EN 50 130-x-y	Poplachové systémy – všeobecné požadavky
ČSN EN 50 131-x-y (ČSN CLC/TS 50 131-x-y)	Poplachové zabezpečovací a tísňové systémy
ČSN EN 62676-1-1	Dohledové videosystémy pro použití v bezpečnostních aplikacích
ČSN EN 60839-11-1	Poplachové a elektronické bezpečnostní systémy
ČSN EN 50134-1 (ČSN CLC/TS 50 131-x-y)	Poplachové systémy – Systémy přivolání pomoci
ČSN EN 50136-1 (ČSN CLC/TS 50 131-x-y)	Poplachové systémy – Poplachové přenosové systémy a zařízení
ČSN CLC/TS 50398	Poplachové systémy – Kombinované a integrované systémy
ČSN CLC/TS 50661-1 (ČSN EN 50398-1)	Poplachové systémy – Vnější perimetr zabezpečovacích systémů

Základním kamenem pro normu ČSN EN 50131-1 poplachové zabezpečovací a tísňové systémy je ochrana a konstantní zvyšování bezpečnosti v prostorech, které jsou střeženy. Na základě toho právě norma ČSN EN 50131-1 poplachové zabezpečovací a tísňové systémy vytvořila pro jednodušší přehled různé úrovně zabezpečení a tato norma právě říká : *„I&HAS a jeho komponenty jsou odstupňovány tak, aby poskytovaly požadovanou úroveň zabezpečení. Stupně zabezpečení berou v úvahu úrovně rizika závisící na typu prostředí, hodnotě majetku a očekávanému typickému vetřelci nebo lupiči.“* [43]

Stupeň zabezpečení 1 – Nízká rizika

„Předpokládá se, že vetřelec nebo lupič mají malou znalost I&HAS a mají omezený sortiment běžně dostupných nástrojů “ [43] Ve stupni zabezpečení 1 se můžeme nejčastěji setkat s byty, rodinnými domy a garážemi.

Stupeň zabezpečení 2 – Nízká až střední rizika

Předpokládá se, že vetřelec nebo lupič mají omezené o I&HAS a používají běžného nářadí a přenosných přístrojů. " [43] Ve stupni zabezpečení 2 se můžeme nejčastěji setkat s komerčními objekty.

Stupeň zabezpečení 3 - Střední až vysoká rizika

„*Předpokládá se, že vetřelec nebo lupič jsou obeznámení s I&HAS a mají rozsáhlý sortiment nástrojů a přenosných elektrických zařízení "* [43] Ve stupni zabezpečení 3 se můžeme nejčastěji setkat s peněžními ústavy, směnárnami.

Stupeň zabezpečení 4 – Vysoká rizika

„Používá se tehdy, má-li zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že vetřelec nebo lupič jsou schopní nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů" [43] Ve stupni zabezpečení 4 se můžeme nejčastěji setkat s objekty nejvyššího významu - státní instituce, jaderná zařízení.

Norma ČSN CLC/TS 50661-1

Pro naše účely je nejvíce směrodatná norma označena ČSN CLC/TS 50661-1 . Tato technická specifikace je specifikující pro vnější a perimetrické zabezpečovací systémy (EPSS), které poskytují detekci narušitele ve vnějších prostorech vně uzavřené budovy instalované na perimetru vně budovy. Zahrnuje čtyři stupně sabotáže, čtyři třídy prostředí a čtyři provozní kategorie. „*Dále technická specifikace specifikuje požadavky na funkcionalitu instalovaného systému EPSS, ale nezahrnuje požadavky na návrh, plánování, provoz nebo údržbu, Tyto specifikace budou vytvořeny následně v normě CLC/prTS 5O661-7* ." [44]

Dle normy ČSN CLC/TS 50661-4 „ *EPSS může být vytvořena z jedné fyzické jednotky nebo její funkce mohou být poskytovány kombinaci více zařízení. A také systém EPSS může být provozován ve spojení s jinými elektronickými zabezpečovacím a poplachové systémy jako jsou I&HAS,VSS a ACS*." Další rozhraní s jinými zabezpečovacími systémy jsou příbuzná, pokud nejsou v rozporu s povinnými požadavky této technické specifikace. [44]

Dále norma ČSN CLC/TS 50661-1-4 hovoří o tom, že EPSS musí poskytovat indikaci systémových informací pro uživatele/obsluze EPSS. Indikace musí být poskytnuty pomocí indikátoru. „*Indikátory pro účely zkoušky diagnostiky poruch nebo konfiguraci mohou být umístěny na jednotlivých komponentech systému EPSS. Indikátory mohou být jednoduché signální indikátory (zapnuto/vypnuto, světlo/zvuk), jednoduchá vizualizace založená na textu (například klávesnice), pokročilé operační software a aplikace běžící na standardní vybavení IT nebo na jiných vhodných vizuální nebo audio zařízení*.“ [44]

EPSS musí obsahovat jeden nebo více napájecích zdrojů, které mohou poskytovat energii z externích zdrojů (například napájení ze sítě místních), místních zdrojů (například generátoru), konečných zdrojů (například baterii), nebo obnovitelných zdrojů (například solární energie). EPSS může používat více typů napájecích zdrojů. [44]

Norma ČSN CLC/TS 50661-1-5 je uvedeno, že komponenty EPSS musí být klasifikovány dle jejich způsobilosti danému prostředí a stanoven stupeň dle jejich vlastnosti. [44]

Komponenty musí být vhodné pro použití v jedné z následujících prostředí. Tato norma hovoří o čtyřech třídách prostředí. V prvních dvou prostředí jsou definovány prostřední převážně jako vnitřní, ve kterých se samotné komponenty používají při stálé anebo nestálé teplotě. Třída prostředí III Vnější: Vlivy prostředí vyskytující se obvykle vně budovy přičemž komponenty EPSS nejsou plně vystaveny povětrnostním vlivům nebo vlivům uvnitř budovy, kde podmínky prostředí dosahuje extrému.

Třída prostředí IV Venkovní: Vlivy prostředí vyskytující se obvykle vně budov přičemž komponenty EPSS jsou plně vystaveny povětrnostním podmínkám [44]

Tabulka 2 Norma ČSN EN 60839 [45]

Číslo normy	Název normy
ČSN EN 60839-11-1	Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty

Norma ČSN EN 60839-11-1 popisuje obecné požadavky na funkčnost elektronických systémů kontroly vstupu (EACS) pro jejich použití v bezpečnostních aplikacích. Dále tato norma definuje různé stupně zabezpečení a funkčnosti systémů kontroly vstupu přiřazené ke každému z těchto stupňů. V této části normy nejsou obsaženy požadavky pro návrh, plánování, provoz nebo údržbu ty nalezneme v další části ČSN EN 60839-11-2.[45]

Tabulka 3 Dělení normy ČSN EN 62676 [46]

Číslo normy	Název normy
ČSN EN 62676-1-1	Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně
ČSN EN 62676-1-2	Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-2: Systémové požadavky – Výkonové požadavky na video přenos
ČSN EN 62676-2-1	Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 2-1: Video přenosové protokoly – Obecné požadavky

Nedílnou součástí perimetrických systémů jsou dohledové videosystémy neboli (VSS), doposud zvané CCTV, proto je potřeba zmínit i technickou normu, která se těmto systémům věnuje. ČSN EN 62676-1-1 tato norma předepisuje minimální požadavky pro VSS, používané pro zabezpečení aplikace. Touto normou jsou specifikovány minimální výkonnostní a funkční požadavky, které mají být sjednané mezi zákazníkem a dodavatelem v rámci provozních požadavků pro zajištění bezpečnostní služeb. [46]

V případě použití radarů na ochranu perimetru musí vše být v souladu s normou IEC 62368. Tato norma se vztahuje na bezpečnost elektrických a elektronických zařízení v oblasti audio/video, informační a komunikační technologie. Také vše musí být v souladu s rozhodnutím Českého telekomunikačního úřadu, který vydal všeobecné oprávnění č. VO-R/10/12.2019-9 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu. [47] [48]

8.2 Standardy požadavku pro perimetrickou ochranu

Jednotlivé standardy vždy hovoří o jednotlivých účelech, předmětu daných prvků, nebo předmětech a stanovují nám požadavky na zabezpečení námi předem určených cílů.

