

**VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH  
STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE**

**BAKALÁŘSKÁ PRÁCE**

**PERSPEKTIVNÍ PROSTŘEDKY PERIMETRICKÉ  
OCHRANY OBJEKTŮ**

**Autor práce:** Jaroslav Vaněček  
**Studijní obor:** Bezpečnostně právní činnost ve veřejné správě  
**Forma studia:** Kombinovaná  
**Vedoucí práce:** doc. JUDr. PhDr. Jiří Bílý, CSc  
**Katedra:** Katedra právních oborů a bezpečnostních studií

2020

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.  
Žižkova tř. 6, 370 01 České Budějovice

### ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Jaroslav Vaněček

Studijní program: Bezpečnostně právní činnost

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Místo studia: Příbram

**Název bakalářské práce: Perspektivní prostředky perimetrické ochrany objektů**

**Název bakalářské práce v anglickém jazyce: Promising means of perimeter protection of objects**



Katedra: Katedra právních oborů a bezpečnostních studií

Vedoucí bakalářské práce (jméno a příjmení, titul): doc. JUDr. PhDr. Bílý, CSc.




Datum zadání bakalářské práce (měsíc, rok):

Cíl bakalářské práce:

Hlavním cílem práce je seznámit s prostředky perimetrické ochrany objektů. Upozornit na nové hrozby, proti kterým je nutné objekty chránit (drony) a porovnat stávající způsoby ochrany s efektivitou použití nových moderních technických prostředků.

Student: Jaroslav Vaněček	6.4.2019 datum	 podpis
Vedoucí práce: doc. JUDr. PhDr. Bílý, CSc.	8.4.2019 datum	 podpis

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	15.4.19 datum	 podpis
Prorektorka pro studium a vnitřní záležitosti: RNDr. Růžena Ferebauerová	18.4.19 datum	 podpis
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	22.4.2019 datum	 podpis



Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce – v elektronické podobě ve veřejně přístupné části infodisku VŠERS a v tištěné podobě knihovnou VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce doc. JUDr. PhDr. Jiřímu Bílému, CSc, za cenné rady, připomínky a metodické vedení práce.

## ABSTRAKT

VANĚČEK, J. *Perspektivní prostředky perimetrické ochrany objektů*. České Budějovice: Vysoká škola evropských a regionálních studií, 2020. 70 s. Vedoucí bakalářské práce: doc. JUDr. PhDr. Jiří Bílý, CSc.

**Klíčová slova:** ochrana, perimetr, detektor, dron, kamera, termokamera.

Bakalářská práce se zabývá historií zabezpečovacích zařízení, vývojem a současnými možnostmi perimetrické ochrany objektů. Popisuje jednotlivé zabezpečovací detektory, princip činnosti a efektivitu jejich použití. Práce upozorňuje na nutnost implementace důležité součásti ochrany perimetru a to ochrany proti dronům, nové hrozbě, které se stává stále aktuálnější. Seznamuje s vývojem dronů a uvádí možnosti ochrany proti jejich možnému zneužití. Na praktickém příkladu návrhu kamerového systému autor dokládá efektivitu využití moderních metod zabezpečení.

## ABSTRACT

VANĚČEK, J. *Promising Means of Perimeter Protection of Objects*. České Budějovice : The College of European and Regional Studies, 2020. 70 p. Supervisor: doc. JUDr. PhDr. Jiří Bílý, CSc.

**Key words:** protection, perimeter, detector, drone, camera, thermal camera.

This bachelor's thesis deals with the history of security systems, evolution and nowadays features of a perimeter protection of a premises. The work describes particular security sensors, principles of their work and usage efficiency. The necessity of an anti-drone protection implementation, as new threat - becoming more actual, is highlighted in the work. The evolution in the drone branch is introduced with the possibilities of exploitation. The usage effectivity of such modern methods is demonstrated on practical example of security camera system.

# Obsah

Úvod.....	9
1 Cíl a metodika bakalářské práce .....	10
2 Perimetrická ochrana objektů.....	11
2.1 Historie zabezpečovací signalizace .....	11
2.2 Základy objektové ochrany .....	12
2.3 Dělení ochrany objektu .....	12
2.3.1 Klasická ochrana .....	13
2.3.2 Režimová ochrana.....	14
2.3.3 Fyzická ochrana .....	14
2.3.4 Technická ochrana .....	15
2.4 Ochrana perimetru .....	15
3 Specifikace jednotlivých prvků perimetrické ochrany.....	16
3.1 Mechanické zábranné systémy perimetrické ochrany.....	16
3.1.1 Zdi .....	16
3.1.2 Ploty .....	16
3.1.3 Průchozí prvky zdí a plotů .....	17
3.2 Prvky elektronického zabezpečení perimetrické ochrany.....	17
3.2.1 Mikrofonické kabely .....	18
3.2.2 Štěrbinové kabely.....	19
3.2.3 Infračervené závory a bariéry.....	19
3.2.4 Mikrovlnné závory .....	20
3.2.5 Zemní tlakové hadice .....	21
3.2.6 Venkovní infračervené pasivní detektory .....	22
3.2.7 Vibrační detekční systémy .....	23
3.2.8 Uzavřené kamerové systémy CCTV .....	24
4 Drony, technologie a možnost ochrany.....	27
4.1 Historie dronů.....	29

4.2	Druhy dronů .....	30
4.3	Technologie a autonomie dronů .....	31
4.4	Provoz bezpilotních prostředků v České republice .....	32
4.5	Antidronová ochrana .....	33
4.5.1	Radiofrekvenční analyzátory .....	35
4.5.2	Detekce prostřednictvím mikrofonů .....	35
4.5.3	Radarové detektory .....	36
4.5.4	Optické detektory .....	36
4.5.5	Příklady antidronových systémů .....	36
5	Nové technické prostředky perimetrické ochrany.....	42
5.1	Termokamery .....	42
5.2	Optická vlákna.....	44
5.3	Laserová technologie – LiDAR.....	46
5.4	Radarová technologie .....	48
5.5	Pokročilá videoanalýza.....	50
5.6	Porovnání kamerového systému klasická/termální technologie .....	53
	Seznam použitých zdrojů .....	63
	Seznam zkratk .....	67
	Seznam obrázků .....	69



## Úvod

Už od pradávna obyvatelé středověkých měst, královských hradů nebo celých států budovali opevnění a linie, které oddělovali okolní svět a pomáhali chránit vlastní území před vnějším nepřítelem. Tato myšlenka přetrvala do dnešní doby, jen se postupně změnil charakter a forma jejich střežení.

Perimetrickou ochranu lze v dnešní době definovat jako systémy a technologie, které chrání lidi a aktiva zamezením neoprávněných fyzických vniknutí po celém obvodu objektu. Jednotlivé vrstvy systému by měli chránit hranice a vnitřní prostory areálu s omezeným přístupem. Každá vrstva by měla pomoci odradit, zpozdit a detekovat vniknutí.

V posledním desetiletí pomohly technologické pokroky rozšířit systémy obvodového zabezpečení o nová řešení. Ty byly historicky používané k detekci narušení ve vojenských zařízeních, kritické infrastruktúře a dalších vysoce rizikových místech. Nyní je lze využít i v ostatních oblastech vyžadujících zvýšenou ochranu. Obvodové zabezpečení může zahrnovat oplocení, detekci jeho narušení, kontrolu přístupu, kamerové systémy a další. Typ používaných systémů a technologií závisí na pravděpodobných rizicích vniknutí, která začínají vandalismem, protesty aktivistů, krádeží, mohou být špionáží a v nejhorším případě končit terorismem.

# 1 Cíl a metodika bakalářské práce

V moderních bezpečnostních systémech se stále více uplatňují systémy pokročilé videoanalýzy, integrace radarových systémů a další perspektivní prostředky jako například detekce prostřednictvím laserů a optických vláken. S rychlým rozvojem elektroniky a zvýšení dostupnosti termálních kamer je aktuální jejich nasazení v rámci perimetrické ochrany objektů.

Cílem práce je seznámit s účelem a důležitostí zabezpečení objektů perimetrickou ochranou a popsat perspektivní technické prostředky využitelné k zabezpečení hranice objektů. Tyto nové metody zabezpečení bych chtěl analyzovat a srovnáním s doposud používanými systémy prokázat efektivitu jejich využití. Na praktickém příkladu bych také porovnal rozdíl v zabezpečení perimetru objektu prostřednictvím klasického kamerového systému a s využitím termálních kamer. Práce si dává také za cíl upozornit na nové možnosti ohrožení, které přicházejí s velkým rozšířením bezpilotních létajících prostředků, které mohou být zneužity k ohrožení důležitých objektů, jako jsou letiště, elektrárny a další objekty zvláštního významu.

Navrhované moderní možnosti zabezpečení nabízí příležitost ke zvýšení a zlepšení bezpečnostních opatření. Využití nových technologií a softwaru posílí fyzickou ochranu objektu a poskytne bezpečnostním pracovníkům nástroj pro efektivní výkon práce.

## 2 Perimetrická ochrana objektů

### 2.1 Historie zabezpečovací signalizace

Důležitým mezníkem ve vývoji přenosu informace byl vynález telegrafu v roce 1835 a jeho reálné využití v propojení Washingtonu a Baltimoru v roce 1844. O tři roky později newyorský inženýr Cornelius Anderson propojil telegrafem požární hlásky s centrálním stanovištěm a dále jednotlivé požární stanice, čím došlo k výraznému zkrácení doby reakce osazenstva požární stanice na poplachový signál. V roce 1851 byl v Bostonu schválen a budován systém veřejných hlásičů. Zatažením páky hlásiče došlo k roztočení vroubkovaného kola, které spínalo jednotlivé kontakty a došlo tak k odeslání signálů na centrální stanici, které identifikovaly konkrétní hlásič. Podobný systém byl vybudován koncem 19. století v Hamburku kde byl funkční až do roku 1976.<sup>1</sup>

Roku 1853 si pan Augustus Pope ze Sommersville nechal patentovat první elektrický zabezpečovací systém vytvořený kombinací kontaktů instalovaných na dveřích a oknech, baterií a zvonku. Svůj patent následně prodal Edwinu T. Holmesovi, který systém dále rozvíjel. Začal vyrábět izolované vodiče a vymyslel mnoho dalších elektrických součástí. Postupně vyvinul zařízení, které bylo schopno, pomocí barevných klapek, identifikovat stav každého zabezpečeného okna nebo dveří. S pomocí integrovaných hodin mohl také definovat časy zapínání a vypínání systému v určitý čas. V roce 1858 Holmes využil známé myšlenky centralizovaných pultů a vybuďoval první centrály elektrické ochrany v Bostonu a New Yorku. Ty sloužily převážně prominentním zákazníkům – Bowery Bank, Montreal Bank, John Jacob Astor, Tiffany a další.<sup>2</sup>

Rozvoj elektroniky po druhé světové válce, průmyslová výroba polovodičů, a miniaturizace přinesla rychlý rozvoj nových technologií a nových možností. Tyto technologie byly využitelné ve vývoji prostředků elektronických zabezpečovacích zařízení.

---

<sup>1</sup> KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. aktualizované vyd. Blatná : Blatenská tiskárna, 2006. 13s. ISBN 80-902938-2-4.

<sup>2</sup> KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. aktualizované vyd. Blatná : Blatenská tiskárna, 2006. 13-14s. ISBN 80-902938-2-4.

## 2.2 Základy objektové ochrany

Obecně ochrana znamená vytvoření bezpečného prostředí pro daný subjekt. Pro vytvoření efektivní ochrany musíme vědět, co je nutné chránit – předmět ochrany a cíl ochrany – proti čemu chráníme. Prostředky použité ochrany jsou bezpečnostním systémem, který představuje integrovaný celek zajišťující:

- osobní bezpečnost – ochrana osob;
- informační bezpečnost – ochrana informací;
- majetkovou bezpečnost – ochrana majetku.

Bezpečnostní systém obsahuje:

- mechanické ochrany – zábranné prostředky;
- elektronické ochrany – poplachové systémy;
- režimové ochrany – technicko - organizační opatření.

Při návrhu systému platí:

- absolutní ochrana neexistuje – vše může být překonáno;
- jedna skupina ochrany nic neřeší;
- technika člověka nenahradí – rozhodnutí zda se jedná o reálné ohrožení a následná reakce musí být na rozhodnutí člověka.<sup>3</sup>

## 2.3 Dělení ochrany objektu

Obr. 1: Dělení ochrany objektu podle AGA<sup>4</sup>



<sup>3</sup> KINDL, J. *Projektování bezpečnostních systémů. I. díl, EPS, EZS*. 1. vyd. Zlín : Univerzita Tomáše Bati, 2004. 93s. ISBN 80-7318-165-7.

<sup>4</sup> KINDL, J. *Projektování bezpečnostních systémů. I. díl, EPS, EZS*. 1. vyd. Zlín : Univerzita Tomáše Bati, 2004. 93s. ISBN 80-7318-165-7.

### **2.3.1 Klasická ochrana**

Zábranné systémy – ochrana spočívá v instalování takových mechanických zařízení, které by měli umožnit objekt chránit. Jedná se o prostředky pro ohraničení prostor, vstupní bezpečnostní systémy dveří a oken, mříže, bezpečnostní skla, fólie a uzamykací systémy. Mechanické zábranné systémy můžeme rozdělit do tří oblastí:

- prostředky obvodové ochrany;
- prostředky objektové ochrany;
- prostředky individuální ochrany.<sup>5</sup>

#### **Prostředky obvodové ochrany**

Jedná se o vnější mechanické zábrany, které jsou od zabezpečeného objektu prostorově vzdáleny a nejsou přímo součástí vlastního objektu. Jsou umístěny na parcele objektu, její volné ploše a často vymezují právní hranici pozemku. Nejdůležitějšími prvky uvedeného typu ochrany jsou ploty a zdi. Součástí jsou také prvky umožňující vstupy - dveře, branky, vjezdy.

#### **Prostředky objektové ochrany**

Základními prvky objektové ochrany objektů jsou zařízení zabezpečující všechny stavební otvory objektů – dveře, okna, vikýře, balkonová a sklepní okna, uzávěry technických a jiných šachet apod. Ve velké míře jsou zde zastoupeny různé druhy bezpečnostních dveří, zárubní a kování. Pro zabezpečení okenních otvorů pak instalace okenních fólií a mříží.

#### **Prostředky individuální ochrany**

Slouží jako samostatné úschovné prostředky pro úschovu nejrůznějších cenných předmětů. Jedná se hlavně o mobilní případně stabilní trezory, příruční poklady, trezorové skříně opatřené zámkovým systémem.

---

<sup>5</sup> KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. aktualizované vyd. Blatná : Blatenská tiskárna, 2006. 39s. ISBN 80-902938-2-4.

### **2.3.2 Režimová ochrana**

Režimovou ochranou je myšlen soubor administrativně organizačních opatření, která stanovují podmínky a postupy pro efektivní fungování ochrany objektu. Tato opatření můžeme rozdělit na vnější a vnitřní.

#### **Vnější režimová opatření**

Tato opatření definují podmínky pro vstupy a výstupy ze zabezpečeného objektu a to jak pro vstup a výstup osob tak podmínky vjezdu a výjezdu vozidel.

#### **Vnitřní režimová opatření**

Stanovují popis pohybu osob a vozidel uvnitř objektu, vymezují například různé oblasti a definují okruhy osob a podmínky jejich vstupu do daných oblastí.<sup>6</sup>

### **2.3.3 Fyzická ochrana**

Fyzickou ochranou se rozumí pravidelné (nemusí být nepřetržité) střežení objektu nebo dohled nad majetkem objednavatele, dohodnuté reagování na poplachový signál, zjišťování příčin vzniklé situace a informování majitele, případně policie. Střežení obvykle provádějí pracovníci specializovaných bezpečnostních služeb, kteří jsou dislokováni přímo v objektu nebo v jeho bezprostředním okolí. Nepravidelnou kontrolu mohou provádět pracovníci výjezdových skupin bezpečnostních agentur, kteří v různých intervalech provádějí fyzickou kontrolu objektu. Služby fyzické ostrahy mají jen preventivní charakter. Zaměstnanci, kteří vykonávají střežení, nemají žádné speciální pravomoci. Pokud přesto dojde k zadržení pachatele je možné, dle § 76, odst. 2 trestního řádu, omezit ho v pohybu, pokud je to nutné ke zjištění totožnosti, k zamezení útěku nebo k zajištění důkazů. Následovat musí bezodkladně předání policii.<sup>7</sup>

---

<sup>6</sup> KINDL, J. *Projektování bezpečnostních systémů. I. díl, EPS, EZS*. 1. vyd. Zlín : Univerzita Tomáše Bati, 2004. 94s. ISBN 80-7318-165-7.

<sup>7</sup> JELÍNEK, J. *Jak zabezpečit byt, dům, chatu, automobil*. Praha: Grada, 2000. 17s. ISBN 80-7169-931-4.

### 2.3.4 Technická ochrana

Technická ochrana objektů neslouží primárně jako ochrana, zařízení, které by znemožňovalo ohrožení objektu, ale slouží jako detekční systém. Upozorňuje na napadení objektu, informuje o jeho stavu, předává informaci o napadení.<sup>8</sup>

Technická ochrana objektů podporuje klasickou ochranu a zefektivňuje ochranu fyzickou. Tento typ ochrany představují hlavně elektronická zařízení – elektrický zabezpečovací systém, uzavřené televizní okruhy, elektrické přístupové systémy, elektrická požární signalizace, zařízení pro ochranu dat a informací případně jiná speciální technika.<sup>9</sup>

## 2.4 Ochrana perimetru

První linií ochrany objektu je jeho perimetr. Zvláště v případě strategicky významných objektů, jaderných elektráren, letišť apod. je důležité pokus o jeho narušení spolehlivě detekovat, ověřit narušení, předat o něm informaci a zajistit odpovídající reakci. Vzhledem k rozsáhlosti střežených objektů, není možné zabezpečit střežení pouze fyzickou ochranou, ale je nutné vybudovat prvky klasické a technické ochrany objektů.<sup>10</sup>

Funkce perimetrické ochrany:

- odrazení narušitele;
- znemožnění vstupu narušitele;
- zpomalení narušitele při překonávání klasické ochrany – mechanických zábranných prostředků;
- detekce narušení.

Možná skladba perimetrické ochrany:

- mechanické zábranné systémy;
- poplachový zabezpečovací systém;

<sup>8</sup> KINDL, J. *Projektování bezpečnostních systémů. I. díl, EPS, EZS*. 1. vyd. Zlín : Univerzita Tomáše Bati, 2004. 94s. ISBN 80-7318-165-7.

<sup>9</sup> KONÍČEK, T., KOCÁBEK, P. *Cesta k bezpečí*. 1. vyd. Praha : BEN - technická literatura, 2002. 20s. ISBN 80-7300-032-6.