Hlavním cílem u perimetrické ochrany je odražení narušitele, identifikování a případné zamezení neoprávněného pohybu osob uvnitř perimetru a v neposlední ředě zpomalení jeho postupu. Ochrana samotného perimetru slouží především k detekci osoby a v nejlepším případě k úspěšné detekci a možnosti zajištění narušitele.

Hlavním cílem je

- Ochrana osob a majetku
- Zamezení vniku osoby do hlídané oblasti
- Při vniku osoby do objektu zajistit jeho identifikaci.
- Vytvoření podmínek pro snížení nároků na využívání hlídání pomocí fyzické ostrahy
- Předcházení a zefektivnění dosavadního řešení
- Zajištění souladu s platnými právními předpisy, technickými normami.

Standard pro ochranu perimetru je zajištění za pomoci mechanických zábranných systémů

„a) v případě objektu, který je v celé délce vymezen oplocením, se uplatňují pouze požadavky na oplocení a vjezdová a vstupní místa situovaná v oplocení;

b) v případě objektu, jehož perimetr tvoří plášť budovy, se uplatňují pouze požadavky na stavební konstrukce a ochranu stavebních otvorů v plášti budovy;

c) v případě objektu, jehož perimetr tvoří částečně oplocení a částečně plášť budovy, se uplatňují požadavky na oplocení a stavební konstrukce v příslušné části perimetru.“ [44]

Jako standard pro perimetrickou ochranu se považuje instalace prvků, které zajistí správný chod a při vyhlášení poplachu narušitelem určí přesnou lokaci. Dalším ze standardů je instalace prvků, které mají v dané oblasti nejvhodnější odolnost vůči tamnímu počasí. Jejich spolehlivost je na dostatečné úrovni, kterou si stanovil investor. Jako další standard se považuje co nejmenší náchylnost na falešné poplachy. Jednotlivé detektory musí mít možnost být vždy provázány s dohledovým video systémem.

9 MODELOVÉ SITUACE S POUŽITÍM RADAROVÝCH SYSTÉMŮ

V této kapitole si ukáži výhody a nevýhody použití radarových systému. Tyto systémy se dají použít u různých typů objektů s různou prioritou zabezpečení. Pro stupeň zabezpečení 1 – nízká rizika, které jsou nejčastěji určena pro zabezpečení rodinných domků se perimetrické systémy nevyužívají a to především pro jejich vysokou pořizovací cenu. Stupeň zabezpečení 2 – nízká až střední rizika - nejčastěji se týkají zabezpečení komerčních budov, anebo terminálů kontejnerové dopravy. Pro stupeň zabezpečení 3 - střední až vysoká jsem vybral jako příklad velvyslanectví Ruské federace. V posledním stupni zabezpečení 4 – vysoké riziko ukážu použití radarových systémů pro ochranu letiště. Dalším bodem modelových situací bude ukázka možného použití radarových systémů pro ochranu perimetru v bojových podmínkách pro přesun vojenských jednotek.

9.1 Využití moderních radarových systému pro přesun skupiny vojáků

K přesunu vojenských jednotek dochází velmi často, například pro průzkum pozemního cíle. Pro malou jednotku je vydán bojový rozkaz, který obsahuje všechny informace o úkolu. Například jaké je v dané oblasti počasí, samotná trasa přesunu, časový harmonogram, rozpis neseného materiálu, plán pro vysazení a vyzvednutí a samozřejmě i plán reakce při napadení za přesunu nebo v cílovém místě. Jednotka postupuje po jednotlivých předem určených pointech až k cíli. Při přesunu se dělají krátké a dlouhé přestávky. Krátká přestávka maximálně do 5min, vždy jen zakleknutí, nesundává se ani batoh. Při dlouhé přestávce, která trvá něco přes 10 minut je pauza určená pro napití a sundání batohu. Vždy odpočívá jen 50% jednotky a zbytek střeží, po krátké době se vymění. Pokud by došlo k útoku na jejich pozici, jednotka vedená jako průzkumná se nepouští do protiútoku, jen se vyváže z boje a vrací se k poslednímu pointu. Pokud vše dopadne dobře, průzkumná jednotka se dostane k cílovému místu a rozloží si základnu. Základna je místo vždy nedaleko od jejich pozorovacího místa, ze kterého pozorují prostor, kde je pravděpodobný výskyt nepřátelských jednotek, techniky anebo cíle. Dosud ochrana základny a pozorovacího místa spočívala v rozdělení perimetru mezi všechny buddy-teamy, které se mezi sebou střídaly v jeho hlídání, dále i z několika do předu vyslanými hlídkami pro ochranu vnějšího perimetru. Mezi sebou se vždy střídají po předem domluvených časových úsecích. Pokud bychom mohli vybavit takovouto jednotu přenosným laserovým lokátorem, umístil by se tento indikátor narušení perimetru improvizované základny například na vyvýšené místo (možnost umístění je i do koruny stromů kvůli neodhalení pozice jednotky), nebo uprostřed ležení viz obrázek, a to poblíž

středu ležení a k němu by byl připojen malý přenosný monitor, který by umožnil zpozorování blížící se nepřátelské hlídky a ukázal by směr, odkud se blíží. Tato možnost využití těchto moderních systémů v boji při přesunech jednotky by zajistila její bezpečí a i lepší regeneraci po těžkém přesunu. Tyto výhody by při případném boji s nepřátelskými jednotkami byly ku prospěchu a vedly by k menším ztrátám na životech při nočním napadení. Tato možnost má i svoji nevýhodu a to, že musí být použit laserový radiolokátor, který využívá pro skenování svého okolí vyšší barevné spektrum, než které dokážou spatřit nepřátelé za pomoci použití nočního vidění. Většina z těchto výrobků vidí barevné spektrum okem nespatřitelné v hodnotách okolo 750-850nm vlnové délky. Mnoho laserových radiolokátorů pracuje na vlnové délce okolo 850-920nm.

Obrázek 34 Radarový systém pro ochranu perimetru utábořené jednotky. [49]

Dalším uplatněním radarových systémů by mohlo být například v oblastech uschovávání a překladiště kontejnerových nákladů. Tyto místa jsou z důvodu jejich uložení často velmi neadekvátně zabezpečeny a to díky nemožnosti zajistit mechanické zabrané systémy po celou dobu provozu a následného elektronického systému podél celé hranice a uvnitř pozemku. Bohužel v těchto oblastech se velmi často setkáváme s jednoduchým zajištěním obvodu pomocí nízkého často i nevyhovujícího plotu a kromě základního kamerového

systému není zajištěna oblast jiným způsobem. Na základě stále rostoucí kriminality ve společnosti se dá předpokládat, že pachatel vstoupí do hlídaného areálu za účelem odcizit cennosti uschovány v přepravních kontejnerech. Poslední zábranou před otevřením kontejneru je běžný visací zámek. Tady spatřuji velkou budoucnost laserových radiolokátorů.

9.2 Terminál kontejnerové přepravy Nýřany.

Tento přepravní terminál společnosti Metrans sídlící na okraji měst Tlučná a Nýřany slouží k přepravě lodních kontejnerů s jakýmkoliv materiálem uvnitř. Lodní kontejnery jsou do objektu přivezeny pomocí kamionové dopravy a dále se již přemisťují za pomoci vlakové dopravy. Především se jedná o naložení a přeložení kontejnerů vezoucích jednotlivé výrobky od různých společností až přes různé zboží směřující mimo Českou republiku.