<sup>10</sup> LUKÁŠ, L. *Bezpečnostní technologie, systémy a management*. 1. vyd. Zlín : VERBUM, 2011. 231s. ISBN 978-80-87500-05-7.

- prostředky průmyslové televize.

### **3 Specifikace jednotlivých prvků perimetrické ochrany**

#### **3.1 Mechanické zábranné systémy perimetrické ochrany**

Úkolem mechanickým zábran, překážek a bariér je při pokusu o napadení objektu vytvořit určitou časovou počáteční prodlevu mezi časem napadení a časem dokončení narušení objektu. Hodnota časové prodlevy může definovat určité kritérium bezpečnostní úrovně překážky – mechanického zábranného systému.<sup>11</sup>

##### **3.1.1 Zdi**

Zděná konstrukční bariéra musí být pro svůj účel obvodové ochrany pevná, bytelná, její minimální výška musí být 2,5 metru, musí být vystavená na podezdívce. Zeď musí znesnadnit, případně zabránit vstupu do chráněné zóny přezením, podlezením případně podhrabáním.

##### **3.1.2 Ploty**

Oproti zdím jsou ploty tvořeny převážně pevnou nosnou konstrukcí tvořenou ukotvenými sloupky s výplní pletivem případně železnými profily. Ocelové konstrukce musí být dostatečně chráněny proti povětrnostním vlivům antikorozní ochranou, která zabezpečí dlouhou životnost konstrukce.

Provedení antikorozní ochrany:

- zinkování;
- dvouvrstvý nátěrový systém;
- žárové zinkování;
- kombinované systémy s polyesterovou ochranou.<sup>12</sup>

---

<sup>11</sup> SKŘIVAN, Z. et al. *Nebojte se zlodějů: zabezpečovací technika v praxi*. 1. vyd. Praha : Grada, 1994. 19s. ISBN 80-7169-096-1.

<sup>12</sup> IVANKA, J. *Mechanické zábranné systémy*. Zlín : UTB ve Zlíně, 2010. 120 s. ISBN 978-80-7318-910-5.



### 3.1.3 Průchozí prvky zdí a plotů

Jsou důležitou součástí mechanických zábranných systémů, jedná se hlavně o vstupní branky a vjezdové brány. U objektů střežených fyzickou ostrahou jsou často navázány na systémy s kontrolou vstupu a vjezdu vozidel. V daném případě mohou být jejich součástí systémy pro elektronickou kontrolu vstupu vybaveny například čtečkami RFID čipů ovládajících vstupní turnikety. Elektronické přístupové systémy umožňují flexibilním nastavení oprávnění, které je možné dělit na personální, místní a časové.<sup>13</sup> Vjezdové brány mohou zabezpečovat systémy pro rozpoznávání registračních značek vozidel s oprávněním vjezdu. U objektů vyžadující vysoký stupeň zabezpečení se využívají elektromechanické silniční bariéry zabráňující vjezdu neoprávněných vozidel.

## 3.2 Prvky elektronického zabezpečení perimetrické ochrany

Jedná se o čidla a elektronické systémy detekující narušení vnějších částí rozlehlých objektů, komplexů budov nebo továren na samostatném pozemku. Existují řady druhů čidel, jejich činnost je založena na různých fyzikálních principech, z nichž každé je určeno pro specifickou část chráněného území dle optimálního využití principu detekce.

Konstrukce takových čidel, jejich mechanické a klimatické krytí, odpovídá účelu jejich vnějšího použití a odlišují se tak od prvků elektronických zabezpečovacích systémů určených pro vnitřní použití. Rozdílné jsou také samotné detekční parametry čidel, kdy se od venkovních očekávají dosahy detekce v řádech desítek až stovek metrů a ideálně s co možná nejširším prostorovým pokrytím oblasti.

V případě venkovních zabezpečení je problém v množství podnětů a vlivů, na které by neměla čidla reagovat. Jedná se zejména o:

- pohyb listí a větví stromů;
- proudění vzduchu;
- sníh a déšť;
- pohyb zvěře;

---

<sup>13</sup> KONÍČEK, T., KOCÁBEK, P. *Cesta k bezpečí*. 1. vyd. Praha : BEN - technická literatura, 2002. 125s. ISBN 80-7300-032-6.

- dopravní ruch v bezprostřední blízkosti hranice objektu.<sup>14</sup>

Výběr vhodné varianty elektronického zabezpečení perimetru objektu, vycházející z důkladné znalosti objektu a vlivů, které mohou ovlivnit činnost systému je zásadní pro eliminaci falešných poplachů a spolehlivost celého systému ochrany objektu.

### 3.2.1 Mikrofonické kabely

Princip činnosti a provedení:

Mechanické namáhání nebo vibrace mikrofonického kabelu jsou převáděny na elektrický signál, který je zpracováván ve vyhodnocovací jednotce. Kabel umožňuje akustický odposlech k rozpoznání charakteru narušení. Vyhodnocovací jednotka umožňuje definovat úroveň odezvy vyhlášení poplachu.

Použití a montáž:

Používá se k ochraně plotů, lze ho aplikovat i pod omítku. Nejčastěji je vpleten přímo do osnovy drátěného plotu. Předpokladem je dostatečná tuhost oplocení. Ideální je montáž současně s budováním oplocení. Délka jednoho úseku může být až 300 metrů.<sup>15</sup>

Výhody a nevýhody použití:

Výhodou jsou nízké náklady instalace a minimum nutných zemních prací. Falešné poplachy mohou být způsobeny povětrnostními vlivy, jakou je silný déšť, kroupy a silný vítr. Mohou být způsobeny také pohyby zvěře. Funkci může narušovat silné elektrické nebo elektromagnetické pole v blízkosti vedení kabelu. Proškolené obsluha může formou akustického odposlechu rozpoznat charakter narušení a volit tak správný způsob reakce na indikovaný poplach.<sup>16</sup>

---

<sup>14</sup> KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. aktualizované vyd. Blatná : Blatenská tiskárna, 2006. 96s. ISBN 80-902938-2-4.

<sup>15</sup> SKŘIVAN, Z. et al. *Nebojte se zlodějů: zabezpečovací technika v praxi*. 1. vyd. Praha : Grada, 1994. 119s. ISBN 80-7169-096-1.

<sup>16</sup> KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. aktualizované vyd. Blatná : Blatenská tiskárna, 2006. 97-98s. ISBN 80-902938-2-4.

### 3.2.2 Štěrbinové kabely

Princip činnosti a provedení:

Jedná se o speciální koaxiální kabel, který má ve svém stínění vytvořeny štěrbinový. Kabel je většinou instalovaný v páru s definovaným odstupem. Jeden kabel generuje elektromagnetické pole, jehož změny jsou druhým kabelem vyhodnocovány. Při pohybu osoby v blízkosti kabelů dojde ke změně elektromagnetického pole a tato změna je vyhodnocovací jednotkou interpretována jako poplach.

Použití a montáž:

Kabel je ve většině případů určen pro podzemní instalaci, kde je tak kopírován obvod střeženého objektu. Některé typy kabelů mohou být instalovány na nosnících nad povrchem. Délka jednoho úseku může být, dle typu kabelu, 100 – 200 metrů.<sup>17</sup>

Výhody a nevýhody použití:

S instalací tohoto typu detektoru jsou spojeny rozsáhlé zemní práce kolem celého střeženého objektu, což výrazně prodražuje instalaci zabezpečení. Falešné poplaky mohou být způsobeny pohybem zvířete a vlivy silných elektrických a elektromagnetických polí. Výhodou je možnost kopírování hranice objektu, není nutné vytvářet přímé úseky.<sup>18</sup>

### 3.2.3 Infračervené závory a bariéry

Princip činnosti a provedení:

Jedná se o nejčastěji používaný prvek perimetrické ochrany objektů. Detektor je tvořen vysílací a přijímací stranou, mezi kterými probíhají paprsky v infračerveném spektru. Přijímací strana vyhodnocuje dopad jednotlivých paprsků a dle definované logiky indikuje přerušení jednoho či více paprsků poplachem. Pro eliminaci ovlivnění přijímací strany jinými světelnými zdroji, pracují infračervené závory a bariéry v pulzním režimu. Pro bezproblémový provoz ve ztížených klimatických podmínkách

---

<sup>17</sup> SKŘIVAN, Z. et al. *Nebojte se zlodějů: zabezpečovací technika v praxi*. 1. vyd. Praha : Grada, 1994. 122s. ISBN 80-7169-096-1.

<sup>18</sup> KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. aktualizované vyd. Blatná : Blatenská tiskárna, 2006. 100-101s. ISBN 80-902938-2-4.

bývají pouzdra detektorů vybavena vyhříváním. Vzdálenost mezi zdrojem infračervených paprsků a přijímací stranou detektoru může být až 250 metrů.<sup>19</sup>

Použití a montáž:

Montáž bariér vyžaduje stabilní instalační sloupky s přímou viditelností mezi jednotlivými komponenty bariéry. Návrh musí zabezpečit překrývání jednotlivých střežených úseků, aby nevznikali místa, které nejsou střežena.

Výhody a nevýhody použití:

Tento druh čidel je v porovnání s ostatními obvodovými detektory relativně levný ale vyžaduje při instalaci kabeláže její dimenzování s ohledem na vyšší příkony vyhřívání jednotlivých krytů detektorů. Systém je citlivý na jevy, které mohou narušit viditelnost mezi vysílačem a přijímačem infračervených paprsků jako jsou mlha, padající sníh silný déšť. Výrobci tak detektory vybavují automatikou, která v případě dlouhodobého zaclonění čidel, vyřazuje jednotlivé segmenty z provozu pro eliminaci falešných poplachů.

### 3.2.4 Mikrovlnné závory

Princip činnosti a provedení:

Detektor vytváří elektromagnetické pole mezi vysílačem a přijímačem, který vyhodnocuje změnu tohoto pole při vstupu narušitele do detekční zóny. Mikrovlnné závory využívají ke své činnosti kmitočty 2,5 až 12 GHz. Signál, který je generován vysílačem dále modulován pro zabezpečení větší odolnosti detektorů proti vyhodnocování planých poplachů na základě cizích zdrojů signálů na stejných kmitočtech. Obvyklý tvar střeženého prostoru je elipsoid s výrazným poměrem velké a malé osy, kdy poměr elipsoidu v obou osách vzrůstá se zvětšením vzdáleností mezi vysílačem a přijímačem.<sup>20</sup>

---

<sup>19</sup> SKŘIVAN, Z. et al. *Nebojte se zlodějů: zabezpečovací technika v praxi*. 1. vyd. Praha : Grada, 1994. 120s. ISBN 80-7169-096-1.

<sup>20</sup> SKŘIVAN, Z. et al. *Nebojte se zlodějů: zabezpečovací technika v praxi*. 1. vyd. Praha : Grada, 1994. 121s. ISBN 80-7169-096-1.

Použití a montáž:

Mikrovlnné bariéry mají velmi dlouhý dosah použití, obvykle 200 až 300 metrů. Efektivně je možné používat tyto detektory i jako operativně využitelná technika s instalací prostřednictvím stativů. Při instalaci je důležité správně umístění vysílače a přijímače systému, aby nevznikali místa, které lze podlézt, případně by docházelo k zastínění částí střeženého prostoru.

Výhody a nevýhody použití:

Mezi hlavní výhody použití mikrovlnné bariéry je výše uváděný dlouhý dosah detektoru a při správně provedené instalaci a přizpůsobení střeženého prostoru, odolnost proti falešným poplachům. Zásadní podmínkou pro správnou činnost systému je vyloučení pohybujících se objektů v prostoru střeženého elipsoidu – odstranění keřů, větví a údržba porostu. Případný pohyb větví i travin může být zdrojem planých poplachů.<sup>21</sup>

### **3.2.5 Zemní tlakové hadice**

Princip činnost a provedení:

Zemní detektor je hydraulické čidlo, které je tvořeno soustavou dvou paralelně uložených tlakových hadic. Tyto hadice jsou plněny nemrznoucí směsí a jsou napojeny na tlaková čidla. Ta převádějí změnu tlaku na elektrické signály, které vyhodnocují změny tlaku v jednotlivých hadicích a je tak možné vyloučit změny, které jsou způsobeny podněty vznikající mimo střežený prostor, ty jsou vyhodnoceny podobně v obou větvích systému. Anomálie, která je způsobená narušitelem střeženého prostoru způsobí pak výrazný rozdíl tlaku v jednotlivých snímačích.

Použití a montáž:

Instalace zařízení vyžaduje rozsáhlé zemní práce. Jednotlivé úseky mohou být dlouhé až 200 metrů s roztečí jednotlivých hadic přibližně 100 centimetrů

---

<sup>21</sup> SKŘIVAN, Z. et al. *Nebojte se zlodějí: zabezpečovací technika v praxi*. 1. vyd. Praha : Grada, 1994. 121s. ISBN 80-7169-096-1.

Výhody a nevýhody použití:

Výhodou použití zemní tlakové hadice je možnost kopírování libovolného tvaru objektu. Není nutné dodržovat přímé linie, jak je tomu u ostatních perimetrických detektorů. Je možné takto zabezpečovat i různě členité střezené úseky. Způsob vyhodnocování změny tlaku eliminuje detekci planých poplachů, hydraulický systém pak vylučuje jeho ovlivnění vnějším elektromagnetickým polem.<sup>22</sup>

### 3.2.6 Venkovní infračervené pasivní detektory

Princip činnosti a provedení:

Infračervený pasivní detektor (PIR) obsahuje pyroelektrický snímač, který je citlivý na dopad infračerveného záření. To je vyzařováno jakýmkoli reálným tělesem o teplotě vyšší než 0 K (tj. – 273,1°C). Jakákoli změna dopadajícího tepelného záření na povrch pyroelektrického elementu způsobí generování elektrického impulsu, který je dále vyhodnocován.<sup>23</sup>

Pro definování detekční charakteristiky detektoru je před element umístěna fresnelova čočka, která rozděluje střezžený prostor na jednotlivé segmenty. Při průchodu narušitele napříč takto definovanými zónami dochází na pyroelektrickém elementu ke generování pulsů a následnému vyvolání poplachu. Pro správnou detekci jsou zóny na čočce vytvořeny jak ve vertikální tak v horizontální rovině. Infračervená pasivní čidla pro venkovní použití mají robustní provedení, odlišně nastavené vyhodnocování generování pulsů a často také soustavu několika pyroelektrických elementů. Pro zabezpečení klimatické odolnosti jsou kryty čidel vytápěny.<sup>24</sup>

Použití a montáž:

Dosah venkovních PIR čidel může být až 150 m. Montáž je nutné provádět dle instalované fresnelovi čočky a její detekční charakteristiky a to s ohledem na požadovaný dosah konkrétního čidla a jeho zorný úhel. Výhodné je využití

---

<sup>22</sup> SKŘIVAN, Z. et al. *Nebojte se zlodějů: zabezpečovací technika v praxi*. 1. vyd. Praha : Grada, 1994. 123s. ISBN 80-7169-096-1.

<sup>23</sup> BURDA, K. *Základy elektronických zabezpečovacích systémů*. 1. vyd. Brno : Akademické nakladatelství CERM, 2017. 34s. ISBN 978-80-7204-967-7.

<sup>24</sup> UHLÁŘ, J. *Technická ochrana objektů: II. díl, Elektrické zabezpečovací systémy II*. 1. vyd. Praha : Policejní akademie České republiky, 2005. 209s. ISBN 80-7251-189-0.

maskovacích šablon, kterými lze vydefinovat zájmovou zónu a vyloučit tak poplarchy vzniklé pohybem mimo hranice střeženého prostoru.<sup>25</sup>

Výhody a nevýhody použití:

Speciální venkovní PIR detektory jsou díky vícenásobným pyroelektrickým elementům a vyhodnocovacím obvodům přizpůsobeným pro venkovní použití odolné proti falešným poplachům. Ty mohou vznikat působením různým povětrnostním vlivům - víření vzduchu, dopadajícím slunečnímu záření apod.

### 3.2.7 Vibrační detekční systémy

Princip činnosti a provedení:

Systém propojených adresovatelných vibračních detektorů, které je možné umístit na rozličné mechanické zábranné systémy – běžné i průmyslové pletivo, betonové i plechové oplocení. Instalace je možná i do vnitřku konstrukcí případně pod povrch. Diferenciálním vyhodnocováním signálů z jednotlivých detektorů umožňuje eliminovat falešné poplarchy způsobené prudkým deštěm, silným větrem, kroupami apod. Adresace čidel umožňuje přesné definování vzniku poplachu.<sup>26</sup>

Použití a montáž:

Systém umožňuje vytvářet linie ochrany dlouhé až 1,5 kilometru. Modulární provedení umožňuje snadné rozšíření systému. Vhodná je jeho integrace do kamerových systémů s přímým ovládním PTZ kamer.

Výhody a nevýhody použití:

Absence pohyblivých částí předurčuje dlouhou životnost popisovaného systému. Výhodou je také snadná instalace a případný servis.

---

<sup>25</sup> KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. aktualizované vyd. Blatná : Blatenská tiskárna, 2006. 74s. ISBN 80-902938-2-4.

<sup>26</sup> SIEZA. Peridect. *Sieza.cz* [online]. [cit. 2019-11-15]. Dostupné z WWW: <<https://www.sieza.com/cz/produkty/peridect#article208>>.

### 3.2.8 Uzavřené kamerové systémy CCTV

Kamerové systémy představují důležitou součást perimetrické ochrany objektů. Zásadní roli pak mají v případě ostrahy rozlehlých objektů, kde slouží jako prostředek pro ověření poplachových výstupů z ostatních prvků perimetrické ochrany objektu. Jsou na ně přímo systémově navázány a členům fyzické ochrany objektu tak automaticky po vyhlášení poplachu, nabízejí vizuální informaci o dění v konkrétním úseku perimetru.<sup>27</sup>

Kamerový systém je možné instalovat také jako soubor senzorů – kamer, kdy je na základě videoanalytických funkcí automaticky detekováno narušení perimetru objektu. Takový systém vyžaduje důkladnou přípravu projektu, kde je nutné vyhodnotit snímací charakteristiky kamer, použitých objektivů a jejich ohniskových vzdáleností pro zajištění požadovaného pokrytí střeženého prostoru. Návrh musí vyloučit absenci míst, která nejsou pokryta kamerovým systémem. Zároveň je ale třeba použít efektivního počtu kamerových bodů – senzorů.<sup>28</sup>

#### Historie snímací techniky

Rok 1878 - první záznamy o pokusech přenést obraz elektronickou cestou - telegrafický přenos obrazu.

Rok 1881 - první dokumentovaný přenos obrazu v Londýně.

Rok 1884 – patentován Nipkowův kotouč – vynalezen princip řádkovaného rozkladu obrazu, který je v televizní technice používán dodnes.