Obrázek 35 Terminál kontejnerové dopravy u Nýřan [Upraveno z: https://mapy.cz]

9.2.1 Stávající bezpečnostní prvky objektu a okolí

Hlavní příjezdová cesta do objektu je hlídání ostrahou v počtu dva muži a pes. Příjezdová cesta je zajištěna závorou a každé projíždějící vozidlo je podrobeno kontrole. Další boční vjezd do objektu vedle administrativní budovy je uzamčen za pomoci visacího zámku. Okolo celého objektu je postaven plot s vrcholovou ochranou a na několika místech jsou umístěny kamery. Perimetr vnější a vnitřní je možné pozorovat pomocí instalovaného systému CCTV. Zajištění vjezdové brány pro příjezd a odjezd vlakové soupravy je za pomoci elektronicky ovládané brány. Všechny kontejnery jsou vybaveny visacím zámkem a plombou, která nám říká, zda nebyl kontejner otevřen.

9.2.2 Aktiva

Nejdůležitějším aktivem v tomto terminálu jsou lodní kontejnery a jejich obsah a jednotlivé stroje, používající se pro přemístění kontejnerů.

9.2.3 Identifikace hrozeb

Pro identifikaci hrozeb tohoto terminálu bylo postupováno na základně zkušeností hodnotitele z jiných oblastí s podobnou bezpečnostní situací. Mezi největší hrozbu patří vstup organizované skupiny za účelem získání zboží přepravovaného v kontejnerech a to skrz vjezdovou bránu při nepozornosti ostrahy objektu, přes boční vchod do objektu za pomoci zneškodnění visacího zámku, vniknutím do objektu přes neuzavřenou bránu pro vlakovou dopravu, anebo překonáním perimetrické ochrany přes oplocení, nepovolený vstup personálu terminálu do jednotlivých kontejnerů za účelem obohacení o zboží uvnitř kontejnerů a požár uvnitř objektu.

9.2.4 SWOT analýza

Při této analýze se hodnotí S – strenght (silné stránky), W – weaknes (slabé), O – opportunity (příležitost), T – threat (hrozba). Zpravidla by tuto metodu měla sestavovat nezaujatá osoba z vnějšího prostředí. [50]

Tabulka 4 SWOT analýza

SWOT Analýza terminálu	
Pomocné vlastnosti	**Škodlivé vlastnosti**
Silné stránka	**Slabé stránky**
• Perimetr vnější a vnitřní je možné pozorovat pomocí instalovaného systému CCTV • Obvodový plot s vrcholovou ochranou • Nonstop ostraha 24/7	• Vstup přes hluchá místa kamer umístěné na perimetru • Boční vchod do objektu • Vstup skrz bránu určenou pro odjezd a přejez vlakové dopravy. • Vniknutí na pozemek skrz vjezdovou bránu.
Příležitosti	**Hrozby**

• Vniknutí do objektu mimo pracovní dobu • Napadaní fyzické ostrahy uvnitř objektu	• Odcizení cenností v přepravních kontejnerech • Znehodnocení používaných stroju • Požár uvnitř objektu

9.2.5 Analýza rizik metodou PNH

Analýza rizik uvedena v tabulce níže, byla provedena tzv. metodou PNH, kdy je počítána míra rizika, složena ze tří faktorů a to P – pravděpodobnosti výskytu rizika, N – následků rizika a H – názorem hodnotitele. Výsledkem je součin všech tří hodnot. Celkový výsledek je interpretován v pěti možných rizikových stupních v následujícím rozsahu.[51]

Tabulka 5 Rizikové stupně metody PNH

Rizikový stupěň	**R**	**Míra rizika**
I.	> 90	Nepřijatelné riziko
II.	45-90	Nežádoucí riziko
III.	11-45	Mírné riziko
IV.	3-10	Akceptovatelné riziko
V	< 3	Bezvýznamné riziko

Tabulka 6 Tabulka bodového hodnocení dle PNH

P - Pravděpodobnost	
Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5
N-Následky způsobené rizikem	
Mírné následky	1
Střední následky	2
Středně až těžké následky	3
Těžké následky	4
Fatální následky	5
H - Názor hodnotitelů	

Zanedbatelný vliv na míru nebezpečí	1
Malý vliv na míru nebezpečí	2
Větší až nezanedbatelný vliv na míru ohrožení	3
Velký a významný vliv na míru nebezpečí	4
Více významných a nepříznivých vlivů na závažnost a následky ohrožení	5

Tabulka 7 Tabulka rizik dle metody PNH

Posuzování činnosti: Rizika objektu					
Identifikace nebezpečí	**Vyhodnocení závažnosti rizika**				**Bezpečnostní opatření**
	P	**N**	**H**	**R**	
Vniknutí na pozemek skrz vjezdovou bránu.	2	4	2	16	Využívání spolehlivé a prověřené bezpečnostní služby.
Vniknutí na pozemek skrz boční vchod	3	4	4	48	Využití modernějších systému pro detekování a hlídání perimetru. Pořízení kvalitnějšího zámku na vrata.
Vniknutí na pozemek skrz vrata pro vjezd vlakové dopravy	3	4	3	36	Renovace automatického zavírání vrat po průjezdu. Využití modernějších systému pro detekování a hlídání perimetru.
Vstup přes hluchá místa kamer umístěné na perimetru	4	4	4	64	Využití modernějších systému pro detekování a hlídání perimetru
Napadaní fyzické ostrahy pro obchůzkové činnosti	2	3	3	8	Využití modernějších systému pro detekování a hlídání perimetru proti překvapení fyzické ostrahy ze zálohy.
Požár na pozemku	1	3	1	3	Dodržování protipožárních zásad. Případně instalace požárních hlásičů.

9.2.6 Vyhodnocení

V rámci analýzy rizik byla použita SWOT a PHN metoda, kterými bylo zjištěno následující:

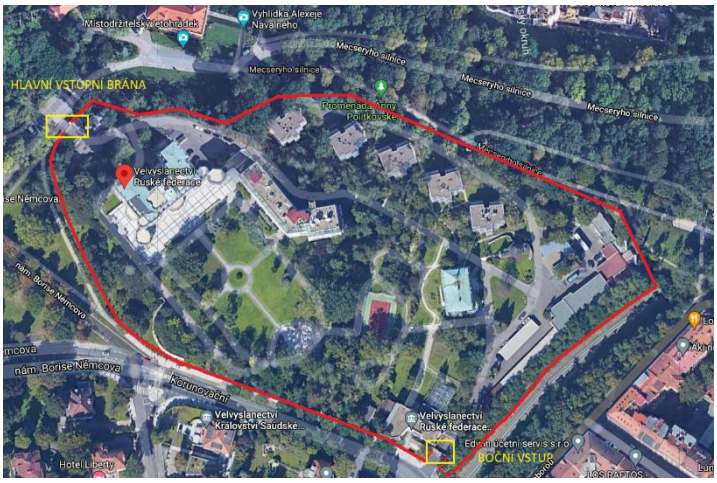
- Objekt se jeví jako v celku dobře zabezpečen proti běžným pachatelům, ale v případě organizované skupiny, která by si tento objekt vybrala záměrně a je znalá bezpečnostního systému a obchůzkových časů fyzické ostrahy objektu- není velký problém se na tento pozemek nepozorovaně dostat a následně zde způsobit nemalou finanční ztrátu. Jako nejvíce problematická část bezpečnostní ochrany se ukázalo vniknutí na pozemek přes hluchá místa kamerového systému. Další problematickou části se ukázalo vniknutí na pozemek skrz špatně zabezpečený boční vchod.
- Z obou analýz mě vyšly vysoká rizika překonání stávajícího zabezpečení. Proto navrhuji renovaci bezpečnostního systému. Velmi vyhovujícím produktem pro zlepšení bezpečnosti perimetrické ochrany tohoto objektu je laserový radiolokátor plus technologie od společnosti Accur8vision. Firma zajistí 3D vymodelování celého terminálu kontejnerové přepravy, do kterého následně umístí laserové radiolokátory. Výhodou systému je možnost nastavení různých zón a u nich jednotlivé proměnné, například časové období ochrany perimetru. Během pracovní doby odstřeženo a jinak zastřeženo. 3D model bude sloužit pro snadnější přehlednost ostrahy v objektu a možnost zjištění přesné lokace narušitele. Další nespornou výhodou oproti různým jiným bezpečnostním systémům pro ochranu perimetru je orlí přehled o hlídaném objektu. Lokátory jsou umisťovány na vysoké stožáry právě pro jasný přehled a možnost sledování narušitele i v oblasti mezi kontejnery, kde by ho ostatní systémy nemuseli mít možnost sledovat a posílat na ARC přesnou lokaci. Díky navržené renovaci bezpečnostního systému se minimalizují i další bezpečnostní rizika, které zmiňuji v analýze. V poslední řadě analýza rizik hodnotila případné fyzické napadení ostrahy uvnitř areálu, podle mne je to akceptovatelné riziko a fyzická ostraha na místě bude postupovat podle předem nastavených a naučených postupů pro tyto situace.

9.3 Terminály lodní kontejnerové přepravy

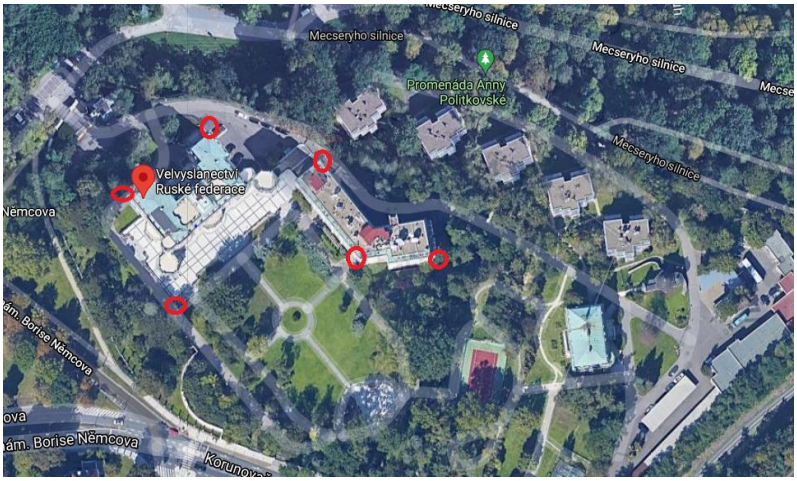
Další uplatnění radarových systémů je například v oblastech jako jsou nejrůznější přístavy, speciálně místa sloužící k naložení a vylodění kontejnerových nákladů. Tyto přístavy jsou často velmi neadekvátně zabezpečeny. Většinou díky nemožnosti zajištění plnohodnotného mechanického zabraného systému, který by tvořil pomyslnou hranici podél celého hlídaného objektu. Bohužel v těchto překladištích se setkáváme se zajištěním vstupu pouze přes pevninu. Nejčastěji je tento prostor zajištěn vjezdovou bránou, která je vybavena nonstop bezpečnostní službou. Tato ostraha na vstupu dohlíží na vjezd osobám jen s povolením a provádí kontrolu vozidel vjíždějících i odjíždějících. Samotná perimetrická ochrana je zabezpečena nejčastěji infrazávorami a nebo plotovým vibračním detektorem. Většinou je tento způsob elektronické ochrany perimetru doplněn kamerový systémem CCTV. Vnitřní prostor terminálu překladiště lodních kontejnerů není chráněn nijak jinak než pomocí kamerového systému. Vstup přes přilehlou vodní plochu není ve většině případech chráněn nijak. Po vstupu pachatele do areálu přes vodní plochu je zboží umístěné v lodních kontejnerech chráněno jen pomocí visacích zámků. Velmi vhodné je doplnění stávajících systémů o moderní systémy, jenž dokáží zajistit celkovou ochranu - jak samotného perimetru, tak i vnitřní části a právě i zmiňovaný vstup přes vodní plochu. Do jednotlivých objektů je možná instalace koridorových radarových systémů. Tento systém nedoporučuji, jelikož v těchto přístavech zůstávají kotvit velké dopravní lodě i přes noc a je zapotřebí je pomocí muringových a vazácích lan zakotvit ke břehu, tato lana způsobují přerušení koridorových radarů. Je proto lepší do zmiňovaných lokalit instalovat radarové technologie, které zabezpečí celý perimetr, a to jak vstup přes oplocení objektu, tak i přes vodní plochu. Tyto systémy by měly být propojeny s kamerovými systémy CCTV a vždy při detekci narušitele zaměří kameru na danou oblast pro možnost přenosu videozáznamu k operátorovi. Pro tyto případy je zapotřebí instalovat kamerový systém s nočním viděním, přísvitem anebo rovnou termokamery. Kamery by měly být umístěny na vysoké stožáry právě pro jasný přehled a možnost sledování narušitele i v oblasti mezi kontejnery. Ostatní systémy neumožnují instalaci na vyvýšená místa a díky tomu nelze sledovat narušitele i v oblastech mezi kontejnery. Tato místa jsou často označována jako nehlídané prostory a díky tomu je v nich umožněno narušiteli nepozorovaně zmizet. Proto jsou pro tuto oblast nevhodné jiné systémy hlídání perimetru.

9.4 Velvyslanectví Ruské federace

Dalším uplatněním a použití radarových systémů ukáži na velvyslanectví. Objekt a pozemek, kterého se analýza týká, se nachází nedaleko centra hlavního města Prahy. Budova Ruské federace je zděná cihlová třípodlažní budova s podsklepením a s pochozí střechou. Pozemek je po celém svém obvodu oplocený plotem o výšce 250 cm, plot je tvořen částečně železnou hradbou a cihlovým zdivem. Pozemek okolo budovy je travnatý a částečně zalesněný. Dosavadní způsob zabezpečení mi není znám, ale mohu se jej pokusit odhadnout. Hranice pozemku bude nejspíše, jak je velkým zvykem, chráněna infra závorami a případně ochrana perimetru bude doplněna Pir detektory. Dalším prvkem, který se velmi často objevuje v těchto oblastech je statická kamera. Pokud se podíváme na tento systém, spatřuji v něm několik nedostatků. Kamery nedokážou zajistit v dostatečné míře detekování osob bez falešných poplachů, způsobené pohybem větví stromů a keřů v jejich blízkosti. Pokud bychom se zaměřili na ochranu hlavní budovy velvyslanectví Ruské federace- byl by naším hlavním úkolem zajištění nepřetržité ochrany perimetru okolo budovy a to například za pomoci VLP16-01 LiDAR detectoru v následujícím rozložení (viz obrázek). Tento způsob rozložení laserových lokátorů umožňuje nepřetržité skenování celého okolí budovy a v případě detekování narušitele zajistí zaměření přítomných PTZ kamer na narušenou zónu. V případě propojení s SW od společnosti A8V bychom mohli redukovat citlivost lokátoru a to z důvodu, že jejich běžná detekovaná vzdálenost je 100m.



Obrázek 36 Perimetr Velvyslanectví Ruské federace [Upraveno z: https://mapy.cz]



Obrázek 37 Rozvržení VLP16-01 LiDAR detectoru na Velvyslanectví Ruské federace [Upraveno z: https://mapy.cz]