Rok 1934 - vynález snímací elektronky – ikonoskopu (V. N. Zvorykin).

Rok 1936 - stanice BBC zahájila pravidelné televizní vysílání.

Rok 1941 - první průmyslově vyrobená kamera pro střežící účely.

Polovina 60 let - zdokonalování snímací elektronky Vidikon – cenově dostupná snímací elektronka i pro CCTV s dobrou rozlišovací schopností a citlivostí.

---

<sup>27</sup> ČANDÍK, M. *Objektová bezpečnost II*. 1. vyd. Zlín : Univerzita Tomáše Bati, 2004. 100s. ISBN 8073182173.

<sup>28</sup> UHLÁŘ, J. *Technická ochrana objektů III. Díl, Ostatní zabezpečovací systémy*. Praha : Policejní akademie České republiky, 2006. 246s. ISBN 80-7251-235-8.



80. léta – počátek vývoje CCD snímacího prvku obrazu – požadavek na miniaturizaci, dlouhou životnost, vysokou citlivost a nízké výrobní a pořizovací náklady.

1985 – první komerční CCD kamera na trhu, převrat ve vývoji obrazových snímacích prvků – umožněn rozvoj CCTV<sup>29</sup>

### **Základní rozdělení kamerových systémů**

#### Analogové kamerové systémy

Signál je přenášen prostřednictvím koaxiálních kabelů s konektory BNC nebo Cinch od kamery až k místu jeho využití. Využívá se norma typu PAL. Základem je analogový signál snímáný bezpečnostní kamerou v rozlišení 720 x 576 obrazových bodů a poměrem stran 4:3. Analogové kamery s vysokým rozlišením pak 960 x 576 bodů. Vedení koaxiálních kabelů je omezeno na 100 metrů v závislosti na jeho kvalitě. Nekvalitní koaxiální kabel, případně velká vzdálenost pak přidává do obrazu šum, ztrácí se ostrost a barvy. Pokud je nutná delší vzdálenost pro přenos signálu, je možné použít převodníky na vedení UTP, případně prostřednictvím optického vlákna. Výhodou analogových kamerových systémů je jejich jednoduchá obsluha, kompatibilita bezpečnostních kamer a DVR rekordérů různých výrobců a jednoduchá instalace bez nutnosti složité konfigurace.<sup>30</sup>

#### AHD kamerový systém

Jedná se o nejnovější technologii pro přenos analogového video signálu ve vysokém rozlišení prostřednictvím koaxiálního kabelu. Technologie může pracovat s rozlišením až 1920 x 1080 obrazových bodů. Zpracování signálu potlačuje případný šum při nízkých úrovních osvětlení a převádí digitální signál do jednoho modulovaného analogového signálu. To umožňuje jeho přenos na delší vzdálenosti, až 500 metrů bez zpoždění a ztrát. Pro vedení signálu se používají koaxiální kabely s možností využití převodníků na UTP případně optický kabel. Prostřednictvím jednoho koaxiálního kabelu je možné přenášet video signál, audio signál a obousměrnou datovou komunikaci RS485.

---

<sup>29</sup> KŘEČEK, S. *Ochrana majetku systémy průmyslové televize*. 1. vyd. Praha : Grada, 1997. 23-27s. ISBN 80-7169-402-9.

<sup>30</sup> BURDA, K. *Základy elektronických zabezpečovacích systémů*. 1. vyd. Brno : Akademické nakladatelství CERM, 2017. 108s. ISBN 978-80-7204-967-7.

## Digitální kamerový systém

Maximální rozlišení je dáno použitou kamerou, datovou propustností trasy a záznamovým zařízením, teoreticky zde není omezení další omezení. Tyto kamerové systémy využívají běžného protokolu TCP/IP a sítě ethernet. Pro přenos je tak využíván UTP kabel s možností napájení kamery prostřednictvím POE. Kamera obsahuje videosever s LAN výstupem RJ45. Uvedené kamerové systémy používají pro přenos a zpracování digitálního signálu kompresní formáty:

Kompresa M-JPEG – zpracovává celé jednotlivé obrázky, části obrazu bez pohybu se nefiltrují a vzniká tak velký objem dat náročný jeho další zpracování a ukládání.

Kompresa MPEG-4 – komprimuje jak video tak audio signál podobně jako v případě M-JPEG ale již s větší účinností.

Kompresa H.264 – modernější kompresní formát který již dokáže podstatně zredukovat velikost digitálního záznamu a to až o 80% ve srovnání s M-JPEG.

Digitální kamerové systémy neobsahují žádné analogové prvky a nejsou tak omezeny normou analogového signálu.<sup>31</sup>

### **Osvětlení snímané scény**

Osvětlení je důležitou součástí návrhu perimetrické ochrany prostřednictvím uzavřených kamerových okruhů. Světla by měla být instalována s ohledem na celkové světelné podmínky ve střežené oblasti. Nesprávný návrh a instalace osvětlení znemožňuje efektivní využití kamerového systému pro plnění jeho účelu. Hlavní cíl instalace osvětlení je zviditelnění útočníka a vyloučení možnosti využití neosvětlených míst pro narušení ochrany perimetru. Správné nasvícení hranice střeženého objektu zlepšuje účinnost ochrany a umožní bezproblémový přehled prostřednictvím CCTV. Úroveň osvětlení musí být navržena s ohledem na použité kamery a jejich citlivost, ta se za posledních několik let výrazně zvětšila a kamery jsou tak schopné pracovat i s minimální úrovní osvětlení. To přesto musí vytvořit dostatečný kontrast mezi útočníkem a pozadím snímané scény. Tradiční halogenová osvětlovací tělesa jsou postupně nahrazována LED osvětlením ve viditelné části spektra případně IR LED

---

<sup>31</sup> SECURIA. Informace o Bezpečnostních systémech. *Securia.cz* [online]. [cit. 2019-10-15]. Dostupné z WWW: < <https://securia.cz/informace-o-bezpecnostnich-systemech/226-zakladni-rozdeleni-kamerovych-systemu>>.

v infračervené oblasti. LED osvětlení nabízí mnoho výhod – rychlá aktivace, nízká spotřeba a dlouhá životnost.

Typickým příkladem je instalace světla společně s kamerou na jednu sloupku, dojde tak k optimálnímu pokrytí scény bez tmavých oblastí. Světla jsou instalována v jednom směru, nejsou tak oslňovány další instalované kamery protisvětlem.

Možností je také kombinace LED osvětlení v infračerveném i viditelném spektru. IR LED je použito pro nepřetržité nasvícení scény pro potřeby CCTV a viditelné LED osvětlení je spouštěno na základě výstupu z ostatních prvků perimetrické ochrany. Poskytne tak nejen možnost odstranění případného narušitele, tak možnost správného vyhodnocení narušení obsluhou kamerového systému. Tato instalace je možná právě v případě použití LED zdrojů, halogenové osvětlení, z důvodu pomalého náběhu, není možné použít.

## **4 Drony, technologie a možnost ochrany**

O dronech nebo také bezpilotních létajících prostředcích (UAV) slyšíme v dnešní době ze všech stran. Před několika lety se jednalo o velmi drahá zařízení, jejichž využití bylo převážně ve vojenské oblasti. Technologie dronů se ale neustále, díky pokroku v elektrotechnice a elektronice, vyvíjí a to hlavně v oblasti miniaturizace a autonomie. Každá další generace dronů je o něco menší, lehčí a levnější než předchozí generace. Vývoj nových materiálů a účinnější baterie umožňují bezpilotním létajícím prostředkům delší dolet, větší maximální výšku letu a zvýšení užitečného zatížení. To nám do budoucna skýtá velké možnosti využití dronů v různých oblastech našeho života. S tím ale přicházejí i nové hrozby - ohrožení soukromí, ohrožení fyzické a informační bezpečnosti a cílené útoky schopné způsobit jak velké materiální škody tak i ohrozit lidské životy.

Nebezpečí, které bezpilotní létající prostředky představují, dokumentují události, které se staly v nedávné době. V prosinci roku 2018 se v blízkosti londýnského letiště Gatwick objevily dva neznámé drony a nastalá situace ovlivnila nejméně 760 letů a zasáhla až 110 000 lidí tak jak bylo uvedeno v médiích: *„Letadla mířící na přistání byla odkazována na letiště v londýnském Heathrow, do Manchesteru, Birminghamu, případně i do Francie nebo Nizozemska. Podle deníku The Guardian se změny dotknou až 110 000 lidí. Zrušeno zatím bylo nejméně 760 letů. Ředitel provozu letiště Chris*

*Woodroofe uvedl, že po člověku, kdo drony řídí, pátrá policie. „Ve vzduchu máme i vrtulník, ale policie nás odrazuje od toho, abychom se pokoušeli drony sestřelit,“ řekl. Varoval, že potrvá dalších 24 hodin, než se provoz letiště vrátí k normálu. Podle velitele pátrání Justina Burtenshawa jde o jasný záměr poškodit provoz na letišti v Gattwicku. „Kdykoliv máme za to, že se blížíme k pilotovi, dron zmizí. Kdykoliv se pokusíme provoz letiště otevřít, dron se znovu objeví,“ uvedl. Policie však vyloučila, že by se mohlo jednat o teroristický útok.“<sup>32</sup>*

*Další závažnou událostí, byl útok pomocí dronů na ropná zařízení společnosti Saudi Aramco na východě Saúdské Arábie v září 2019 : „Deset dronů provedlo úspěšný útok na saúdskoarabská ropná zařízení, produkce ropy země klesla na polovinu. Dronový útok, který ovlivní celý svět. Tak by se ve zkratce dala popsat událost, ke které došlo v sobotu v Saúdské Arábii. Během útoku se skupinkám dronů podařilo úspěšně zaútočit na dvě největší ropná zařízení v zemi a paralyzovat je. Podle dostupných informací tak snížili produkci ropy o 5,7 milionů barelů denně, což je polovina produkce, největšího světového vývozce ropy, Saúdské Arábie a téměř pět procent ropy vytěžených celosvětově za jeden den. O jaký typ dronů šlo, zatím není jasné. Americký ministr zahraničí Mike Pompeo obvinil ze spoluúčasti na útoku Irán, s tím že neexistuje důkaz, že by Jemenští povstalci doposud disponovali sofistikovanou dronovou technologií. Útok bude mít hned několik důsledků. Tím prvním bude pravděpodobně zdražení ropy na světových trzích, ačkoliv Saudská Arábie slíbila, že případný deficit doplní ze svých rezerv, a to samé přislíbily také Spojené státy. Dalším důsledkem bude vyšší nasazení při vývoji a aplikaci protidronových opatření. Létající roboti se totiž ukazují jako čím dál tím schopnější zbraň schopná vykonávat akce v týle nepřítele. Navíc těmito systémy disponuje čím dál tím více armád světa a z futuristické technologie se stává de facto konvenční a běžně využívaný zbraňový systém.“<sup>33</sup>*

---

<sup>32</sup> Remy. Neznámé drony zastavily provoz na letišti Gatwick. Jde o záměr, říká policie. *iDnes.cz* [online]. Praha : Mafra, 2018. 20. prosince 2018 13:01 [cit. 2019-11-07]. Dostupné z WWW: <[https://www.idnes.cz/zpravy/zahranicni/gatwick-letiste-provoz-preruseni-londyn.A181220\\_080119\\_zahranicni\\_remy](https://www.idnes.cz/zpravy/zahranicni/gatwick-letiste-provoz-preruseni-londyn.A181220_080119_zahranicni_remy)>.

<sup>33</sup> Pierre. Deset dronů provedlo úspěšný útok na saúdskoarabská ropná zařízení, produkce ropy země klesla na polovinu. *Otechnice.cz* [online]. Praha : Mopax, 2019. 15. září 2019 [cit. 2019-11-07]. Dostupné z WWW: <<https://otechnice.cz/deset-dronu-provedlo-uspesny-utok-na-saudskoarabska-ropna-zarizeni-produkce-ropy-zeme-klesla-na-polovinu/>>.

## 4.1 Historie dronů

Pokud chápeme dron jako bezpilotní létající prostředek užitý k určitému účelu, tak první takové vojenské využití bylo v roce 1849. Rakouští vojáci použili balóny s podvěšenými výbušninami, kterými zaútočili na Benátky. Část vypuštěných balónů skutečně způsobily Benátčanům škody, některé však vítr zanesl zpátky nad zákopy rakouských vojáků.

Vývoj a výroba létajících strojů těžších než vzduch pak změnil situaci i v případě pokusů o stavbu bezpilotního prostředku. Pouze 16 let po prvním letu bratří Wrightů s ovládaným letadlem vyvinula Velká Británie bezpilotní letadlo, v podstatě létající bombu, kterou chtěli použít proti německým vzducholodím a případně proti pozemním cílům. Po několika neúspěšných pokusech byl však projekt zrušen – pro britskou armádu měla bezpilotní letadla omezený vojenský potenciál. Americké armádě se však v roce 1918 podařilo úspěšně otestovat nový bezpilotní prostředek, ale byl již vyvinut příliš pozdě, aby ho bylo možné využít ve válce a nikdy tak v boji nebyl nasazen.

Dalším impulsem ve vývoji nových technologií v oblasti UAV byla druhá světová válka. Na obou stranách bojiště byly využívány různé druhy dálkově ovládaných strojů a to pro samotný útok na nepřátele, tak pro trénování vlastní protiletectvé ochrany. Vývoj zbraňových systémů v období studené války přinesl i pokroky v technologii bezpilotních létajících strojů. V padesátých letech minulého století začala americká armáda testovat stroje schopné nést fotografickou techniku a provádět tak výzvědné lety.<sup>34</sup> Moderní válčení s drony začalo v roce 1982, kdy byly bezpilotní stroje společně s pilotovanými letadly použity Izraelskou armádou. Použití dronů minimalizovalo ztráty a vojenský potenciál nasazení UAV způsobil velké investice do dalšího vývoje. Moderní vojenské drony slouží obvykle jako pozorovací prostředky ovládané pilotem na dálku, které monitorují vybrané lokality, vytvářejí dokumentaci prostředí a označují pozice nepřátel. Dalším možným využitím je taktický průzkum - autonomní let k předem vybraným cílům. Některé UAV jsou využity přímo i k bojovým akcím, mají vyztužený trup s možností zavěšení munice. Využití

---

<sup>34</sup> ZALOGA, S. a PALMER, I. *Unmanned aerial vehicles: robotic air warfare, 1917-2007*. New York : Osprey, 2008. 10s. ISBN 18-460-3243-1.

nevojenských dronů začalo kolem roku 2006 a to pro potřeby ostrahy hranic, pomoc při živelných katastrofách a požárech, inspekce technologických celků a další.<sup>35</sup>

Vývoj bezpilotních leteckých systémů se nevyhnul ani České republice. Nejaktivnější byl a je Vojenský technický ústav letectva a protivzdušné obrany v Praze. Nejznámějším bezpilotním průzkumným letounem byl Sojka III. Byl určen převážně pro letecký průzkum v reálném čase a monitoring. Nasazen byl u rotý bezpilotních průzkumných prostředků Pozemních sil Armády České republiky v období od října 2000 až do svého vyřazení v roce 2010. Nyní je k vidění v kbelském muzeu.<sup>36</sup>

## 4.2 Druhy dronů

Multirotorové – nejoblíbenější typ dronů rozšířený jak mezi profesionály, tak i amatéry. Využívají se jak pro pořizování leteckých snímků, video dohled a průzkum. Provedení těchto UAV může být rozdílné podle počtu instalovaných rotorů a to v provedení se třemi, čtyřmi, šesti případně osmi motory. Hlavním omezením u těchto létajících prostředků je omezené doba letu, ta se pohybuje v rozmezí 20 - 30 minut a malé užitečné zatížení.

Drony s pevným křídlem – je zde využito stejných principů jako v případě tradičních letadel, vztlaku je dosahováno na křídle dopředným pohybem letounu. Zařízení jsou schopna provozu po dobu několika hodin a mohou tak mapovat rozsáhlé oblasti. Velkou nevýhodou je nemožnost zůstat nad jedním bodem zájmu. Problematický je také start a přistání, kdy je v případě větších dronů nutná startovací dráha a sítě eventuálně padáky pro zachycení dronu. V případě malých dronů s pevným křídlem lze využít i ručního vypouštění prostředku.

Vrtulník s jedním rotorem – látající prostředek s jedním hlavním rotorem pro svislý tah a ocasním rotorem pro stabilitu letu. Větší rotor oproti multikoptérám je účinnější v generování tahu. To umožňuje zvýšení užitečného zatížení. Nevýhodou je zvýšená složitost, vyšší cena zařízení, vibrace a nebezpečí hrozící od velké vrtule hlavního rotoru.

---

<sup>35</sup> WOLF, H.G. *Drones: safety risk management for the next evolution of flight*. New York: Routledge, Taylor & Francis Group, 2017. 11-13s. ISBN 978-1-138-20355-6.

<sup>36</sup> KARAS, J. a TICHÝ, T. *Drony*. Brno : CPRESS, 2016. 17s. ISBN 978-80-251-4680-4.

Hybridní drony s pevným křídlem – nová kategorie létajících prostředků kombinujících výhody pevného křídla a možnosti vznášet se nad konkrétním místem. Podle typu provedení umožňují také kolmý start a přistání.

### 4.3 Technologie a autonomie dronů

Technologie dronů se neustále vyvíjí, nové inovace a velké investice přinášejí na trh každých několik měsíců pokročilejší drony. Technologie bezpilotních létajících prostředků zahrnuje aerodynamiku, použité materiály, elektroniku a software. Použité jsou lehké kompozitní materiály pro snížení hmotnosti a zvýšení odolnosti trupu, tato kombinace umožňuje v případě vojenských dronů dosahovat vysokých nadmořských výšek. Drony mohou být vybaveny nejmodernější technologií, jakou jsou termokamery a lasery.

Důležitou součástí řídicí jednotky dronů je navigační systém. Často je používán duální systém využívající navigační systémy GPS a GLONASS. Systém letu je tak možný se stabilizací polohy založenou na vyhodnocování dat z navigačního systému, případně let bez této podpory. V tomto případě může být pro stabilizaci polohy dronu využit obraz z palubních kamer.

Vysoce přesná navigace umožňuje nejen stabilizaci UAV, automatický návrat na místo startu ale také aplikace jako 3D mapování, průzkum krajiny a vyhledávací a záchranné operace. V nejnovějších strojích jsou implementované další skupiny senzorů, které zabezpečují skenování okolí a detekci překážek. Jedná se o ultrazvukové, infračervené a laserové senzory. To umožňuje zcela autonomní let bez nebezpečí srážky.