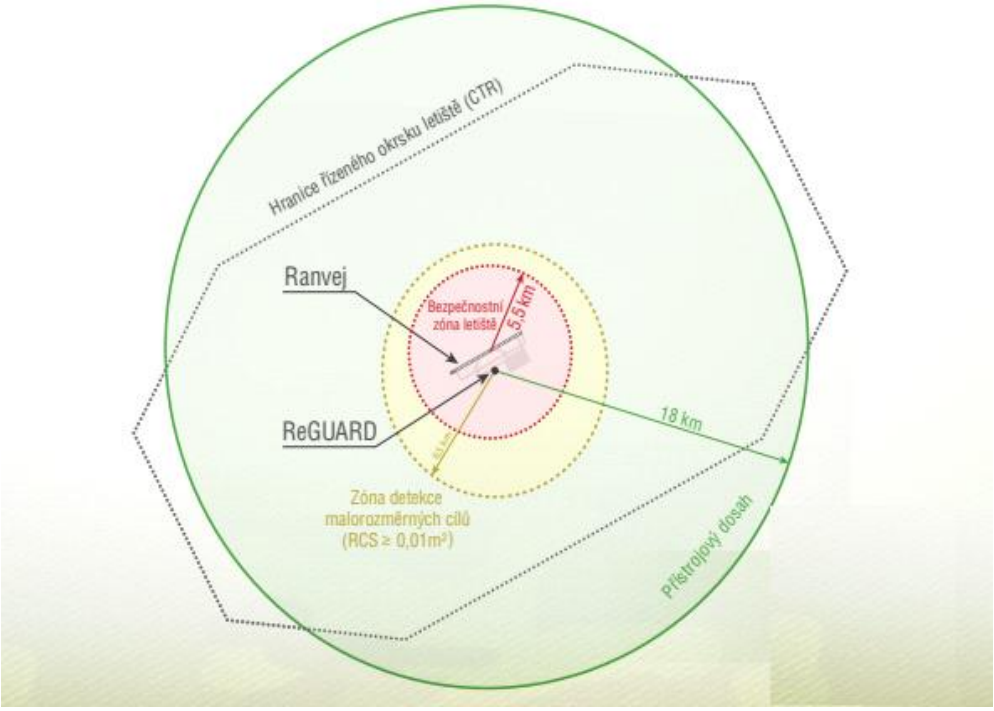
Dalším hrozbou pro velvyslanectví je nepovolený přelet, sledování této hlídané oblasti pomoci bezpilotních letounů. Pro detekování těchto strojů se dá využít Lidar Opal - P 1000 od společnosti OPAL BY LUMIBIRD, který umožnuje detekovat drony v oblasti až na vzdálenost 1000m. Tímto by se rapidně zvedlo zajištění perimetrické ochrany pro velvyslanectví oproti běžným způsobu zajištění ochrany.

9.5 Zajištění perimetrické ochrany letiště

Pro další modelovou situaci jsem si vybral náhodné letiště. Pokud se podíváme na běžné zajištění perimetrické ochrany letiště - z velké části jsou tyto prostory jen oplocené a detekce osob zajištěna pomocí PTZ kamer. Alternativou je doplnění ochrany perimetru objektu o perimetrické systémy hlídání. Ty jsou primárně zaměřeny na ochranu samotné hranice pozemku proti narušitelům, ale žádný systém z nich nedokáže zajistit ochranu proti vzdušným cílům. A právě letiště jsou jedny z nejzranitelnějších objektů, ve kterých by přítomnost bezpilotních prostředků napáchala velké problémy v provozu. Existují i situace, kdy byl záměrně či účelně použit dron k sledování letadla při startu či při rolování po ranveji byl vtáhnut do motoru. A právě proto je zapotřebí těmto situacím předcházet.

Zatištění ochrany perimetru za pomoci jakéhokoliv radarové technologie má nespornou výhodou, která tu již byla zmíněna několikrát a tou je přesná lokace narušení v perimetru a následné sledování narušitele. Pro zajištění perimetrické ochrany letiště se ideálně hodí typ radaru od společnosti RETIA. Její produkt ReGUARD je jedinečná svého druhu. Tento radar

zajistí ochranu letiště- jak proti pozemním narušitelům, tak i proti těm vzdušným. Pokud se použitě radar v celokruhovém režimu, dokáže zajistit ochranu letišti v různých úrovní. V první úrovni, která se nachází od radaru do vzdálenosti 6,5 km zajistí detekování všech bezpilotních letounů do velikosti 0,01m2 a do výšky 1,5km, pro další úroveň jsou to typy letounů do velikosti 0,1m2 a do výšky 2km a už ve vzdálenosti 18km dokáže detekovat letadla o velikosti 1m2 a to maximálně ve výšce 3km.V této oblasti samozřejmě detekuje i jakékoliv pozemní vozidlo či osobu. Díky jeho aktivnímu zaznamenávání lze vystopovat za pomoci letových drah, místo odkud startoval a zjistit tak i jeho provozovatele. Další výhodou tohoto přístroje, ale která se v běžných podmínkách nepoužívá, je možnost jeho zařazení do anti-dronového systému, která zajištuje protivzdušnou obranu a případnou destrukci dronu či jiných bezpilotních letadel.



Obrázek 38 Zajištění ochrany letiště[24]

Dílčí závěr

V této kapitole jsem ukázal jednotlivé technologie a jejich využití pro různé stupně zabezpečení. Díky různým typům modelových situací je ukázaná nesporná výhoda těchto moderních technologie oproti běžně používaných systémům perimetrické ochrany, které by nedokázali zabezpečit tak velké území s takovou přesností.

10 ZHODNOCENÍ PRINCIPŮ A FUNKCE

Pokud se chceme podívat na laserové radiolokátory a začít je mezi sebou hodnotit, jedná se o velmi obtížnou studii. Pokud bych se na ně podíval ze základního principu - nebudou mít mezi sebou velké rozdíly. Systém Lidar vždy naskenuje své okolí a následně softwarová nástavba tuto naskenovanou oblast prověří a v případě nesrovnalostí detekuje změny. Základním rozdílem je kvalita zpracování samotného software a jeho nadstavbou. Pro srovnání jsem vybral laserový lokátor od společnosti QUANERGY - AQ-8 Lidar Sensor, OPAL BY LUMIBIRD - OPAL ™ 3D LiDAR skener, OUSTER – OSO, VELODYNE – PUK. K tomuto výběru produktů jsem došel analýzou dosavadního trhu, při které jsem zjistil, že existuje mnoho laserových lokátoru stejného, anebo velmi podobného typu a pro zhodnocení jejich funkcí a principů by nebylo vidět mnoho rozdílů. Při identifikaci a rozboru jednotlivých laserových systémů pro detekování narušitele v perimetru jsem postupoval srovnávací metodou, resp. vyhodnocení nejpravděpodobnějších potřebných funkcích na jednotlivých prvcích. Všechny tyto informace jsem vytáhl z katalogů jednotlivých výrobců.

Tabulka 8 Srovnání parametrů výrobků Lidar

	OPAL - P 1000	M-8	OS1 - 128	PUK
Výrobce:	OPAL BY LUMIBIRD	QUANERGY	OUSTER	VELODYNE
Metoda skenování	Risley Prisms	TOF	TOF	TOF
Maximální dosah :	10000 m	150 m	120 m	100 m
Horizontální zorné pole :	120°	360°	360°	360°
Vertikální zorné pole :	------	12,4°	45°	30°
Počet laserových kanálu :	12	8	128	16
Vlnová délka :	1500 nm	905 nm	850 nm	905 nm
Podpora programu Accur8vision	NE	NE	ANO	ANO
Podpora programu QORTEX DTC	NE	ANO	NE	NE
Podpora programu 3DRI	ANO	NE	NE	NE
Detekce Dronů	ANO	NE	NE	NE
Cena produktu	75 000 $.	8 000 $	7 500 $	5 600 $

Pokud se podíváme letmo na vytvořenou tabulku - prvním velkým rozdílem je metoda skenování. Většina ze skenerů používá metodu skenování TOF a jediný OPAL-P1000 využívá novodobější a přesnější metodu Risley Prisms. Dalším obrovským milníkem je maximální dosah možnosti detekování. Běžné prvky se pohybují mezi 100m až 250m. V této kategorii převyšuje své konkurenty OPAL, který dokáže s velmi velkou přesností detekovat i malé narušitele v jeho hlídaného perimetru na vzdálenost až okolo 1000m.

Další mnou sledovanou kategorií bylo zorné pole. V ní se většina porovnávaných produktů držela zajištění ochrany celého perimetru neboli sledování 360°. Výhodou sledování velké oblasti je jejich využitelnost u větší části hlídaných prostorů. OPAL-P můžeme spíše začlenit do kategorie výsečových/koridorových laserů, protože jeho zorné pole je do 120°.

Dalším faktorem je počet laserových kanálů, v této kategorie se pohybujeme běžně v jednotkách kanálů s výjimkou laseru od společnosti OUSTER, která rapidně zvýšila počet kanálů kvůli lepší kvalitě snímání detailů. Nejčastěji se pro naše laserové radiolokátory používají polovodičové lasery GaAs, GaAlAs, GaInAs s vlnovou délkou 650 – 905 nm.