Nezbytnou součástí řídicí jednotky dronu je inerciální měřicí jednotka. Obsahuje jeden nebo více akcelerometrů a gyroskopů. Porovnává a vyhodnocuje všechny síly působící na dron, detekuje všechny změny v jeho poloze, rychlosti a náklonu, spolu s ostatní elektronikou tak zajišťuje letovou stabilitu.<sup>37</sup>

Ovládání drohu probíhá prostřednictvím ovladačů bezdrátově komunikujících s řídicí jednotkou stroje. Pro komerční drony je nejčastěji využito kmitočtové pásmo 2.4 GHz a 5 GHz. Instalace vícepásmových přijímačů umožňuje letět pouze na základě

---

<sup>37</sup> ŘEŠÁTKO, J. a KOCOUREK, J. *Drony - Praktická příručka pro majitele dronů DJI*. Praha : Telink, 2019. 20s. ISBN 978-80-7346-228-4.

živého přenosu videa. Na displeji ovladače jsou zobrazeny také všechny dostupné telemetrické údaje – výška, vzdálenost, rychlost, počet dostupných signálů z družic GPS případně GLONASS a poloha. Komerčně dostupné drony mají dosah řízení a živého náhledu s přenosem videa v kvalitě Full HD až 8 kilometrů. Nově je možné využít prakticky neomezený dosah živě přenášeného živého náhledu bez většího zpoždění obrazu prostřednictvím instalovaných LTE datových modemů.<sup>38</sup>

Pro zavěšení kamery jsou součástí konstrukce až 3 osé stabilizátory. Jsou nezbytné pro dokonalé letecké snímkování a záznam videa. Umožňují eliminaci vibrací dronu a zabezpečují nastavenou polohu kamery v jakékoli letové poloze samotného UAV. Zavěšeny jsou až 4K kamery umožňující záznam až 30 snímků za sekundu.

#### 4.4 Provoz bezpilotních prostředků v České republice

Provoz bezpilotních létajících prostředků je v České republice upraven zejména Doplnkem X – Bepilotní systémy, Předpisu L2 – Pravidla létání. Při provozu UAV tak není možné využít všechny vlastnosti, které technika umožňuje, zejména řízení dronu jen na základě živého náhledu videa a využití maximálního doletu, jak je uvedeno v Doplnku X – *„S výjimkou, kdy ÚCL povolí jinak, musí být bezpilotní letadlo provozováno v přímém dohledu pilota, tj. takovým způsobem a do takové vzdálenosti, aby: a) pilot během pojiždění a letu mohl udržovat trvalý vizuální kontakt s bezpilotním letadlem i bez vizuálních pomůcek jiných než brýle a kontaktní čočky na lékařský předpis; a b) pilot, nebo kromě pilota i poučená osoba, mohla sledovat a vyhodnocovat dohlednost, překážky a okolní letový provoz.“*<sup>39</sup>

V Doplnku X je také vyloučena možnost přepravování nebezpečného nákladu případně shazování nákladu – *„10. Nebezpečný náklad - Bepilotní letadlo nesmí být použito k přepravě nebezpečných látek nebo zařízení, která by mohla způsobit obecné ohrožení, kromě provozních náplní v množství přiměřeném účelu letu. 11. Shazování nákladu -Bepilotní letadlo nesmí být použito ke shazování předmětů za letu, kromě*

<sup>38</sup> ŘEŠÁTKO, J. a KOCOUREK, J. *Drony - Praktická příručka pro majitele dronů DJI*. Praha : Telink, 2019. 23s. ISBN 978-80-7346-228-4.

<sup>39</sup> Letecká informační služba. Doplněk X – Bepilotní systémy. *Aim.rlp.cz* [online]. [cit. 2019-11-5]. Dostupné z WWW: < <https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-2/data/effective/doplX.pdf> >.



*leteckých veřejných vystoupení a soutěží, včetně příprav na ně, jsou-li přijata přiměřená opatření proti ohrožení dle ustanovení 3.*<sup>40</sup>

Jelikož v každé z členských zemí EU jsou pravidla létání s bezpilotními prostředky řešeny nezávisle, rozhodl se Evropský parlament sjednotit tato pravidla. Ta tak budou ve všech zemích vycházet ze stejných nařízení. Zavádí se speciální zóny i kategorie dronů. Návrh pravidel Evropské unie pro provozování dronů vypracovala evropská agentura pro bezpečnost letectví EASA.

Dne 12. března 2019 přijala Evropská komise celounijní pravidla obsahující technické požadavky pro drony. V souladu s nařízením o agentuře EASA stanoví tato nová pravidla základní zásady pro zajištění bezpečnosti, ochrany před protiprávními činy a ochrany soukromí a osobních údajů. Jejich cílem je také snížit administrativní zátěž a podpořit inovace. Nařízení rovněž odstraňuje některá pravidla, která by mohla omezovat podnikání. Předpokládá se, že tak bude dosaženo právní jistoty pro odvětví, které zahrnuje velký počet malých a středních podniků a začínajících podniků. Nařízením se dále zavádí přístup k bezpečnosti založený na rizicích a výkonnosti. To znamená, že zohledňuje různá rizika spojená s jednotlivými odvětvími civilního letectví. Například vrtulníky nebo lehká sportovní letadla podléhají jednodušším a levnějším schvalovacím postupům než komerční letadla.<sup>41</sup>

## **4.5 Antidronová ochrana**

Do nedávné doby počítal návrh ochrany perimetru objektu jen do výše doporučeného mechanického zábranného systému a jen několik málo centimetrů nad toto zabezpečení. Nyní, vzhledem k rozvoji technologií, tak jak je uvedeno výše, je nutné počítat se zabezpečením až jednotky stovek metrů nad hranice perimetru. Možnosti realizace této ochrany se vyvíjejí tak jak se vyvíjejí technologie UAV ale jako všechna realizovaná protiopatření jsou často o krok zpět.

---

<sup>40</sup> Letecká informační služba. Doplněk X – Bepilotní systémy. *Aim.rlp.cz* [online]. [cit. 2019-11-5]. Dostupné z WWW: < <https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-2/data/effective/doplX.pdf> >.

<sup>41</sup> Evropská rada. Drony: reforma bezpečnosti letectví v EU. *Consilium.europa.eu* [online]. [cit. 2020-03-2]. Dostupné z WWW: < <https://www.consilium.europa.eu/cs/policies/drones/> >.

Obr. 2: Příklad současného střežení perimetru<sup>42</sup>



Současné systémy protidronové ochrany jsou velmi finančně nákladné a jsou tak realizovány jen u objektů kde by výskyt dronů mohl ohrozit životy nebo zdraví případně způsobit vysoké materiální škody například letiště, jaderné elektrárny a jiná kritická infrastruktura. Vzhledem k poměrně jednoduché možnosti zneužití i komerčně prodávaných dronů bude instalací obranných systémů přibývat. Dron je již dnes možné, kromě narušování letového provozu a vstupování do soukromí druhých, použít k pašování, přenášení zbraní a drog, špionáži, zakládání požárů i páchání teroristických útoků. Nebezpečí nehrozí jen perimetru objektů ale i v místech s velkou koncentrací osob – sportovní utkání, velká shromáždění, kulturní akce apod. Zde nehrozí jen samotný pád stroje ale i úmyslný útok prostřednictvím dronu – zanesení výbušniny, chemikálie, biologických materiálů.

Ochranu proti dronům můžeme rozdělit na dvě základní kategorie:

- Monitorování;
- Protiopatření.

Monitorovací systém může být buď pasivní, nebo aktivní, případně využívá obou přístupů. Pasivní systémy zaznamenávají a vyhodnocují signály v různých pásmech kmitočtového spektra, akustické signály a pomocí kamer případně termokamer sledují střežený prostor. Aktivní systémy vysílají signály a analyzují jejich odrazy.

<sup>42</sup> Dedrone. Products Overview. *dedrone.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: <<https://www.dedrone.com/products/counter-drone-solution>>.

Systémy by měly plnit jednotlivé funkce:

- detekce – zjištění pohybu dronu v definované oblasti;
- klasifikace – rozpoznání dronu, eliminace falešných poplachů detekcí jiných pohybujících se objektů;
- identifikace – identifikace typu detekovaného zařízení, například podle analýzy radiové komunikace mezi dronem a ovladačem;
- vyhledání a sledování – například 3D mapování pohybu dronu a určení polohy jeho pilota;
- varování – provázanost s dalšími systémy ochrany, zajištění předání informace a aktivace systému protiopatření.

#### **4.5.1 Radiofrekvenční analyzátory**

Systém je vybaven analyzátory radiofrekvenčního spektra a anténním systémem. Neustále dochází ke skenování kmitočtových pásem a nově zachycené signály jsou analyzovány a porovnávány s knihovnou signálů známých dronů. V případě nově zachyceného signálu jsou aktivovány další součásti systému. Pro lokalizaci polohy jsou použity soustavy vhodně rozmístěných antén pro účely triangulace, případně systém obsahuje speciální vyhledávací směrové antény. Je tak možné lokalizovat polohu dronu i polohu pilota. Detekce může být obtížná v městských aglomeracích, kde je velké využití kmitočtového spektra. Nemožná je detekce dronu, který letí na předem definovaných trasách a není tak nutná komunikace mezi UAV a pilotem.

#### **4.5.2 Detekce prostřednictvím mikrofónů**

Jedná se o další z možných částí antidronového detekčního systému. Zařízení detekuje dron na základě analýzy zaznamenávaných audio signálů z instalovaných mikrofónů. V praxi je to řešeno sadou mikrofonních polí ve spojení s počítačovou analýzou. Ta umožňuje nejen samotnou detekci ale také vyhodnocení polohy zdroje akustického signálu – dronu. Akustickou analýzu lze obtížně použít v místech s hlučným prostředím, jako jsou letiště a městská zástavba.

### **4.5.3 Radarové detektory**

Soustava vysílače a přijímače radiofrekvenčních signálů s kmitočtem několik GHz, který v definovaném sektoru (až 360°) vysílá krátké pulzy a vyhodnocuje signály odražené od překážek. Pokročilou analýzou je možné omezit výskyt planých poplachů. Speciální antidronové radarové systémy umožňují detekovat a lokalizovat i menší cíle. Tyto detektory jsou do systémů doplněny pro detekci autonomních dronů.

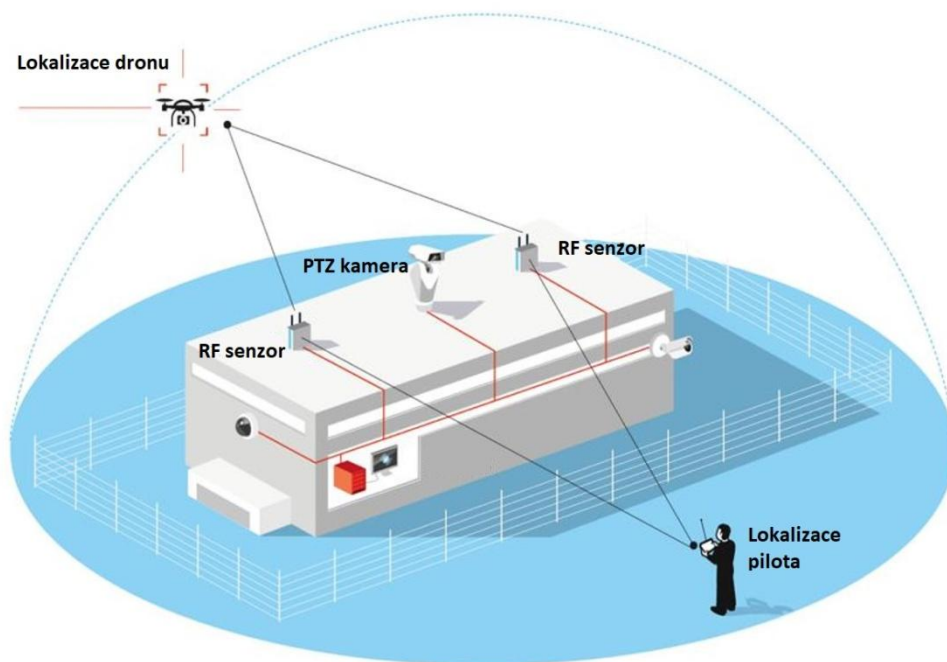
### **4.5.4 Optické detektory**

Jedná se o otočné kamerové systémy snímající střežený prostor ve viditelném spektru, které jsou pro možnost detekce za snížené viditelnosti a v noci doplněny termokamerou. Za detekci a eliminaci falešných poplachů odpovídají analytické video nástroje. Systém zaznamenává pohyb dronu a dokumentuje jeho letovou trasu.

### **4.5.5 Příklady antidronových systémů**

Dedrone – bezpečnostní systém Dedrone je automatické řešení proti dronům navržený tak, aby pasivně detekoval, klasifikoval a omezoval hrozby založené na dronech. Zaznamenané radiofrekvenční signály jsou zpracovávány a vyhodnocovány pomocí inteligentního softwaru DroneTracker. Následuje porovnávání a analýza zpracovaných dat, která klasifikuje blížící se drony a spouští poplachy varující bezpečnostní personál.

Obr. 3: Dedrone system<sup>43</sup>



Základem systému jsou radiofrekvenční detektory vhodně rozmístěné ve středu objektu. Jednotlivé senzory jsou schopny detekovat dron a pilota v okruhu až 2 kilometrů. Další součástí jsou PTZ kamery s integrovaným zoomem, to umožňuje detekci i malých dronů na velké vzdálenosti. Systém může být dále doplněn radarovými senzory

Obr. 4: Prvky systému Dedrone<sup>44</sup>



Dedrone využívá systém inteligentního učení, který je schopný rozpoznat drony všeho druhu. Díky velké databázi, která je neustále rozšiřována, dokáže rozlišit mezi modely dronů a detekovat rozdíl mezi drony a jinými pohyblivými objekty, jako jsou

<sup>43</sup> Dedrone. Products Overview. *dedrone.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://www.dedrone.com/products/counter-drone-solution> >.

<sup>44</sup> Dedrone. Hardware to Protect against Drones. *dedrone.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://www.dedrone.com/products/hardware> >.

ptáci, letadla nebo jiné objekty. Zaznamenané identifikační znaky jednotlivých dronů jsou aktualizovány prostřednictvím cloudu, což umožňuje systému Dedrone chránit objekty před nejnovějšími hrozbami.

AARTOS X7 Advanced – antidronový systém od německé společnosti Aaronia AG. Jedna s několika možných konfigurací systému jehož jádrem jsou rychlé spektrální analyzátoary a multisektorové vyhledávací antény s detekčním dosahem 3 až 7 kilometrů. Vše je propojeno s řídicím centrem, kde jsou signály vyhodnocovány a porovnávány se signály uloženými v knihovnách pro identifikaci detekovaného UAV. Na základě úrovní signálů z jednotlivých sektorů antén je určen pohyb dronu.

Obr. 5: AARTOS X7<sup>45</sup>

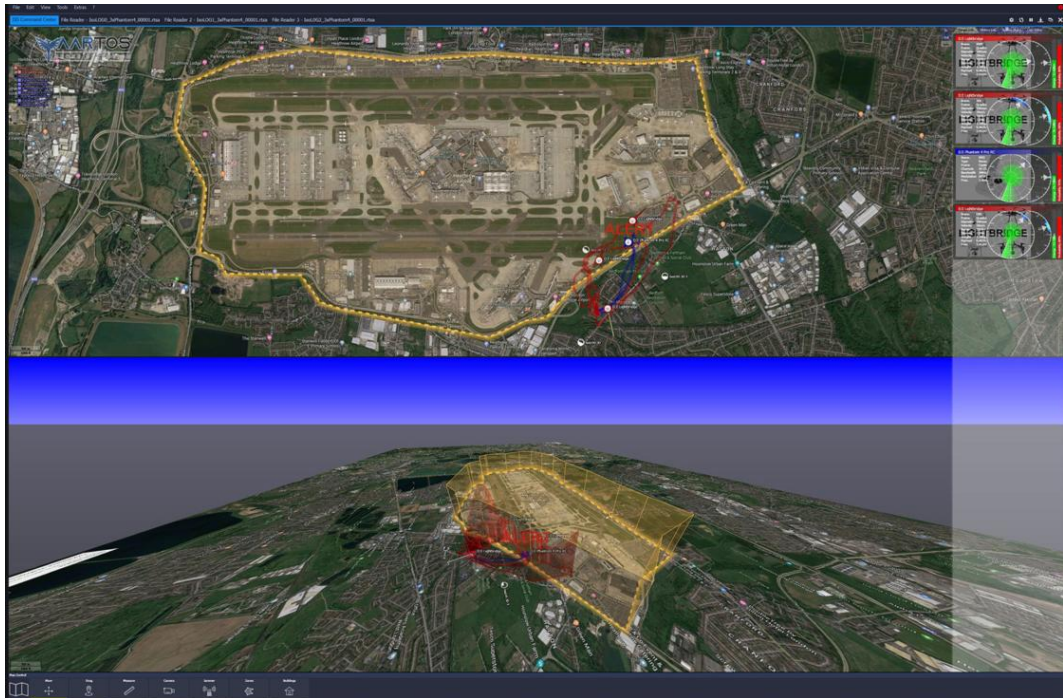


I v tomto případě mohou být do systému zapojeny další detektory - PTZ kamery a radary. Kamery umožňují sledování v oblasti viditelného a infračerveného spektra. To umožňuje dále sledovat dron i v případě přechodu do autonomního módu letu a identifikace potenciálně nebezpečného zatížení dronu. Do systému lze doplnit jakýkoli radar dle potřeb zákazníka. Plně integrovaný radar systému AARTOS umožňuje určit a zobrazit přesnou polohu, směr letu, nadmořskou výšku, rychlost a klasifikaci dronu. Všechny trasy jsou zobrazeny v reálném čase a v 3D zobrazení. Je možné definovat více střežených oblastí

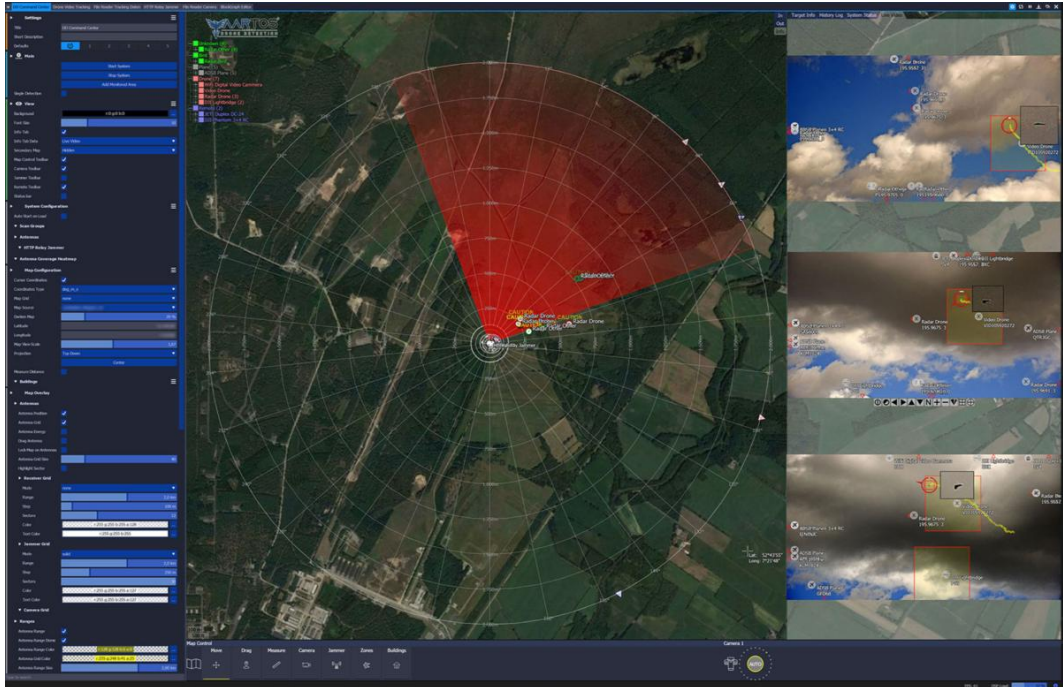
<sup>45</sup> AARTOS DDS. Drone-detection-system. *drone-detection-system.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://drone-detection-system.com/aartos-dds/product-overview/>>.