Předposlední kategorie- tou je propojitelnost s jednotlivými softwary. Pokud se podíváme na A8V je jeho propracování, vytváření jednotlivých zón, různé nastavené citlivosti detekování v oblastech, možnost virtuálního testování systému v reálném prostředí, unikátní zobrazení prvků v 3D prostoru na velmi vysoké úrovni. Dalším softwarem je QORTEX DTC, vývojáři tohoto programu se zaměřili především na nynější problematiku s šířením zákeřného virového onemocnění Covid-19. A jejich výtvor krom běžného hlídání perimetru se zaměřuje na zajištění dostatečné vzdálenosti mezi dvěma a více osobami, informuje operátora o shlukování více osob, dokáže rozpoznat, pokud se jedná o rodiče s dítětem, v případě propojení s termokamerou zajistí detekování osoby se zvýšenou teplotou, v neposlední řadě se vývojáři zaměřili na správu a sčítání například front u velkokapacitních prodejen, úřadů, dokáže optimalizovat obsazenost místnosti a má mnoho dalších vychytávek.

Dále jsem hodnotil možnost kompatibility detektoru s 3DRI softwarem. Zde se vývojáři většinou zaměřili na takzvanou šedou zónu laserových lokátoru a tou je vzdálenost detekce cíle a sledování dronů. Na základě detekce velmi malých předmětu se využívá tato kompatibilita pro několik procesů v přístavech a na vodních cestách, včetně nakládání a vykládání lodí, manipulace s nákladem a automatizace a řízení vodních systémů, v dopravě poskytuje 3D vidění okolního prostředí a pomáhá tak při provozu a řízení jak s posádkou i bez posádky.

V poslední srovnávací kategorii jsem se zaměřil na pořizovací cenu, ta je bohužel veřejně nepřístupná. Jednotlivé firmy nebyly ochotny tyto informace poskytnout. Po konzultaci s vedoucím práce mi bylo doporučeno, abych se pokusil jednotlivé ceny systémů odhadnout. Učinil jsem tak, na základě informací nalezených na internetu anebo získaných od odborníků z praxe. V případe laserového lokátoru určeného především pro detekování malých i větších cílů na vetší vzdálenost OPAL - P 1000 se pořizovací cena pohybuje okolo 75 000 $ (cca

1,58 mil. Kč.) V případě použití chytrého SW 3DRI se cena odvíjí od jeho umístění, zda se jedná o použití pro letecké účely, anebo ochranu perimetru objektu/hranic před bezpilotními letouny a pozemními jednotkami. V základu se tato cena SW pohybuje okolo 220 000 $ (cca 4,5 mil. Kč.). V případě lokátoru M-8 se jeho pořizovací cena odhaduje 8 000 $ (cca 170 tis. Kč.). Pokud bychom k tomuto prvku chtěli přidat ještě jejich unikátní SW QORTEX DTC, která umožnuje detekováni shlukování osob a další autonomní detekce jednalo by se u cenu 190 000 $.(cca 4 mil. Kč.). Pokud bychom chtěli odhodnotit jednu z modelových situacích a vybrali bychom si velvyslanectví Ruské federace. Cena jednoho použitého laserového lokátoru VLP16-01 LiDAR detector se pohybuje okolo 5 600 $ (cca 120 tis. Kč.). V případě potřeby instalovat SW Accur8vision server, area scanning (Photogrammetry), Create a 3D Map se jedná o navýšení rozpočtu 142 000 $ (cca 3 mil. Kč.). V těchto cenách nejsou započteny ceny pro instalaci a montáž, která se běžně pohybuje okolo 28 000 $ (cca 600 tis. Kč.). Tyto systémy mají velké výhody v detekování a dalších velmi spolehlivých systémech, ale jejich pořizovací cena tomu samozřejmě odpovídá. [34] [35] [36] [52]

Z výše uvedeného vyplývá, že není možné jednoznačně říci, který systém je lepší. Záleží vždy na konkrétních požadavcích na systém a tomu následně odpovídá i cena.

V dosavadním srovnávání moderních technologií jsem se zaměřil především na laserové lokátory. Pro ochranu perimetru se také využívají klasické radarové systémy. Tento způsob detekování je založen na vysílači a přijímači rádiových vln, nejčastěji v pásmu mikrovln. Pro srovnání jsem vybral radary od společnosti ReGUARD, Hikvison, Avestech. Dosavadní trh nabízí nepřeberné množství radarů, ale většina z nich je stejného anebo velmi podobného typu a pro zhodnocení jejich funkcí a principů by nebylo vidět mnoho rozdílů. Do porovnání jsem vybral produkty z jednotlivých kategorií.

Tabulka 9 Srovnání parametrů radarových výrobků

	ReGUARD	DS-PRP100	Perimetr Security	Scan-Integrated
Výrobce	RETIA	Hikvision	Avestech	Avestech
Provozní frekvence	X-pásmo	24.05 ~ 24.25 GHz	24.05 ~ 24.25 GHz	24.05 - 24.25 GHz
Detekční schopnost	18km	100m	500m	400m
Úhel záběru	360°	100°	5°	360°
Výškové krytí	3km	3m	3m	4m
Max. počet sledovatelných narušení	----------	32	4	18
Detekce Dronů	Ano	Ne	Ne	Ne
Propojení PTZ kamerami	Ne	Ano	Ano	Ano

Cena produktu	----------	2 000 $	2 300 $	6 000 $

Hlavním rozdílem mezi jednotlivými vybranými radary je jejich použití. Pokud se zaměříme na první radar, jedná se o vojenský radar, který se používá primárně pro sledování hranic a letišť. Použití pro účely ochrany těchto objektů je dáno možností detekování na vzdálenost 18km a rozpětí snímaného pole v 22km. Díky těmto vlastnostem dokáže zajistit detekování osob, vozidel a bezpilotních letounů.

Dalším vybraným radarem je úzce profilovaný radar Perimetr Security od společnosti Avestech, ten se zaměřuje na detekci podél hranic ve vzdálenostech 500m. Dalším produktem od stejné společnosti je Scan-Integrated, tento chytrý radar se zaměřuje na detekování narušitele v těžko dostupných prostředí. Díky jeho propojením s PTZ kamerou dokáže v tu samou chvíli detekovat osobu a zajistit i obraz pro operátora. A to vše v okruhu 200m na každou stranu.

V poslední řadě tu máme radar DS-PRP100 od Hikvision. Tento radar se běžně používá pro ochranu perimetru okolo soukromých i státních budov. Se zajištěním perimetru v úhlu 100° a do vzdálenosti 100m. Hlavním rozdílem je jejich použití v daném prostředí. Dalším rozdílem je provozní frekvence, ta se u většiny pohybuje v rozmezí 24.05 ~ 24.25 GHz, jediný radar ReGuard se pohybuje v pásmu X. Rozdílnou funkcí je počet detekovatelných narušitelů v hlídané oblasti. Jedná se o maximální možnost sledování narušitelů v dané zóně. Naprostá většina z radarů umožnuje propojení s PTZ kamerami, v případe ReGUARD to tak není a to díky velkému sledovanému území, které by kamery nedokázaly pokrýt.