Obr. 6: Náhled vyhodnocovacího software<sup>46</sup>



Obr. 7: Zpracování výstupu z PTZ kamer v reálném čase<sup>47</sup>



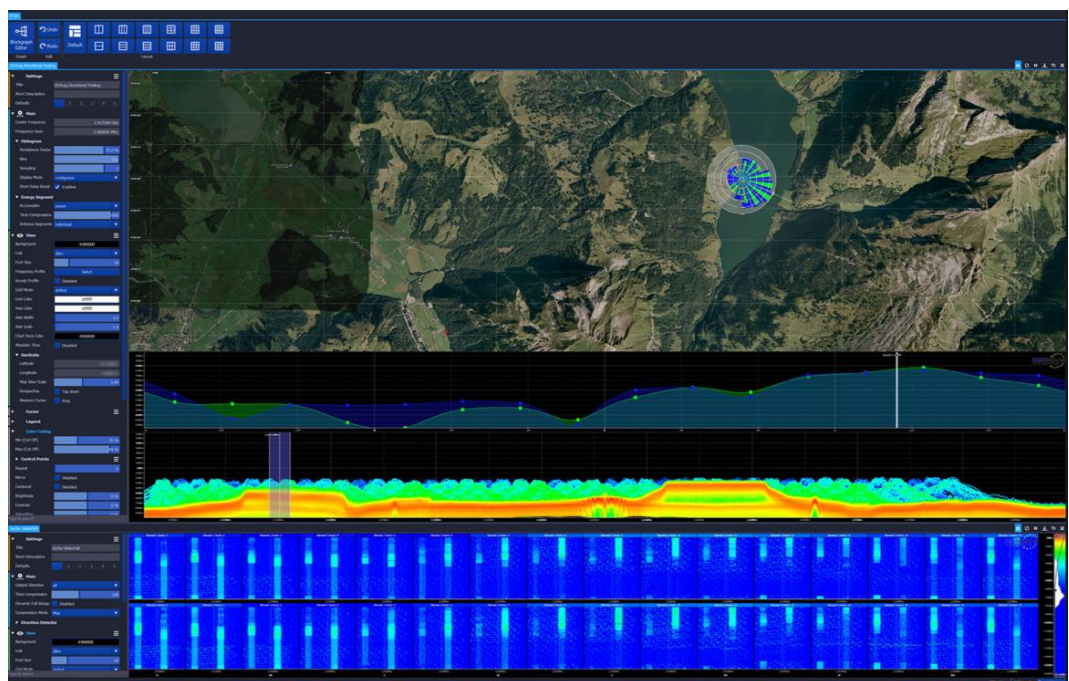
<sup>46</sup> AARTOS DDS. Drone-detection-system software integration. *drone-detection-system.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://drone-detection-system.com/aartos-dds/software-integration/>>.

<sup>47</sup> AARTOS DDS. Drone-detection-system software integration. *drone-detection-system.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://drone-detection-system.com/aartos-dds/software-integration/>>.

Obr. 8: Integrace radaru ve 3D<sup>48</sup>



Obr. 9: Směrové vyhledávání na různých kmitočtech<sup>49</sup>



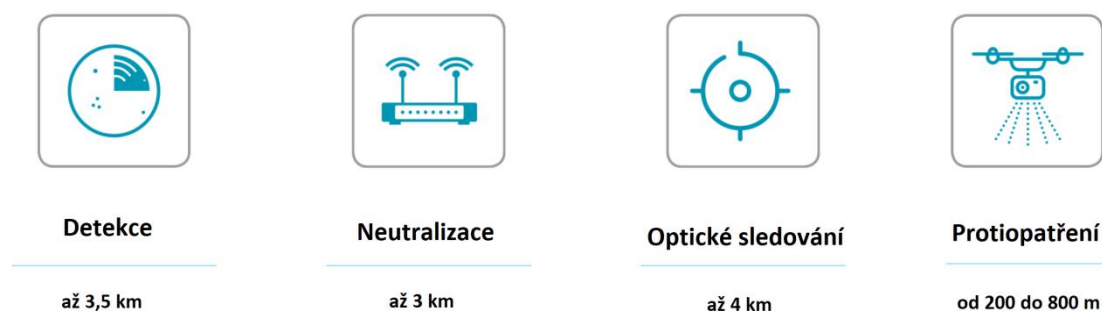
<sup>48</sup> AARTOS DDS. Drone-detection-system software integration. *drone-detection-system.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://drone-detection-system.com/aartos-dds/software-integration/>>.

<sup>49</sup> AARTOS DDS. Drone-detection-system software integration. *drone-detection-system.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://drone-detection-system.com/aartos-dds/software-integration/>>.



SKYLOCK – komplexní ochrana proti dronům. Tento systém nabízí víceúrovňovou ochranu. Jedná se o komplexní systém i s řešením protiopatření v případě detekce dronu. Detekce je založena na lehkém radarovém systému, který je možné instalovat i v obydlených oblastech, je schopen detekovat i malé drony s malou rychlostí a v malé výšce. Určuje vzdálenost, výšku, azimut a rychlost. Je schopen sledovat až 200 cílů současně. Další součástí systému je pasivní radiofrekvenční detektor s anténním systémem tvořeným několika směrovými anténami pro pokrytí 360° a elektrooptický kamerový systém pro sledování oblasti ve viditelném infračerveném spektru.

Obr. 10: SKYLOCK<sup>50</sup>



Systém SKYLOCK nabízí několik možných protiopatření v případě detekce dronu a jeho pohybu v blízkosti zabezpečeného prostoru:

- rušení jednotlivých komunikačních kanálů a signálu GPS;
- detekce operátora – vyhodnocením signálů z 24 směrových antén je lokalizován pilot dronu;
- aktivace dronu, který pomocí vystřelovací sítě odchytil neautorizovaný UAV;
- laserové dělo s dosahem až 800 m;
- automatické zbraňové systémy.

<sup>50</sup> SKYLOCK. Anti Drone Systems *Skylock1.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: <<https://www.skylock1.com>>.

## 5 Nové technické prostředky perimetrické ochrany

Za několik posledních let došlo k velkému pokroku ve vývoji nových technologií využitelných pro zabezpečení perimetru a ke zvyšování dostupnosti v minulosti velmi drahých technických prostředků. Ty je tak možné využít i pro zabezpečení komerčních objektů. Velký pokrok nastal v oblasti termálních kamer, radarů, využití laserů, optických vláken a pokročilých softwarových nástrojů pro analýzu obrazu.

### 5.1 Termokamery

Základním prvkem termokamery je bolometr. Jedná se o pásek z materiálu, jehož elektrický odpor se mění v závislosti na teplotě (obvykle se používají oxidy vanadia nebo amorfní křemík). Snímací pásek se v prostoru bolometrického čipu umísťuje na tepelně izolační nosníky a to tak aby jeho plocha byla vystavena dopadajícímu měřenému záření. Cyklickým měřením odporu materiálu lze stanovit teplotu, která je zdrojem dopadajícího záření. V termokamerách je bolometrická čip složený z jednotlivých mikrobolometrů uspořádaných do maticového formátu určujícího rozlišení kamery. Obvykle se využívá rozlišení 320 x 240, 640 x 480 a u nejmodernějších termokamer pak rozlišení 1240 x 960. Při dopadajícím záření s různou teplotou na čip bolometru jsou elektrické odpory jednotlivých pixelů rozdílné a lze jim dle nastavení přiřadit různé odstíny šedi, případně využít jiných definovaných barevných palet a vzniká tak termografický obraz odpovídajícího rozlišení.<sup>51</sup> Podobně jako je tomu u klasické kamery, vyžaduje termokamera optickou soustavu, která obraz sledovaného prostoru zaostří na čip bolometru. V optické soustavě však v případě termokamery nelze použít sklo, to tepelné záření absorbuje, čočky pro termokamery jsou vyráběny z germánia. To je propustné pro tepelné záření a naopak viditelné záření nepropouští a eliminuje tak možné zkreslení. Velkou výhodou použití termokamery je schopnost zobrazovat objekty nebo osoby v úplné tmě, mlze, prachu nebo kouři. Díky tomu, že atmosféra tlumí viditelné záření podstatně více než záření tepelné, je možné pomocí termokamery rozeznat osoby nebo vozidla na mnohem větší vzdálenost. Další výhodou je skutečnost, že teplotní kontrast lze odstranit podstatně hůře, než kontrast

---

<sup>51</sup> BURDA, K. *Základy elektronických zabezpečovacích systémů*. 1. vyd. Brno : Akademické nakladatelství CERM, 2017. 108s. ISBN 978-80-7204-967-7.

barevný tzn. maskovaná osoba ukrytá v porostu je běžnou kamerou těžko detekovatelná, avšak teplotní kontrast obličeje umožňuje detekci pomocí termálního zobrazení.<sup>52</sup>

Obr. 11: Srovnání zobrazení scény termální a klasickou kamerou<sup>53</sup>



Pro využití odpovídajícího typu termokamery pro její aplikaci do bezpečnostního systému je důležité vědět, jak daleko kamera uvidí. Zde je možné využít Johnsonova kritéria. John Johnson byl vědec vojenských laboratoří, který byl průkopníkem ve zkoumání nočního vidění. Prováděl řadu pokusů a experimentů kde sledoval schopnosti identifikace cílů pomocí analogových senzorů.<sup>54</sup> Byly určeny tři základní definice pro zobrazení cíle a to:

- detekce – schopnost rozlišit objekt na pozadí – minimálně pokrytí 1,5 obrazových bodů;
- rozpoznání – schopnost určit, o jaký druh objektu se jedná, tzn. definovat, zda se jedná o zvíře, osobu, vozidlo, loď a podobně. Nutnost pokrytí minimálně 6 obrazových bodů;
- identifikace – vychází z primárního armádního nasazení, kde znamená, že je reálně možné určit, zda se jedná o „přátelský“ nebo „nepřátelský“ objekt. Pro tuto hranici rozpoznání je nutné pokrytí alespoň 12 obrazových bodů.<sup>55</sup>

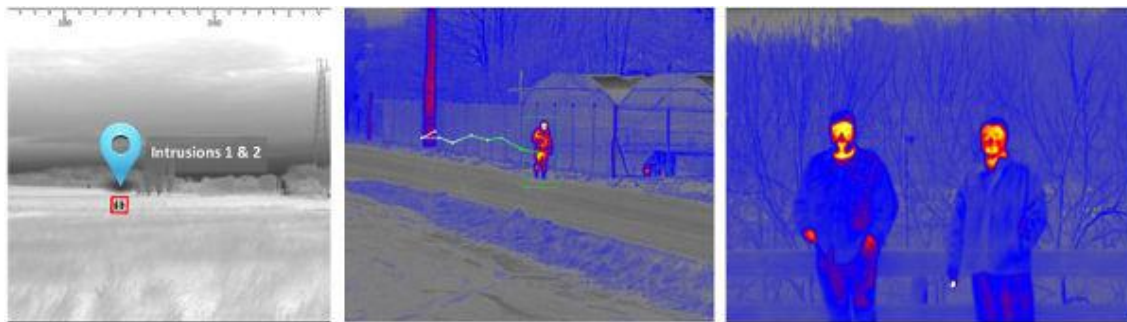
<sup>52</sup> BURDA, K. *Základy elektronických zabezpečovacích systémů*. 1. vyd. Brno : Akademické nakladatelství CERM, 2017. 109s. ISBN 978-80-7204-967-7.

<sup>53</sup> Axis. Thermal imaging. *Axis.com* [online]. [cit. 2020-1-3]. Dostupné z WWW: <<https://www.axis.com/technologies/thermal-imaging/>>.

<sup>54</sup> HGH. Definition of DRI Detection Recognition Identification. *hgh-infrared.com* [online]. [cit. 2020-1-1]. Dostupné z WWW: <<https://www.hgh-infrared.com/FAQ/Perimeter-Security/Definition-of-DRI-Detection-Recognition-Identification-ranges>>.

<sup>55</sup> JINDRA, J. Jak daleko uvidím termokamerou? *ABBAS.cz* [online]. BRNO : ABBAS, 2019. 26. října 2012 [cit. 2020-1-1]. Dostupné z WWW: <<http://www.abbas.cz/clanky/recenze-technika/jak-daleko-uvitim-termalni-kamerou/>>.

Obr. 12 : Příklady detekce, rozpoznání a identifikace cílů<sup>56</sup>



Levý obrázek – na několik kilometrů jsou detekovány na pozadí dva cíle.

Prostřední obrázek – rozpoznání člověka kráčejícího podél plotu.

Pravý obrázek – identifikace dvou mužů (kalhoty, sako), jeden kouří.

Dalším faktorem, který má vliv na dosah termokamery je typ použitého bolometrického snímače. Kamery jsou vybaveny buď chlazeným, nebo nechlazeným snímačem. Chlazené kamery jsou dražší, ale jejich citlivost je o jeden řád větší než v případě kamer nechlazených. Typická chlazená termokamera má rozteč mezi středy sousedících pixelů 15 micronů a s odpovídajícím objektivem může být objekt detekován na vzdálenost 2,1 kilometru. V případě nechlazené termokamery je rozteč středů sousedících pixelů 38 micronů (tato rozteč zabezpečuje, aby se sousedící pixely nechlazeného bolometrického čipu navzájem neovlivňovaly) a detekční vzdálenost může dosahovat maximálně 800 metrů.<sup>57</sup>

## 5.2 Optická vlákna

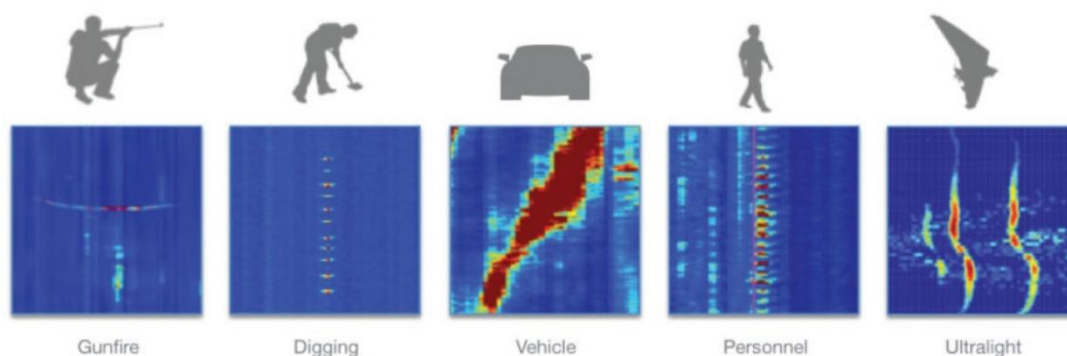
Optická vlákna jsou již mnoho let využívána v komunikacích jako médiu prostřednictvím, kterého lze přenášet velké objemy dat na dlouhé vzdálenosti. Tato vlastnost je samozřejmě široce využívána také v případě zabezpečení perimetrů a to hlavně pro přenos dat pro IP kamerové systémy. Optické vlákno lze však také využít jako samotný detektor narušení perimetru.

<sup>56</sup> HGH. Definition of DRI Detection Recognition Identification. *hgh-infrared.com* [online]. [cit. 2020-1-1]. Dostupné z WWW: <<https://www.hgh-infrared.com/FAQ/Perimeter-Security/Definition-of-DRI-Detection-Recognition-Identification-ranges>>.

<sup>57</sup> JINDRA, J. Jak daleko uvidím termokamerou? *ABBAS.cz* [online]. BRNO : ABBAS, 2019. 26. října 2012 [cit. 2020-1-1]. Dostupné z WWW: <<http://www.abbas.cz/clanky/recenze-technika/jak-daleko-uvitim-termalni-kamerou/>>.

Společnost QinetiQ vyvinula systém, umožňující prostřednictvím běžného optického vlákna detekovat, klasifikovat a přesně lokalizovat řadu činností, včetně pohybu osob, pohybu vozidla, nízko letících letadel, ručního a mechanického kopání, střelby a mnoha dalších činností. Princip činnosti umožňuje Rayleighův rozptyl a reflektometrické měření. Laserový paprsek, vysílaný do optického vlákna, využívá zpětných odrazů od nečistot, které se běžně vyskytují v optickém vláknu. Tím vznikají jemné modulace, které jsou zachycovány ve vyhodnocovací jednotce a jsou dále převáděny na akustický signál.

Obr. 13: Příklad akustické odezvy narušení perimetru<sup>58</sup>

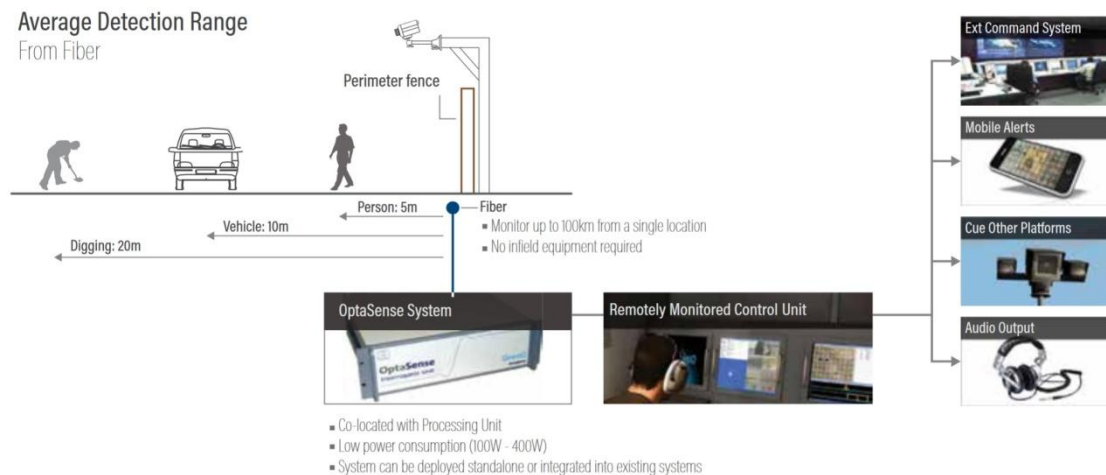


Jednotka do optického vlákna vysílá stabilizovaný puls světla a vytváří tak ve vláknu síť virtuálních mikrofonů. Změnou vysílaného impulsu lze vytvářet virtuální mikrofony v rozestupu 5 až 15 metrů po celé délce vlákna. Spojením vyhodnocovacích jednotek je možné z jednoho místa sledovat trasy dlouhé až 5000 kilometrů.<sup>59</sup>

<sup>58</sup> SECURITY MAGAZÍN. Optické vlákno s ušima dokáže ohlídat až 5000 kilometrů dlouhou trasu. *securitymagazin.cz* [online]. Praha : Security Media. 8. září 2015 [cit. 2020-1-1]. Dostupné z WWW: < <https://www.securitymagazin.cz/security/opticke-vlakno-s-usima-dokaze-ohlidat-az-5000-kilometru-dlouhou-trasu-napriklad-statni-hranice-1404046168.html>>.

<sup>59</sup> RED. Oceňované optické vlákno „s ušima“ dorazilo do Česka. *info.cz* [online]. Praha : CNC. 8. září 2017 [cit. 2020-1-1]. Dostupné z WWW: < <https://www.info.cz/byznys/ocenovane-opticke-vlakno-s-usima-dorazilo-do-ceska-37772.html>>.

Obr. 14: Schematický popis systému OptaSense<sup>60</sup>



Na rozdíl od běžných skrytých senzorů systém OptaSense významně redukuje plané popluchy pomocí přesných algoritmů, které dešifrují a klasifikují typ narušení v reálném čase. Uživatelé jsou na popluchy upozorňováni a s využitím GPS souřadnic může systém přesně určit místo narušení perimetru během několika sekund. Díky tomuto systému lze zvýšit účinnost reakce na detekovaný poplach prostřednictvím fyzické ochrany objektu. Optické vlákno je možné instalovat přímo na oplocení objektu, skrytě pod povrch podél hranice objektu nebo zvolit kombinaci obou možností. Po instalaci vlákna a řídicí elektroniky stačí jen provést kalibraci systému pro přizpůsobení instalovanému prostředí. Veškerá elektronika je uvnitř zabezpečené oblasti a je tak chráněna proti externím vlivům, rušení a podobně. Systém lze také integrovat s ostatními prvky perimetrické ochrany jakou jsou například kamerové systémy.<sup>61</sup>

### 5.3 Laserová technologie – LiDAR

Systém objemové detekce obsahuje laserové vícekanálové detektory LiDAR (16 až 128 paprsků). Laserové paprsky jsou rozptřeny do jednotlivých oblastí s poloměrem dosahu detektorů až 300 m. Detektor vyhodnocuje doby odrazů od pevných překážek a na základě měření doby odrazu vypočítá vzdálenost překážek od

<sup>60</sup> OptaSense. Protecting critical infrastructure and assets. *Optasense.com* [online]. [cit. 2020-1-1]. Dostupné z WWW: < <https://www.optasense.com/security/intrusion-detection/#1480955481921-4d02179a-4e7d>>.

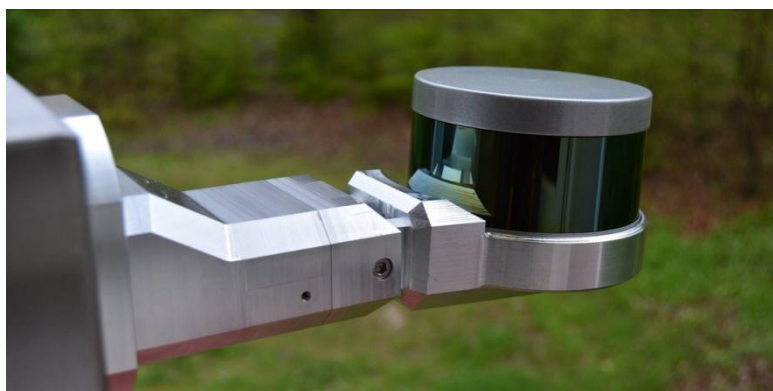
<sup>61</sup> OptaSense. Protecting critical infrastructure and assets. *Optasense.com* [online]. [cit. 2020-1-1]. Dostupné z WWW: < <https://www.optasense.com/security/intrusion-detection/#1480955481921-4d02179a-4e7d>>.



detektoru. Jeden detektor provádí několik set tisíc měření za sekundu s přesností detekce 2 až 3 cm.

Perimetrický bezpečnostní systém využívající tuto technologii dokáže na rozdíl od konvenčních systémů, které obvykle chrání jen perimetry, střežit celou oblast hlídaného prostoru. Pokud narušitel vstoupí do chráněné oblasti, systém je o tom informován. Obsluha bude mít informace o přesné poloze, velikosti a rychlosti jeho pohybu. Zaznamenána bude také celá trajektorie pohybu sledovaného objektu. Systém umožňuje sledovat velké množství cílů současně. Zobrazení a detekce probíhá ve 3D prostoru, je zde možné definovat jednotlivé zóny střežení a to i povolené průchody napříč střeženou zónou. Pro eliminaci falešných poplachů je možné v každé střežené zóně maskovat objekty, které mohou být jejich zdrojem (stromy, keře, vzrostlá tráva apod.).<sup>62</sup>

Obr. 15: Objemový detektor LiDAR od společnosti Velodyne<sup>63</sup>



Systém obsahuje pokročilé systémy pro plánování a návrh zabezpečení perimetru a to i ve 3D prostředí které věrně napodobuje reálný střežený prostor. Do něj je možné přímo vkládat jednotlivé detektory se zobrazením jednotlivých detekovaných oblastí. Technologie umožňuje automatické provázání s PTZ kamerami, které se automaticky zaměřují na místo generovaného poplachu.

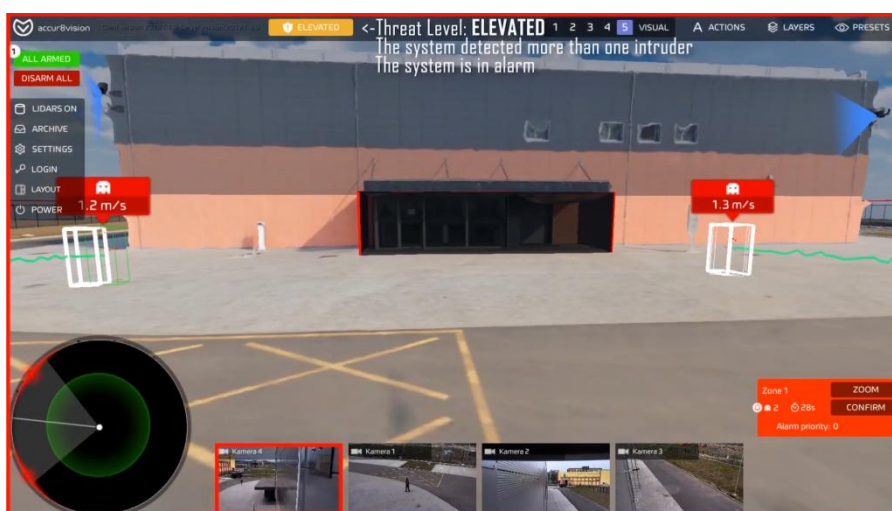
<sup>62</sup> Tacticaware. About Accur8vision. *Accur8vision.com* [online]. [cit. 2020-1-3]. Dostupné z WWW: <<https://accur8vision.com/>>.

<sup>63</sup> Velodyne. Products. *Velodynelidar.com* [online]. [cit. 2020-1-1]. Dostupné z WWW: <<https://velodynelidar.com/products/>>.

Obr. 16: Příklad zobrazení objemové detekce systémem Accur8vision<sup>64</sup>



Obr. 17: Zobrazení trajektorie narušení střežené zóny v systému Accur8vision<sup>65</sup>



## 5.4 Radarová technologie

Radar je technologie pro detekci objektů. Byl vyvinut pro vojenské použití ve čtyřicátých letech minulého století, ale nyní je široce používán v civilních aplikacích, například předpovědi počasí, sledování silničního provozu, prevenci kolizí v letectví a lodní dopravě. Radarový systém vysílá signály sestávající z rádiových vln ve vysokofrekvenčním spektru. Když radarový signál zasáhne objekt, signál se odrazí nebo rozptýluje v mnoha směrech. Část signálu je odražena zpět do radarového systému, kde

<sup>64</sup> Tacticaware. About Accur8vision. *Accur8vision.com* [online]. [cit. 2020-1-3]. Dostupné z WWW: <<https://accur8vision.com/>>.

<sup>65</sup> Tacticaware. About Accur8vision. *Accur8vision.com* [online]. [cit. 2020-1-3]. Dostupné z WWW: <<https://accur8vision.com/>>.



bude detekována přijímačem. Zjištěný signál se vyhodnocuje a může být zobrazován nebo dále zpracováván. Díky svým vynikajícím detekčním schopnostem za zhoršených světelných podmínek, například ve tmě a mlze, může být detektor pohybu založený na radarové technologii efektivním doplňkem perimetrických systémů. Obdobné vlastnosti mají i jiné perimetrické detektory, termokamery vybavené videoanalytikou nebo pasivní infračervené detektory, ale detektor založený na radarové technologii může být jejich efektivní alternativou - může poskytnout více informací na delší vzdálenost. Detekční systém založený na radaru detekuje pouze fyzický pohyb ve scéně, ignoruje čistě vizuální efekty, jako jsou stíny nebo světelné odlesky. Eliminuje tak nejčastější plané poplachy indikované kamerovými systémy.

Obr. 18: Radarový detektor AXIS D2050-VE<sup>66</sup>



Detektor pohybu založený výhradně na radaru neposkytuje žádné vizuální potvrzení. Vhodné je tedy kombinace s PTZ kamerou, která je schopna poplach verifikovat a omezit tak plané poplachy. Aby se usnadnila vizuální interpretace scény, může být radarový obraz snadno integrován a kalibrován pomocí nahrané referenční mapy. S detektorem lze v zabezpečovacím systému zacházet jako s kamerou. Měřením časového zpoždění, fázového posunu, frekvenčního posunu a síly jednotlivých odražených signálů systém získává data o umístění, rychlosti, směru a velikosti pohybujícího se objektu.

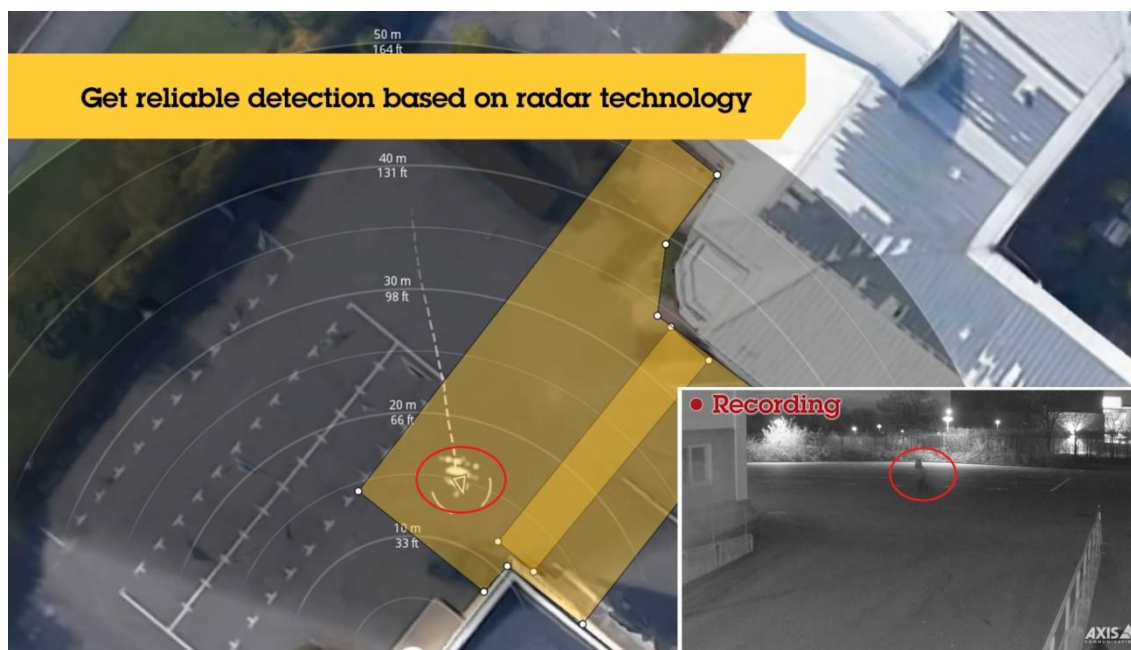
Stejně jako u všech typů detektorů existují i situace, kdy výkon radarového detektoru není zcela optimální. Výkon detekce detektoru se postupně snižuje se vzdáleností a úhlem snímané scény. Malé objekty jsou proto obtížně detekovat na větší vzdálenosti a ve větších úhlech. Přestože detektor může odfiltrovat kymácející se

---

<sup>66</sup> Axis. AXIS D2050-VE Network Radar Detektor. *axis.com* [online]. [cit. 2020-1-3]. Dostupné z WWW: < <https://www.axis.com/products/axis-d2050-ve> >.

nepohyblivé předměty, jako jsou stromy a keře, mohou stále způsobovat falešné poplachy za velmi větrného počasí nebo v případě náhlých porывů větru. Vegetace může také omezit účinnost detekce velmi pomalu se pohybujících objektů.

Obr. 19: Radarový detektor Axis s verifikační PTZ kamerou<sup>67</sup>



## 5.5 Pokročilá videoanalýza

Integrované systémy, které obsahují termovizní a klasické kamery, radary a pokročilý řídicí software, jsou zásadní pro eliminaci různých potenciálních útoků. Společné nasazení poskytuje pokročilý systém detekce narušení perimetru. Například pozemní přehledový radar může detekovat možné hrozby za linií perimetru, když se riziko přibližuje, předává signál kamerám s řízeným natáčením (PTZ), ty jsou tak připraveny k záznamu narušení. Vestavěné analytické funkce pro termální a klasické kamery tak mohou dále identifikovat objekty, informovat oprávněné pracovníky a shromažďovat další důkazy prostřednictvím rozpoznávání obličeje nebo vysoce kvalitních fotografií.

Objekty kritické infrastruktury vyžadují kromě nepřetržitého sledování, také řešení, které poskytuje vysoce spolehlivou detekci narušení s minimálním počtem falešných poplachů. Toto nelze realizovat jinak než s pomocí pokročilé videoanalytiky,

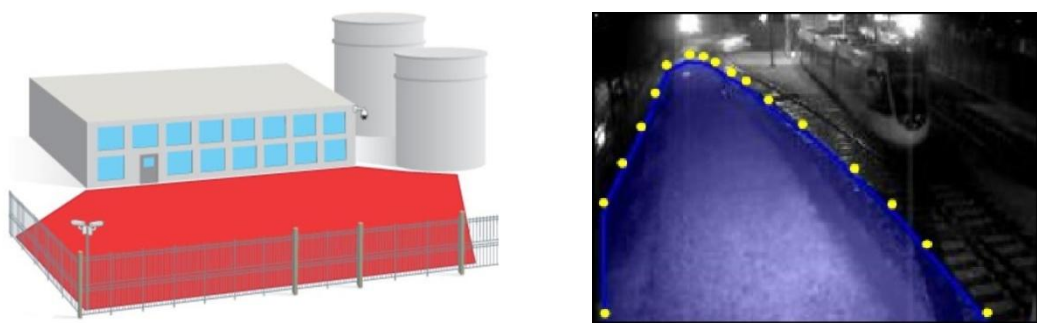
<sup>67</sup> Axis. AXIS D2050-VE Network Radar Detektor. *axis.com* [online]. [cit. 2020-1-3]. Dostupné z WWW: < <https://www.axis.com/products/axis-d2050-ve> >.

kteřá je nezbytná pro jakýkoli účinný a efektivní monitorovací systém. Funkce jako je dynamická detekce událostí a zjednodušená prezentace dat podporuje přesnou analýzu vniknutí a usnadňují odpovídající reakci. Je tak možné prakticky eliminovat falešné popluchy, což umožňuje pracovníkům fyzické ochrany objektu reagovat efektivněji a tak celkově snižovat celkové náklady pro koncového uživatele.

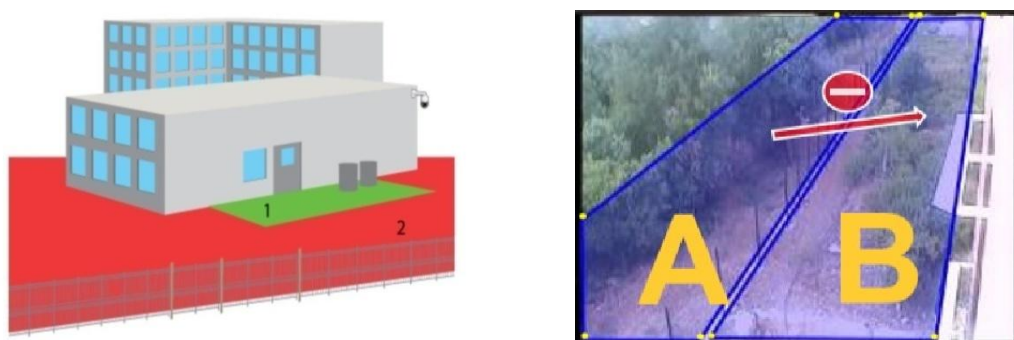
Studie ukázaly, že průměrný člen fyzické ostrahy objektu je schopen udržet dostatečnou pozornost přibližně 20 minut, v případě sledování signálu z kamerového systému s minimální nebo žádnou pohybovou aktivitou. Jakmile uběhne tato doba, jeho koncentrace a pozornost se dále snižuje, čímž se zvyšuje riziko vniknutí do střežených oblastí bez náležité následné reakce odpovědných pracovníků.<sup>68</sup> A právě toto pomáhá řešit videoanalýza za použití různých definovaných scénářů.