V poslední srovnávací kategorii jsem se zaměřil na pořizovací cenu, ta je bohužel veřejně nepřístupná. Jednotlivé firmy mi nebyly ochotny tyto informace poskytnout. Po konzultaci s vedoucím práce jsem se pokusil jednotlivé ceny systémů odhadnout. Učinil jsem tak, na základě informací nalezených na internetu anebo získaných od odborníků z praxe. Ceny radarových lokátoru rapidně klesla oproti Lidar. Bohužel pro první radar se mi nepodařilo dohledat ani rámcové ceny, a proto ji zde neuvedu. V dalších dvou případech se dostáváme na pořizovací ceny v okolo 2 000 $ - 2 500 $ (cca 42 tis. kč. – 52 tis. Kč.), zde cenu určuje především vzdálenost snímání. Pro radar Scan-Integrated od společnosti Avestech se dostáváme na cenu 6 000 $ (cca 126 tis. Kč.) a to díky možnosti sledování zorného pole o úhlu 360° a automaticky připojené PTZ kameře. [22][23] [24]

Dílčí závěr

Pokud bych měl porovnat laserové lokátory a klasické radarové systémy, výrazně se nám ukazují systémy Lidar jako výhodnější v mnoha kategorií. Největší předností je jejich přesnost, utlum falešných poplachů, zorné pole a důmyslnější přenesení skenované oblasti na monitor operátora pro snadnější určování polohy narušitele. Samozřejmě zde hraje velkou roli při výběru cena, která díky kvalitě zpracování rapidně roste. Fotoaparáty, radary a sonary stále stojí dnes mnohem méně než jednotky systému LiDAR. Nicméně se domnívám, že laserové systémy mají jednoznačnou budoucnost v tomto odvětví. I mnoho bezpečnostních poradců, integrátorů a dokonce i někteří výrobci LiDAR hovořili o výhodách LiDAR, jak jsem vícekrát popsal, a zároveň tvrdí, že jejich rozvoj a integrace do běžných systému ještě přijde. [53]

ZÁVĚR

Bakalářská práce začíná stručnou analýzou používaných perimetrických systémů, inteligentních technologií pro obvodovou ochranu a ukázkou radarových systémů. U všech těchto systémů jsou popsány základní funkce, umístění a principy fungovaní. Praktická část je již zaměřena na radarové systémy pro perimetrickou ochranu. Zde byly zpracovány standardy a legislativní požadavky. V další části jsem ukázal výhody využití jednotlivých systémů v modelových situacích podle stupně zabezpečení. Na závěr jsem mezi sebou porovnal podle funkce a dalších vlastností radarové a Lidar systémy.

Při analýze novým trendů v perimetrické ochraně za využití radarových technologií jsem zjistil, že se výrobci snaží využit Lidar technologie i mimo zabezpečovací techniku, a to v automobilovém průmyslu pro autonomní řízení vozidel, díky jeho přesnosti a rychlému zpracování obrazu. Tento rozvoj bude směřovat ke zlevňování všech systémů včetně zabezpečovacího průmyslu, což povede k dalšímu komerčnímu využití právě pro oblast perimetrické ochrany. Další možnou oblastí pro využití systémů Lidar je oblast kriminalistiky. Zde se díky jeho přesnosti může naskenovat místo činu a následně lze z těchto naskenovaných scén rekonstruovat rozmístění všech objektu a nalézt i detaily, kterých si dříve nebylo povšimnuto. Novým trendem v bezpečnostním odvětví by mohlo být detekování narušitele ve vzdálenějším perimetrickém okruhu, čím by se prodloužil čas, které ho je zapotřebí pro přípravu zásahu proti případnému vniknutí do hlídané oblasti.

SEZNAM POUŽITÉ LITERATURY

[1] RONYO. Varya Perimeter / O systému | RFID a RTLS technologie. *Ronyo.eu* [online]. 2021 [cit. 2021-04-22]. Dostupné z: https://www.ronyo.eu/cs/technologies/varya-perimeter/

[2] SILMAN JOUIN. Buried Cable Detection Systems - Southwest Microwave Southwest Microwave. S*outhwestmicrowave.com* [online]. [cit. 2021-04-21]. Dostupné z: https://www.southwestmicrowave.com/products/buried-cable-detection-systems/

[3] PETR SVOBODA. ABBAS - Infrazávory Biris II pro obvodovou ochranu. *Abbas.cz* [online]. 2014 [cit. 2021-04-21]. Dostupné z: https://www.abbas.cz/clanky/recenze-technika/infrazavory-biris-ii-pro-obvodovou-ochranu/

[4] SECURITY NEWS DESK. Perimeter protection at the cutting edge of security - Security News Desk UK. *Securitynewsdesk.com* [online]. 2016 [cit. 2021-04-21]. Dostupné z: https://securitynewsdesk.com/perimeter-protection-at-the-cutting-edge-of-security/

[5] KELCOM. Produkty a řešení | KELCOMPCE. *Kelcompce.cz* [online]. 2009 [cit. 2021-04-22]. Dostupné z: http://www.kelcompce.cz/zabezpecovaci-systemy/produkty-a-reseni/13-Intelli-FLEX

[6] ČSN EN 60839-11-1. Poplachové a elektronické bezpečnostní systémy – Elektronické systémy kontroly vstupu Část 11-1: Požadavky na systém a komponenty [online]. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, Praha 2014, 56 s. [cit. 2021-04-21] Dostupné z : https://csnonline.agentura-cas.cz/

[7] MILAN ŘÍHA. *ŘÍHA, Milan : Bezpečnostní systémy*. Praha: Námořní ak,2011. ISBN 978-80-87103-35-7.

[8] REFLEX. id card door access system. *Reflexsystems.co.uk* [online]. [cit. 2021-04-21]. Dostupné z: https://www.reflexsystems.co.uk/product/card-biometric-door-entry-systems/id-card-door-access-system/

[9] MGR ING RADOMÍR ŠČUREK, Doc. *Biometrická technologie*. *VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA OSTRAVA*. 2015. ISBN 978-80-248-3786-4

[10] STŘÍTESKÝ, Bc Roman. *Problematika ochrany perimetru, zabezpečení vstupu a vjezdu do objektu*. Univerzita Tomáše Bati ve Zlíně 2018. [cit. 2021-03-21]. Dostupné z : https://digilib.k.utb.cz/handle/10563/43232

[11] KAREL JAVŮREK. Galerie - Technologie otisku prstu: (ne)bezpečné zabezpečení, foto. *Zive.cz* [online]. 2015 [cit. 2021-03-21]. Dostupné z: https://www.zive.cz/Client.Gallery/show.aspx?id_file=683458081&article=170784

[12] ERIC BEUK. Iris Scanning Technology & Biometric Vault Security - Safe Haven Private Vaults. *Safehavenvaults.com* [online]. 2019 [cit. 2021-03-23]. Dostupné z: https://safehavenvaults.com/iris-scanning-technology/

[13] VOP CZ. zabezpečení vjezdu vozidel do objektu, identifikace vozidel. *Edb.cz* [online]. 2018 [cit. 2021-04-15]. Dostupné z: https://nabidky.edb.cz/Nabidka-137653-system-pro-zabezpeceni-vjezdu-do-objektu-identifikaci-vozidel-a-kontrola-podvozku

[14] JAN GROHMANN. VOP CZ na výstavě IDEB v Bratislavě. A*rmadni-noviny.cz* [online]. 2018 [cit. 2021-04-21]. Dostupné z: https://www.armadninoviny.cz/vop-cz-na-vystave-ideb-v-bratislave.html

[15] VOP CZ. DOPRAVA. *Vop-security.cz* [online]. [cit. 2021-04-13]. Dostupné z: http://www.vop-security.cz/doprava.html

[16] SIEZA. Systém detekce skrytých osob. *Sieza.com* [online]. [cit. 2021-04-15]. Dostupné z: https://www.sieza.com/cz/produkty/system-detekce-skrytych-osob#article212

[17] JAMCOPTERS. Letecká termografie. *Jamcopters.cz* [online]. 2021 [cit. 2021-04-22]. Dostupné z: https://jamcopters.cz/industry/letecka-termografie

[18] SALEM. MDARS. *Army Guide* [online]. 2021 [cit. 2021-04-15]. Dostupné z: https://mpfdknak6q2uef72eybqisp2mu-hw4pqoxzcs7yk-www-army-guide-com.translate.goog/eng/

[19] ING. FILIP KLASNA. Izrael plánuje masivní nasazení bezpilotních prostředků |.*Security.magazine* [online]. 2015 [cit. 2021-04-15]. Dostupné z: https://www.securitymagazin.cz/security/izrael-planuje-masivni-nasazeni-bezpilotnich-prostredku-1404048290.html

[20] SZÖNYI, O. *RADAR-historie a funkce*. Fakulta jaderná a fyzikálně inženýrská. ČVUT, [online]. [cit. 2021-03-21]. Dostupné z: http://fyzsem.fjfi.cvut.cz/2006-2007/Leto07/proc/radar.pdf