Příklady jednotlivých scénářů systému Axis Perimeter Defender (obr. 20 - 24):<sup>69</sup>

Obr. 20: Vstup do zóny



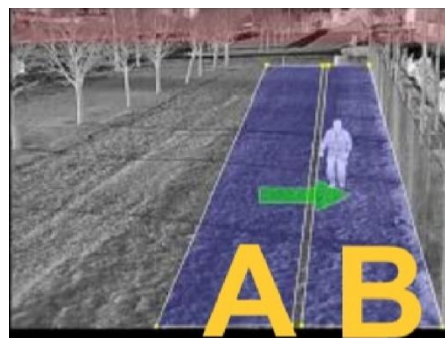
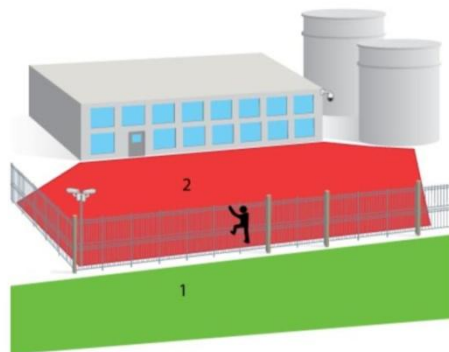
Obr. 21: Vstup přes zónu



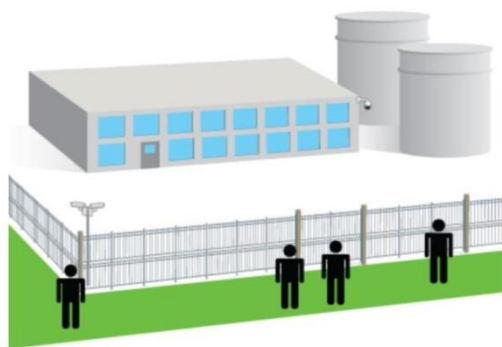
<sup>68</sup> HATTELAND Technology. Intelligent perimeter detection solutions take your security to the next level. *hattelandtechnology.com* [online]. [cit. 2020-1-6]. Dostupné z WWW: <<https://www.hattelandtechnology.com/blog/intelligent-perimeter-detection-solutions-take-your-security-to-the-next-level/>>.

<sup>69</sup> Axis. Axis Perimeter Defender. *axis.com* [online]. [cit. 2020-1-3]. Dostupné z WWW: <<https://www.axis.com/products/axis-perimeter-defender>>.

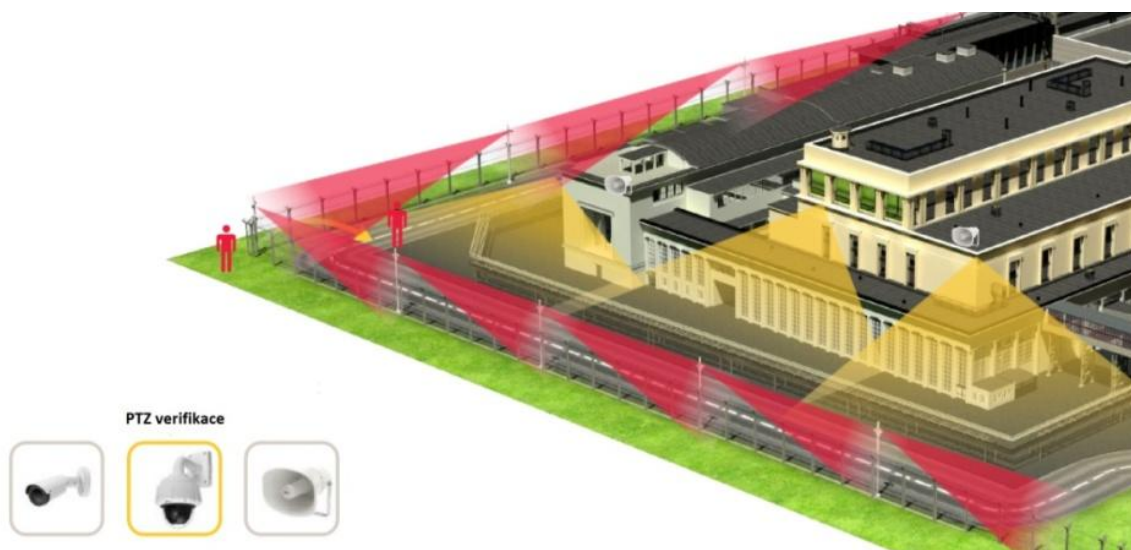
Obr. 22: Přechod zón



Obr. 23: Zdržování se v zóně



Obr. 24: PTZ verifikace





## 5.6 Porovnání kamerového systému klasická/termální technologie

Pro porovnání rozdílu v instalaci kamerového systému sestávajícího z klasických kamer a kamer termálních autor vybral objekt velkokapacitního skladu pohonných hmot nedaleko obce Bělčice na hranicích Jihočeského a Středočeského kraje. Objekt je součástí produktovodní sítě, která se v Čechách začala budovat v roce 1942. Velký rozvoj nastal v období po druhé světové válce, kdy hlavním motorem výstavby a zahušťování produktovodní sítě a skladů pohonných hmot byly strategicko-vojenské plány pro zásobování armády. Výsledkem byla nejhustší produktovodní síť v Evropě a možná i na světě.<sup>70</sup> V období před rokem 1989 byl výše uvedený sklad pohonných hmot přísně střežen příslušníky Československé lidové armády v rámci strážní služby. Areál byl obehnan dvojitým plotem, kde byly jednotlivé sektory střeženy vojáky a služebními psy.

V roce 1994 v rámci privatizačního projektu vznikla společnost ČEPRO, jejímž úkolem je mimo jiné zajištění ochrany státního majetku a státního zájmu v oblasti zásobování pohonnými hmotami v mimořádných situacích. Ta nyní spravuje kromě produktovodů také sklad PHM Bělčice. Rozloha skladu je 122 000 m<sup>2</sup>, v objektu je 19 velkokapacitních nádrží.<sup>71</sup>

Obr. 25: Sklad PHM Bělčice<sup>72</sup>



<sup>70</sup> ČEPRO. *Spolehlivý zdroj od roku 1949*. Poděbrady : Astroprint, 2013. 13-17s.

<sup>71</sup> ČEPRO. *Spolehlivý zdroj od roku 1949*. Poděbrady : Astroprint, 2013. 30s.

<sup>72</sup> Vlastní. Xiaomi Mi Drone 4K

Obr. 26: Sklad PHM Bělčice<sup>73</sup>



Objekt vyžaduje nepřetržité střežení 365 dní v roce a je možné využít celou řadu nástrojů, které jsou uvedeny výše. Vše by mělo být navrženo a instalováno pro spolehlivou a včasnou detekci narušení perimetru střeženého objektu. Obvykle se pro objekt tohoto typu kombinují různé technologie, které se vzájemně doplňují a vytváří bezpečnou hranici střeženého území. Ať už je pro zabezpečení oblasti zvoleno jakékoli řešení nebo technologie, všechny mají své výhody a nevýhody, některé technologie jsou dražší než jiné. Pro získání kompletního přehledu o celkových nákladech pro určité řešení je třeba vzít v úvahu nejen počáteční pořizovací náklady, ale také náklady na instalaci a údržbu. Důležitou kapitolou jsou také požadavky na celkovou spotřebu energií nutnou pro provoz perimetrického zabezpečení. To je třeba hodnotit nejen z pohledu finančních nákladů, ale také ve vztahu k ochraně životního prostředí a to s ohledem na nepřetržitou činnost celého systému 365 dní v roce. Úspora energie bude do budoucna stále důležitější.

### **Vlastnosti srovnávaných systémů perimetrického zabezpečení objektu velkokapacitního skladu PHM Bělčice:**

Uzavřený kamerový systém CCTV instalovaný podél hranice objektu – pro možnost sledování perimetru i za zhoršených světelných podmínek nutno instalovat po celém perimetru osvětlení. Zde je možné využít různé typy světelných zdrojů, vždy je to

<sup>73</sup> Vlastní. Xiaomi Mi Drone 4K

však spojeno s vysokými provozními náklady a náklady na jejich pravidelnou výměnu. Osvětlení musí být navrženo tak, aby nedocházelo k oslnění jednotlivých kamer perimetrického systému. Světlo může proniknout jen do určité vzdálenosti a je problematické zcela osvětlit požadovanou oblast, takže některé prostory mohou zůstat bez dohledu kamer CCTV. Takto vzniklé stíny a prostory mohou poukazovat na možnou cestu útoku narušitele. Osvětlení pomocí LED diod poskytuje ve srovnání s jakýmkoli jiným běžně používaným světelným zdrojem významné úspory spotřeby elektrické energie. LED diody také poskytují dlouhou životnost a nízké náklady na údržbu. Možno také využít infračerveného osvětlení LED.

Výhody:

- Dobrá viditelnost během dne;
- Relativně nízké počáteční náklady.

Nevýhody:

- K pokrytí velkého obvodu je třeba nainstalovat mnoho kamer;
- Omezená detekce v noci. Osvětlení je schopno osvětlit jen určitou plochu – vznik stínů;
- Omezená detekce v mlze, dešti a za zhoršených světelných podmínek;
- Pro instalaci mnoha sloupů pro umístění kamer rozsáhlé stavební práce;
- Vysoká spotřeba energie;
- Vysoké provozní náklady na údržbu osvětlení.

Termovizní kamerový systém - termální zobrazování je dnes široce uznávané jako jedno z nejúčinnějších detekčních řešení. Při použití ve spojení s video analytikou je schopno maximálně eliminovat četnost detekovaných falešných poplachů. Většina využívaných termokamer obsahuje nechlazený termální detektor, neobsahuje tedy žádné pohyblivé součásti, takže nevyžaduje prakticky žádnou údržbu. Technologie tepelného zobrazování nevyžaduje žádné další osvětlení. Kamery disponují vlastní integrovanou video analýzou, čímž vytváří efektivní zařízení pro detekci.

### Výhody:

- Dokonalý přehled o pohybu osob na hranicích objektu;
- Detekce ve dne i v noci;
- Pracuje prakticky za každého počasí;
- Vidí skrz mlhu, déšť, kouř;
- Nízké náklady na údržbu;
- Nízká spotřeba;
- Nemožnost skrytí – tepelný kontrast obtížně maskovatelný;
- Malý počet kamer i pro velké perimetry.

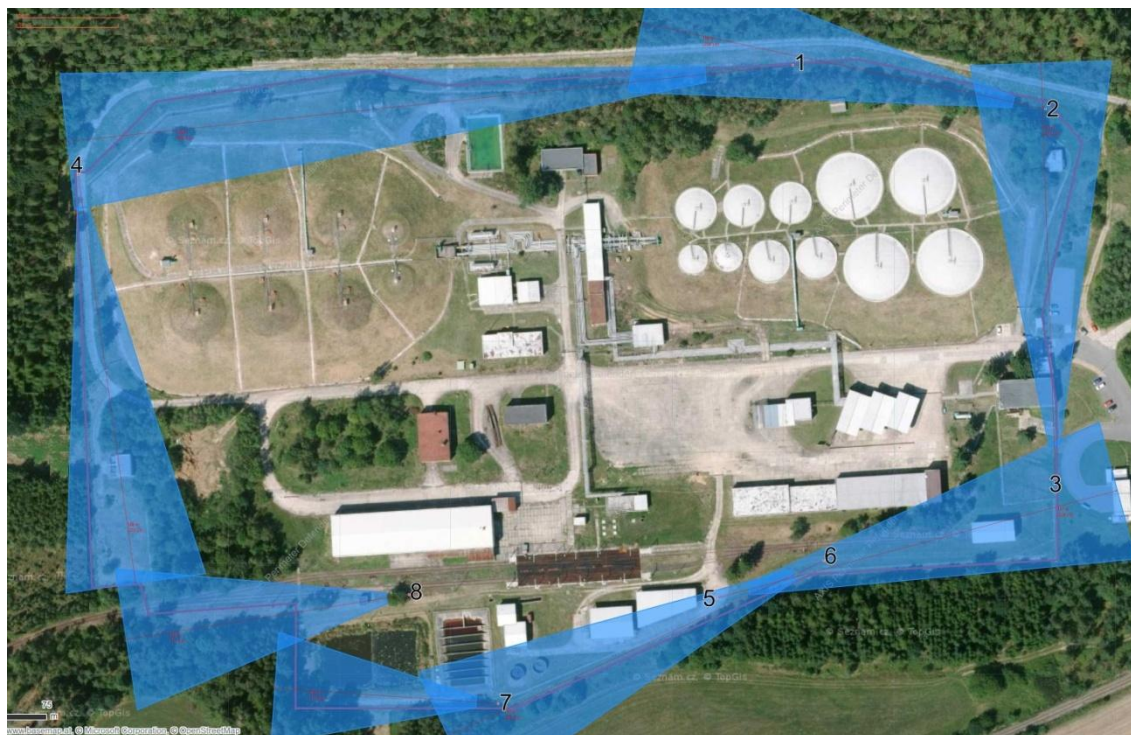
### Nevýhody:

- Narušitel je snadno detekován, ale není identifikován.

Níže autor uvádí možné příklady rozmístění prvků jednotlivých kamerových systémů. V tomto zjednodušeném příkladu nejsou zahrnuty náklady na personál a vybavení během instalace, náklady na údržbu a provoz. Návrh rozmístění jednotlivých prvků kamerového systému byl proveden v aplikaci Design Tool for AXIS Perimeter Defender. Ta umožňuje vytvořit virtuální model zabezpečené oblasti a definovat jednotlivé součásti kamerového systému s požadovanými vlastnostmi. Pro návrh termálního kamerového systému byly vybrány termokamery AXIS Q1941-E s objektivem s ohniskovou vzdáleností pro požadovaný dosah a konkrétní místo instalace. Jedná se o nechlazenou termografickou IP kameru s rozlišením 384 x 288 obrazových bodů. S objektivem 35 mm dokáže kamera rozpoznat pohyb osoby na 1028 metrů.



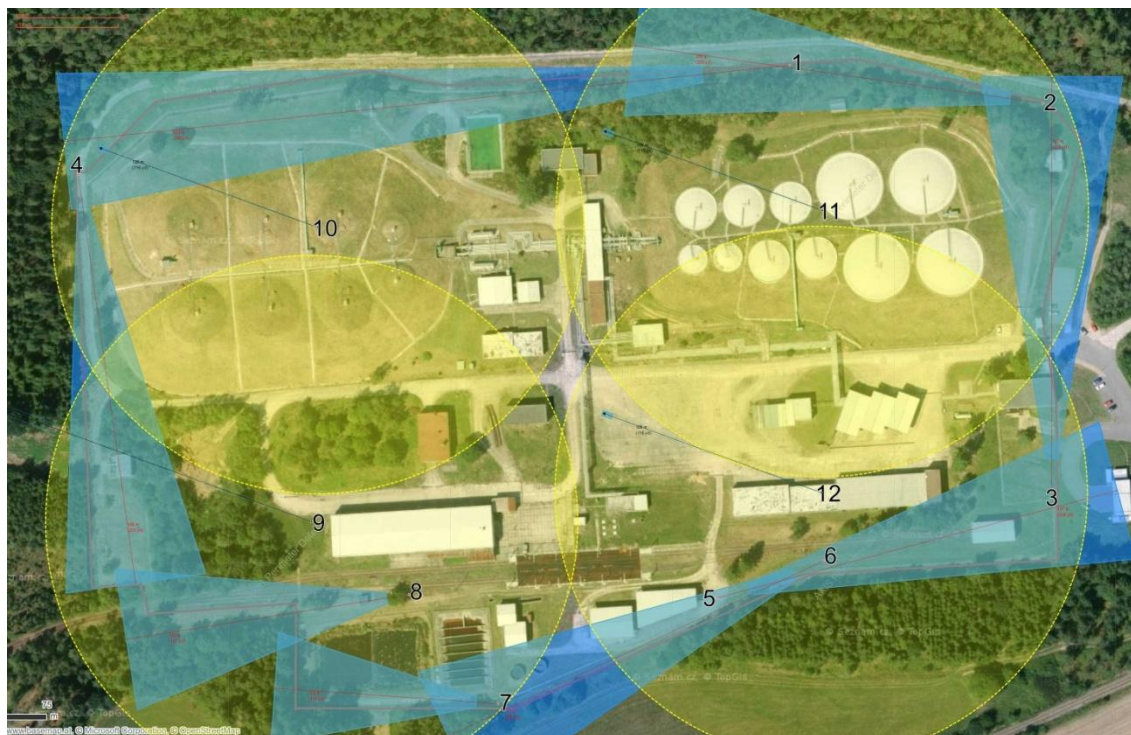
Obr. 27: Návrh termálního kamerového systému pro zabezpečení skladu PHM Bělčice<sup>74</sup>



V případě termokamer je maximální dosah zobrazen pro osobu velikosti 1,7 metru pokrývající 11 obrazových bodů. Dle Johnsonova kritéria to odpovídá bezpečnému rozpoznání osoby (nad 6 obrazových bodů). Celkový perimetr areálu tak pokrylo 8 kamer s možností pokročilé videoanalýzy a možností vazby na PTZ kamery pro možnost následné verifikace a automatického sledování pohybujících se objektů v zorném poli kamery.

<sup>74</sup> Vlastní. Vytvořeno prostřednictvím Design Tool For AXIS Perimeter Defender.

Obr. 28: Návrh termálního kamerového systému s PTZ kamerami<sup>75</sup>



Na obr. 28 je návrh doplněn 4 x PTZ kamerou AXIS Q6052-E. Jedná se o venkovní IP kameru s rozlišení 720 x 576 bodů s 36x optickým zoomem a 12x digitální zoom. Kamera má ultra-rychlý polohovací systém s okamžitým zaostřováním na definovanou plochu. Disponuje řadou inteligentních video funkcí jako je detekce pohybu v obraze a automatické sledování, přesun do předvolené pozice v případě pohybu v zóně a další. Zobrazení pokrytí v návrhu konfigurace kamerového systému na obr. 28 odpovídá schopnosti rozpoznání tváře sledované osoby (ne její identifikace).

AXIS Q1941-E 35 mm – termální IP kamera č. 1, cena 98 394,- Kč

AXIS Q1941-E 19 mm – termální IP kamera č. 2 – 6, cena 72 494,- Kč

AXIS Q1941-E 13 mm – termální IP kamera č. 7 a 8, cena 72 494,- Kč.

**Celková cena navržených termálních kamer – 605 852,- Kč**

AXIS Q6052-E – PTZ IP kamera č. 9 - 12, cena 67 314,- Kč.<sup>76</sup>

<sup>75</sup> Vlastní. Vytvořeno prostřednictvím Design Tool For AXIS Perimeter Defender.

<sup>76</sup> IPSECURE. IP kamery. [IPsecure.cz](http://IPsecure.cz) [online]. [cit. 2020-1-8]. Dostupné z WWW: <https://www.ipsecure.cz/ip-kamery/>.

Obr. 29: Termální IP kamera AXIS Q1941-E<sup>77</sup>



Obr. 30: PTZ IP kamera AXIS Q6052-E<sup>78</sup>



Návrh klasického kamerového systému v případě stejného areálu představuje instalaci devatenácti IP kamer pro potřebu pokrytí perimetru celého areálu. V návrhu autor použil kamery AXIS Q1615-E Mk II. Jedná se venkovní bezpečnostní IP kameru s rozlišením 1920 x 1080 obrazových bodů, snímacím CMOS senzorem s progresivním skenováním a kompresí videa H.264 a MJPEG. Světelnost objektivu je F 1,2.

---

<sup>77</sup> Axis. Axis Q1941-E Thermal Network Camera. *axis.com* [online]. [cit. 2020-1-8]. Dostupné z WWW: < <https://www.axis.com/products/axis-q1941-e>>.

<sup>78</sup> Axis. Axis Q6052-E PTZ Network Camera. *axis.com* [online]. [cit. 2020-1-8]. Dostupné z WWW: < <https://www.axis.com/products/axis-q6052-e>>.



Obr. 31: Návrh klasického kamerového systému pro zabezpečení skladu PHM Bělčice<sup>79</sup>



AXIS Q1615-E Mk II – IP kamera č. 1 - 19, cena 33 644,- Kč<sup>80</sup>

**Celková cena navržených IP kamer – 639 236,- Kč**

Obr. 32: IP kamera AXIS Q1615-E<sup>81</sup>



<sup>79</sup> Vlastní. Vytvořeno prostřednictvím Design Tool For AXIS Perimeter Defender.

<sup>80</sup> IPSECURE. IP kamery. *IPsecure.cz* [online]. [cit. 2020-1-8]. Dostupné z WWW: <https://www.ipsecure.cz/ip-kamery/>.

<sup>81</sup> Axis. Axis Q1615-E Mk II Network Camera. *axis.com* [online]. [cit. 2020-1-8]. Dostupné z WWW: <<https://www.axis.com/products/axis-q1615-e>>.

I v tomto případě je vhodné instalovat PTZ kamery pro možnost verifikace, efektivního zásahu fyzické ostrahy a dokumentace pohybu narušitele po areálu objektu.

AXIS Q6052-E – PTZ IP kamera č. 9 - 12, cena 67 314,- Kč<sup>82</sup>

Ačkoli všechny technologie mají výhody a nevýhody, tento příklad možného rozmístění jednotlivých prvků kamerového systému perimetrické ochrany objektu velkokapacitního skladu PHM Bělčice ukazuje, že využití termálního zobrazování je velmi dobrým a nákladově efektivním řešením pro ochranu perimetru, zejména pokud je třeba tento obvod, stejně jako prakticky ve všech případech, chránit během noci a za zhoršených světelných podmínek. V případě instalace termálního kamerového systému se dají očekávat výrazně nižší náklady na samotný provoz obvodové ochrany uvedeného objektu a to nejen náklady na údržbu ale hlavně výrazně nižší náklady na potřebné energie. Přestože je jediná termovizní kamera nákladnější než kamera CCTV, je potřeba na pokrytí stejné oblasti použít méně kamer. Stavební práce, které je třeba provést, jsou také minimalizovány. V některých případech mohou být kamery namontovány na stávající struktury. Vzhledem k tomu, že termovizní kamery vytvářejí jasný obraz i za nejtemnější noci, není třeba instalovat žádné další doplňkové technologie, jako je osvětlení nebo infračervené přisvícení. To nejen omezuje množství stavebních prací, které je třeba provést, ale také dále snižuje náklady na údržbu.

---

<sup>82</sup> IPSECURE. IP kamery. *IPsecure.cz* [online]. [cit. 2020-1-8]. Dostupné z WWW: <https://www.ipsecure.cz/ip-kamery/>.

## Závěr

Cílem práce bylo seznámit s historií zabezpečovací techniky a současně využívanými technologiemi pro ochranu perimetru objektů. Technických prostředků, které lze k zabezpečení využít, je dnes velké množství. Při jejich začlenění do návrhu bezpečnostního systému je ale nutno zvážit velké množství detailů, které vycházejí z navrhovaných technických zařízení, možných variant a rozsahu útoků, způsobů vniknutí, parametrů oplocení a jeho konstrukčních prvků až po klimatické podmínky a specifika prostředí v okolí střeženého areálu. Jedním ze zásadních kritérií je pak taková konfigurace systému, která omezí generování planých poplachů na minimum.

Praktickým příkladem chtěl autor práce doložit efektivitu jednoho z nových perspektivních prostředků využitelných pro perimetrickou ochranu objektů - termografické zobrazování. Na výše uvedeném návrhu kamerového systému skladu PHM Bělčice se podařilo prokázat výhodnost řešení realizovaného instalací termálních kamer. Byla tím vyvrácena představa o velké finanční náročnosti ve srovnání s běžně dnes využívanými kamerovými systémy. I přesto, že termální kamera může být až násobně dražší než dnes využívané IP kamery v oblasti viditelného spektra, je takto navržený kamerový systém, vzhledem k potřebnému množství jednotlivých komponentů, finančně méně nákladný. Další významné úspory oproti konvenčnímu kamerovému systému přináší menší nároky na počty síťových prvků a kabeláže, absence osvětlení celého perimetru a jeho napájení, menší množství konstrukcí a komponent pro upevnění kamer a další. Termální systém navíc přináší viditelnost i za zhoršených světelných podmínek, mlhy a tmy, menší množství planých poplachů a efektivnější využití pokročilé videoanalýzy.

Rychlý rozvoj elektroniky a elektrotechniky nám dnes umožňuje využívat technologie, které byly ještě nedávno zcela nedostupné, nebo byly výhradně určené jen pro využití ve vojenské oblasti. Zároveň nám ale také přináší nová rizika, na která tato práce chtěla upozornit. Nebezpečí zneužití dronů je nutno zahrnout jako další možný způsob útoku v návrhu nově budovaných bezpečnostních systémů a rozšířit o něj systémy stávající. Je důležité, aby bylo počítáno s tím, že hranice perimetru nekončí těsně nad ochranným plotem nebo zdí, ale pokračuje až stovky metrů nad ní.

## Seznam použitých zdrojů

### Literární zdroje

1. BURDA, K. *Základy elektronických zabezpečovacích systémů*. 1. vyd. Brno : Akademické nakladatelství CERM, 2017. 124 s. ISBN 978-80-7204-967-7.
2. ČANDÍK, M. *Objektová bezpečnost II*. 1. vyd. Zlín : Univerzita Tomáše Bati, 2004. 100 s. ISBN 8073182173.
3. ČEPRO. *Spolehlivý zdroj od roku 1949*. Poděbrady : Astroprint, 2013. 13-17s.
4. IVANKA, J. *Mechanické zábranné systémy*. Zlín : UTB ve Zlíně, 2010. 120 s. ISBN 978-80-7318-910-5.
5. JELÍNEK, J. *Jak zabezpečit byt, dům, chatu, automobil*. Praha: Grada, 2000. 84 s. ISBN 80-7169-931-4.
6. KARAS, J. a TICHÝ, T. *Drony*. Brno : CPress, 2016. 264 s. ISBN 978-80-251-4680-4.
7. KINDL, J. *Projektování bezpečnostních systémů. I. díl, EPS, EZS*. 1. vyd. Zlín : Univerzita Tomáše Bati, 2004. 134 s. ISBN 80-7318-165-7.
8. KONÍČEK, T., KOCÁBEK, P. *Cesta k bezpečí*. 1. vyd. Praha : BEN - technická literatura, 2002. 239 s. ISBN 80-7300-032-6.
9. KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. aktualizované vyd. Blatná : Blatenská tiskárna, 2006. 350 s. ISBN 80-902938-2-4.
10. LUKÁŠ, L. *Bezpečnostní technologie, systémy a management*. 1. vyd. Zlín : VERBUM, 2011. 368 s. ISBN 978-80-87500-05-7.
11. ŘEŠÁTKO, J. a KOCOUREK, J. *Drony - Praktická příručka pro majitelé dronů DJI*. Praha : Telink, 2019. 183 s. ISBN 978-80-7346-228-4.
12. SKŘIVAN, Z. et al. *Nebojte se zlodějů: zabezpečovací technika v praxi*. 1. vyd. Praha : Grada, 1994. 216 s. ISBN 80-7169-096-1.
13. UHLÁŘ, J. *Technická ochrana objektů: II. díl, Elektrické zabezpečovací systémy II*. 1. vyd. Praha : Policejní akademie České republiky, 2005. 229 s. ISBN 80-7251-189-0.
14. UHLÁŘ, J. *Technická ochrana objektů III. Díl, Ostatní zabezpečovací systémy*. Praha : Policejní akademie České republiky, 2006. 246 s. ISBN 80-7251-235-8.
15. WOLF, H.G. *Drones: safety risk management for the next evolution of flight*. New York: Routledge, Taylor & Francis Group, 2017. 182 s. ISBN 978-1-138-20355-6.

16. ZALOGA, S. a PALMER, I. *Unmanned aerial vehicles: robotic air warfare, 1917-2007*. New York : Osprey, 2008. 48 s. ISBN 18-460-3243-1.

### **Elektronické zdroje**

1. AARTOS DDS. Drone-detection-system. *drone-detection-system.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://drone-detection-system.com/aartos-dds/product-overview/>>.
2. AARTOS DDS. Drone-detection-systém software integration. *drone-detection-system.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://drone-detection-system.com/aartos-dds/software-integration/>>.
3. Axis. AXIS D2050-VE Network Radar Detektor. *axis.com* [online]. [cit. 2020-1-3]. Dostupné z WWW: < <https://www.axis.com/products/axis-d2050-ve> >.
4. Axis. Axis Perimeter Defender. *axis.com* [online]. [cit. 2020-1-3]. Dostupné z WWW: < <https://www.axis.com/products/axis-perimeter-defender>>.
5. Axis. Axis Q1615-E Mk II Network Camera. *axis.com* [online]. [cit. 2020-1-8]. Dostupné z WWW: < <https://www.axis.com/products/axis-q1615-e>>.
6. Axis. Axis Q1941-E Thermal Network Camera. *axis.com* [online]. [cit. 2020-1-8]. Dostupné z WWW: < <https://www.axis.com/products/axis-q1941-e>>.
7. Axis. Axis Q6052-E PTZ Network Camera. *axis.com* [online]. [cit. 2020-1-8]. Dostupné z WWW: < <https://www.axis.com/products/axis-q6052-e>>.
8. Axis. Thermal imaging. *Axis.com* [online]. [cit. 2020-1-3]. Dostupné z WWW: < <https://www.axis.com/technologies/thermal-imaging/>>.
9. DEDRONE. Products Overview. *dedrone.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://www.dedrone.com/products/counter-drone-solution> >.
10. DEDRONE. Hardware to Protect against Drones. *dedrone.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://www.dedrone.com/products/hardware>>.
11. Evropská rada. Drony: reforma bezpečnosti letectví v EU. *Consilium.europa.eu* [online]. [cit. 2020-03-2]. Dostupné z WWW: < <https://www.consilium.europa.eu/cs/policies/drones/>>.
12. HATTELAND Technology. Intelligent perimeter detection solutions take your security to the next level. *hattelandtechnology.com* [online]. [cit. 2020-1-6]. Dostupné z WWW: < <https://www.hattelandtechnology.com/blog/intelligent-perimeter-detection-solutions-take-your-security-to-the-next-level/>>.



13. HGH. Definition of DRI Detection Recognition Identification. *hgh-infrared.com* [online]. [cit. 2020-1-1]. Dostupné z WWW: <<https://www.hgh-infrared.com/FAQ/Perimeter-Security/Definition-of-DRI-Detection-Recognition-Identification-ranges>>.
14. IPSECURE. IP kamery. *IPsecure.cz* [online]. [cit. 2020-1-8]. Dostupné z WWW: <https://www.ipsecure.cz/ip-kamery/>.
15. JINDRA, J. Jak daleko uvidím termokamerou? *ABBAS.cz* [online]. BRNO : ABBAS, 2019. 26. října 2012 [cit. 2020-1-1]. Dostupné z WWW: <<http://www.abbas.cz/clanky/recenze-technika/jak-daleko-uvitim-termalni-kamerou/>>.
16. Letecká informační služba. Doplněk X – Bezpilotní systémy. *Aim.rlp.cz* [online]. [cit. 2019-11-5]. Dostupné z WWW: <<https://aim.rlp.cz/predpisy/predpisy/dokumenty/L/L-2/data/effective/doplX.pdf>>.
17. OptaSense. Protecting critical infrastructure and assets. *Optasense.com* [online]. [cit. 2020-1-1]. Dostupné z WWW: <<https://www.optasense.com/security/intrusion-detection/#1480955481921-4d02179a-4e7d>>.
18. Pierre. Deset dronů provedlo úspěšný útok na saudskoarabská ropná zařízení, produkce ropy země klesla na polovinu. *Otechnice.cz* [online]. Praha : Mopax, 2019. 15. září 2019 [cit. 2019-11-07]. Dostupné z WWW: <<https://otechnice.cz/deset-dronu-provedlo-uspesny-utok-na-saudskoarabska-ropna-zarizeni-produkce-ropy-zeme-klesla-na-polovinu/>>.
19. RED. Oceňované optické vlákno „s ušima“ dorazilo do Česka. *info.cz* [online]. Praha : CNC, 2018. 8. září 2017 [cit. 2020-1-1]. Dostupné z WWW: <<https://www.info.cz/byznys/ocenovane-opticke-vlakno-s-usima-dorazilo-do-ceska-37772.html>>.
20. Remy. Neznámé drony zastavily provoz na letišti Gatwick. Jde o záměr, říká policie. *iDnes.cz* [online]. Praha : Mafra, 2018. 20. prosince 2018 13:01 [cit. 2019-11-07]. Dostupné z WWW: <[https://www.idnes.cz/zpravy/zahranicni/gatwick-letiste-provoz-preruseni-londyn.A181220\\_080119\\_zahranicni\\_remy](https://www.idnes.cz/zpravy/zahranicni/gatwick-letiste-provoz-preruseni-londyn.A181220_080119_zahranicni_remy)>.

21. SECURIA. Informace o Bezpečnostních systémech. *Securia.cz* [online]. [cit. 2019-10-15]. Dostupné z WWW: < <https://securia.cz/informace-o-bezpecnostnich-systemech/226-zakladni-rozdeleni-kamerovych-systemu>>.
22. SECURITY MAGAZÍN. Optické vlákno s ušima dokáže ohlídat až 5000 kilometrů dlouhou trasu. *securitymagazin.cz* [online]. Praha : Security Media. 8. září 2015 [cit. 2020-1-1]. Dostupné z WWW: < <https://www.securitymagazin.cz/security/opticke-vlakno-s-usima-dokaze-ohlidat-az-5000-kilometru-dlouhou-trasu-napriklad-statni-hranice-1404046168.html>>.
23. SIEZA. Peridect. *Sieza.cz* [online]. [cit. 2019-11-15]. Dostupné z WWW: < <https://www.sieza.com/cz/produkty/peridect#article208>>.
24. SKYLOCK. Anti Drone Systems *Skylock1.com* [online]. [cit. 2019-11-1]. Dostupné z WWW: < <https://www.skylock1.com>>.
25. Tacticaware. About Accur8vision. *Accur8vision.com* [online]. [cit. 2020-1-3]. Dostupné z WWW: < <https://accur8vision.com/>>.
26. Velodyne. Products. *Velodynelidar.com* [online]. [cit. 2020-1-1]. Dostupné z WWW: < <https://velodynelidar.com/products/>>.
27. Vlastní. Vytvořeno prostřednictvím Design Tool For AXIS Perimeter Defender.
28. Vlastní. Xiaomi Mi Drone 4K

## Seznam zkratek

LiDAR	Light Detection and Ranging
AGA	Asociace technických bezpečnostních služeb Grémium Alarm
RFID	Radio Frequency Identification
PIR	Passive Infrared Sensor
PTZ	Pan Tilt Zoom
CCTV	Closed Circuit Television
CCD	Charge Coupled Device
BNC	Bayonet Neill Concelman Connector
PAL	Phase Alternating Line
UTP	Unshielded Twisted Pair
DVR	Digital Video Recording
AHD	Analog High Definition
POE	Power Over Ethernet
LAN	Local Area Network
IP	Internet Protocol
IR	Infrared
LED	Light Emitting Diode
UAV	Unmanned Aerial Vehicle
GPS	Global Positioning System
GLONASS	Globální družicový navigační systém
HD	High Definition

LTE	Long Term Evolution
ÚCL	Úřad pro civilní letectví
PHM	Pohonné hmoty a mazadla
CMOS	Complementary Metal Oxid Semiconductor

## Seznam obrázků

Obr.1: Dělení ochrany objektu podle AGA	11
Obr.3: Příklad současného střežení perimetru	32
Obr. 3: DEDRONE systém	35
Obr. 4: Prvky systému DEDRONE	35
Obr. 5: AARTOS X7	36
Obr. 6: Náhled vyhodnocovacího software	37
Obr. 7: Zpracování výstupu z PTZ kamer v reálném čase	37
Obr. 8: Integrace radaru ve 3D	38
Obr. 9: Směrové vyhledávání na různých kmitočtech	38
Obr. 10: SKYLOCK	39
Obr. 11: Srovnání zobrazení scény termální a klasickou kamerou	41
Obr. 12 : Příklady detekce, rozpoznání a identifikace cílů	42
Obr. 13: Příklad akustické odezvy narušení perimetru	43
Obr. 14: Schematický popis systému OptaSense	44
Obr. 15: Objemový detektor LiDAR od společnosti Velodyne	45
Obr. 16: Příklad zobrazení objemové detekce systémem Accur8vision	46
Obr. 17: Zobrazení trajektorie narušení střežené zóny v systému Accur8vision	46
Obr. 18: Radarový detektor AXIS D2050-VE	47
Obr. 19: Radarový detektor Axis s verifikační PTZ kamerou	48
Obr. 20: Příklady jednotlivých scénářů Axis Perimeter Defender - Vstup do zóny	49

Obr. 21: Příklady jednotlivých scénářů Axis Perimeter Def. - Vstup přes zónu	49
Obr. 22: Příklady jednotlivých scénářů Axis Perimeter Def - Přejechání zón	50
Obr. 23: Příklady jednotlivých scénářů Axis Perimeter Def - Zdržování se v zóně	50
Obr. 24: Příklady jednotlivých scénářů Axis Perimeter Def - PTZ verifikace	50
Obr. 25: Sklad PHM Bělčice	52
Obr. 26: Sklad PHM Bělčice	52
Obr. 27: Návrh termálního kam. systému pro zabezpečení skladu PHM Bělčice	53
Obr. 28: Návrh termálního kam. systému s PTZ kamerami skladu PHM Bělčice	54