[21] ING. VLASTIMILA CYPRISOVÁ. Pasivní sledovací systém Věra | Armáda ČR. *Army.cz* [online]. 9. březen 2010 [cit. 2021-03-10]. Dostupné z: https://www.acr.army.cz/technika-a-vyzbroj/protivzdusna-obrana/pasivni-sledovaci-system-vera-3504/

[22] HIKVISION. DS-PRP100, Mikrovlnný radar . *Hikvision.com* [online]. [vid. 2021-04-11]. Dostupné z: https://www.hikvision.com/cz/products/Alarm-Products/Security-Radar/Microwave-Radar/ds-prp100/

[23] AVESTECH. Perimeter Security. *Avestech.com* [online]. [cit. 2021-04-11]. Dostupné z: https://www.avestech.com/post/perimeter-security-radar

[24] RETIA. ReGUARD – Víceúčelový 3D radar pro detekci a sledování pozemních a nízkoletících cílů. *Reguard.cz* [online]. [cit. 2021-04-11]. Dostupné z: https://www.reguard.cz/cs/

[25] TOMÁŠ TENCER. *LiDAR – Pořizování 3D dat.* Ústav archeologie a muzeologie *Studijní materiály* [online]. 2012. [cit. 2021-04-11]. Dostupné z: http://fyzsem.fjfi.cvut.cz/2006-2007/Leto07/proc/radar.pdf

[26] DADISICK. Princip Lidar - bezpečnostní radarový skener zakoupený v přístavu Shekou v Shenzhenu. *Dongguan DADI Electronic Technology Co., Ltd*. [online]. 22. duben 2019 [cit. 2021-04-12]. Dostupné z: http://cz.light-curtain.net/news/principle-of-lidar-27976822.html

[27] ING. TOMÁŠ MIKITA, Ph.D. Letecké laserové skenování. Lesnická a dřevařská fakulta.2014[cit. 2021-04-29].
Dostupnéz: http://uhulag.mendelu.cz/files/pagesdata/cz/vgdp/vgdp_gis4.pdf

[28] FINTAN CORRIGAN. Introduction To UAV Photogrammetry And Lidar Mapping Basics. *Dronezon.com* [online]. 2019 [cit. 2021-04-12]. Dostupné z: https://www.dronezon.com/learn-about-drones-quadcopters/introduction-to-uav-photogrammetry-and-lidar-mapping-basics/

[29] JAN GRYGAR. Mobilní laserové skenování. *Mensuro.cz* [online]. 2019 [cit. 2021-04-12]. Dostupné z: https://mensuro.cz/vyuziti-mobilniho-laseroveho-skeneru-geoslam-zeb-horizon/

[30] LADISLAV ŠNAJDÁREK. Metoda 3D Laserového skenování obrobků. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ 2008. [cit. 2021-04-15]. Dostupné z : https://dspace.vutbr.cz/handle/11012/16782

[31] BC. MARTIN STRAPEK. Modelování výroby za pomocí metody 3D Laserscanningu. Západočeská Univerzita v Plzni - Fakulta Strojní. 2015. [cit. 2021-04-15]. Dostupné z : https://dspace5.zcu.cz/handle/11025/25211

[32] SCHITEA, Alexandru, Marius TUEF, Virgil-Florin DUMA a Aurel M. VLAICU. Modeling of Risley prisms devices for exact scan patterns. In: *Modeling Aspects in Optical Metrology IV* [online], 2013, [cit. 2021-04-27]. ISBN 9780819496058. Dostupné z: doi:10.1117/12.2020386

[33] YAO HU. The central ommatidium imaging (a) and ray tracing (b) models with... | Download Scientific Diagram. *Researchgate.net* [online]. 2021 [cit. 2021-04-28]. Dostupné z: https://www.researchgate.net/figure/The-central-ommatidium-imaging-a-and-ray-tracing-b-models-with-Risley-prisms-Risley_fig2_324118732

[34] ACCUR8VISION. accur8vision. *accur8vision* [online]. [cit. 2021-04-12]. Dostupné z: https://accur8vision.com/

[35] GLOBAL SECURITY EXCHANGE. Quanergy Systems, Inc. | LiDAR Sensors and Smart Perception Solutions. *Quanergy.com* [online]. 2021 [cit. 2021-04-27]. Dostupné z: https://quanergy.com/

[36] OPAL. Aerospace LiDAR - Neptec Technologies Corp. *Neptectechnologies.com* [online]. [cit. 2021-04-27]. Dostupné z: https://www.neptectechnologies.com/aerospace-lidar/

[37] Ústavní zákon č. 1/1993 Sb., Ústava České republiky [cit. 2021-04-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/1993-1

[38] Encyklopedický slovník. Praha: Odeon, 1993. Klub čtenářů Odeon. Rodinný klub, sv. 679. ISBN 80-207-0438-8.

[39] Zákon č. 163/2020 Sb. Občanský zákoník. [cit. 2021-04-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2020-163

[40] Zákon č. 40/2009 Sb. Trestní zákoník. [cit. 2021-04-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[41] Zákon č. 141/1961 Sb. Trestní řád. [cit. 2021-04-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141

[42] Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů. [cit. 2021-04-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110

[43] ČSN EN 50131-1 Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky [online]. 2007.40s. Dostupné z: https://csnonline.agentura-cas.cz/

[44] ČSN CLC/TS 50661-1. Poplachové systémy – Vnější perimetr zabezpečovacích systémů – Část 1 : Systémové požadavky [online]. 2019, 56 s. Dostupné z : https://csnonline.agentura-cas.cz/ [cit. 2021-04-21]

[45] ČSN EN 60839-11-1. Poplachové a elektronické bezpečnostní systémy – Elektronické systémy kontroly vstupu Část 11-1: Požadavky na systém a komponenty [online], Praha 2014, 56 s. [cit. 2021-04-21]Dostupné z : https://csnonline.agentura-cas.cz/

[46] ČSN EN 62676-1-1. Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky [online], Praha 2014, 48 s.[cit. 2021-04-21] Dostupné z : https://csnonline.agentura-cas.cz/

[47] ČSN EN IEC 62368-1 ed. 2 (367000) - Zařízení audio/video, informační a komunikační technologie - Část 1: Bezpečnostní požadavky - červenec 2020 - Technické normy - Ing. Jiří Hrazdil.[online]. [cit. 2021-04-29]. Dostupné z: https://shop.normy.biz/detail/510030

[48] VO-R/10/12.2019-9 Všeobecné oprávnění - Český telekomunikační úřad. [online]. 2019 [cit. 2021-04-29]. Dostupné z: https://www.ctu.cz/vseobecne-opravneni-c-vo-r10122019-9

[49] CHRISTIAN WOLFF. Perimeter Surveillance Radar - Radartutorial. *Radartutorial.eu* [online]. 2019 [cit. 2021-04-25]. Dostupné z: https://www.radartutorial.eu/02.basics/rp28.en.html

[50] SWOT analýza , *ManagementMania.com* [online]. 2020 [cit. 2021-04-16]. Dostupné z: https://managementmania.com/cs/swot-analyza

[51] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert. ISBN 978-80-247-4644-9

[52] BC. JAROSLAV BUBENÍČEK. *Možné dělení typů a druhů laserů* [online]. 2017 [cit. 2021-04-28]. Dostupné z: http://www.lt.cz/e-learning/laser/mozne-deleni-typu-a-druhu-laseru

[53] WARD, Chris. LiDAR-Powered Safe Distancing Technology, *Security.magazine* [online]. 2020 [cit. 2021-05-08]. Dostupné z: https://www.securitymagazine.com/articles/92556-lidar-powered-safe-distancing-technology

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PTZ Pan tilt zoon.

CCTV Closed Circuit Television.

ARC Alarm receiving centre.

DPPC Dohledové přijímací a poplachové centrum.

A8V Accur8vision.

ČSN Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

SW Software.

I&HAS Intrusion and Hold-up alarm Systém.

EPSS External perimeter security systems.

TOF Time of Flight.

VSS Video surveillance systém.

Sb. Sbírka zákonů.

PZTS Poplachová zabezpečovací a tísňový systém.

SPZ Státní poznávací značka.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK