

Návrh integrovaného kamerového systému

Draft of integrated camera system

Bc. Jan Koňářík

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Jan Koňářík**
Osobní číslo: **A12311**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **prezenční**

Téma práce: **Návrh integrovaného kamerového systému**
Téma anglicky: **A Design for Integrated Camera Systems**

Zásady pro vypracování:

1. Vymezte technické požadavky na integrované poplachové systémy.
2. Analyzujte technické požadavky na integraci kamerových systémů v bezpečnostních aplikacích.
3. Popište způsoby technických řešení integrace kamerových systémů s poplachovými a nepoplachovými aplikacemi.
4. Zpracujte návrh integrace kamerového systému pro modelový objekt komerčního typu.
5. Pojednejte o vývojových trendech v integračních technologiích kamerových systémů.

Rozsah příloh:

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

Seznam odborné literatury:

1. VALOUCH, Jan. Projektování bezpečnostních systémů. [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5. 152 s.
2. VALOUCH, Jan. Projektování integrovaných systémů. [skriptum]. Zlín: UTB, 2013. ISBN 978-80-7454-296-1 152 s.
3. LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management. 1. vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.
4. LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012. 387 s. ISBN 978-80-87500-19-4.
5. LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management III. 1. vyd. Zlín: VeRBuM, 2013. 456 s. ISBN 978-80-87500-35-4.
6. LOVEČEK, Tomáš. REITŠPÍS, Josef. Projektovanie a hodnotenie systémov ochrany objektov. Žilina: EDIS - vydavateľstvo ŽU, 2011. 281 s. ISBN 978-80-554-0457-8.
7. LOVEČEK, T., NAGY, P. Bezpečnostné systémy: kamerové bezpečnostné systémy. Žilina: Žilinská univerzita v Žiline, 2008. 272 s. ISBN 978-80-8070-893-1.

Vedoucí diplomové práce:

Ing. Jan Valouch, Ph.D.

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

7. února 2014

Termín odevzdání diplomové práce:

27. května 2014

Ve Zlíně dne 7. února 2014



prof. Ing. Vladimír Vašek, CSc.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Úvodní část diplomové práce představuje analýzu technických požadavků na integraci poplachových a nepoplachových aplikací. Tato část je doplněna analýzou požadavků na integraci kamerových systémů. Praktická část práce tvoří popis stávajících možností integrace kamerových systémů. Stěžejní výstup představuje návrh integrace kamerového systému pro modelový objekt komerčního typu. V závěru práce jsou uvedeny informace o vývojových trendech v integračních technologiích.

Klíčová slova: kamera, bezpečnost, integrace, kamerový dohledový systém, poplachové aplikace

ABSTRACT

The introductory part of the thesis presents an analysis of the technical requirements for the integration of alarm and non-alarm applications. This section is supplemented with an analysis of requirements for the integration of CCTV systems. The practical part consists of a description of existing camera systems integration capabilities. The key output represents the integration of the CCTV system for commercial type of building. The conclusion provides information about future trends in integration technologies.

Keywords: camera, security, integration, CCTV surveillance system, alarm application

Rád bych poděkoval všem, kteří mě podporovali při tvorbě této diplomové práce. Zejména děkuji svému vedoucímu práce Ing. Janu Valouchovi Ph.D., jenž mi pomáhal vybírat téma ke zpracování a se kterým jsem mohl prokonzultovat případné nedostatky práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD	9
I TEORETICKÁ ČÁST	10
1 INTEGROVANÉ POPLACHOVÉ SYSTÉMY	11
1.1 POPLACHOVÉ ZABEZPEČOVACÍ A TÍŠŇOVÉ SYSTÉMY	12
1.2 SYSTÉMY KONTROLY VSTUPŮ	12
1.3 ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE	13
1.4 MECHANICKÉ ZÁBRANNÉ SYSTÉMY	13
1.5 OSTATNÍ POPLACHOVÉ A NEPOPLACHOVÉ APLIKACE.....	14
2 KAMEROVÉ SYSTÉMY	16
2.1 SKLADBA KAMERY	16
2.2 SKLADBA KAMEROVÉHO SYSTÉMU.....	17
2.2.1 Skladba kamerového systému dle normy ČSN EN 50132-1	17
2.2.2 Skladba kamerového systému s popisem komponentů.....	19
3 TECHNICKÉ POŽADAVKY NA INTEGRACI	21
3.1 TECHNICKÉ POŽADAVKY NA INTEGROVANÉ POPLACHOVÉ SYSTÉMY.....	21
3.1.1 Všeobecná klasifikace	21
3.1.2 Systémové požadavky	22
3.1.3 Požadavky na centrální ovládací zařízení	23
3.2 TECHNICKÉ POŽADAVKY NA INTEGRACI KAMEROVÝCH SYSTÉMŮ V BEZPEČNOSTNÍCH APLIKACÍCH	23
3.2.1 Stupně zabezpečení	24
3.2.2 Funkční požadavky	24
3.2.3 Integrace kamerových systémů v bezpečnostních aplikacích.....	25
II PRAKTICKÁ ČÁST	28
4 ZPŮSOBY INTEGRACE KAMEROVÉHO SYSTÉMU	29
4.1 HARDWAROVÁ INTEGRACE KAMEROVÉHO SYSTÉMU	30
4.1.1 Integrace IN/OUT	30
4.1.2 Ústředna PZTS jako integrační prvek	31
4.1.3 Integrace s využitím prvku kamerového systému	32
4.1.4 Automatizační systém jako integrační prvek	33
4.2 SOFTWAREVÁ INTEGRACE KAMEROVÉHO SYSTÉMU	34
4.2.1 Způsoby softwarové integrace	34
4.2.1.1 Software ústředn poplachových systémů	34
4.2.1.2 Software pro uživatelskou správu	35
4.2.1.3 Vizualizační software	35
4.2.1.4 Integrační software systémů budov	36
4.2.2 Softwarové nástroje pro integraci kamerových systémů	36
4.2.2.1 VAR-NET Integral	36
4.2.2.2 Software firmy Milestone.....	39
4.2.2.3 Omnicast, Genetec Security Center a Integra	42
4.2.2.4 NetRex.....	45
5 NÁVRH INTEGROVANÉHO KAMEROVÉHO SYSTÉMU	47

5.1	BEZPEČNOSTNÍ POSOUZENÍ OBJEKTU	48
5.1.1	Zabezpečované hodnoty	48
5.1.2	Budova	49
5.1.3	Vlivy působící na integrovaný systém a mající původ ve střeženém objektu	51
5.1.4	Vlivy působící na integrovaný systém a mající původ vně střeženého objektu	52
5.1.5	Stanovení stupně zabezpečení	52
5.1.6	Stanovení tříd prostředí	53
5.2	NÁVRH ZABEZPEČENÍ	53
5.2.1	Nákres zabezpečení	54
5.2.2	Zvolené technické prvky	57
5.2.3	Konfigurace systému	64
5.2.3.1	Konfigurace kamerového systému	65
5.2.3.2	Konfigurace PZTS	66
5.2.3.3	Konfigurace přístupového systému	67
5.2.3.4	Konfigurace EPS	68
5.2.4	Hlášení poplachu	68
5.2.5	Zásah	69
5.2.6	Údržba systému	71
5.2.7	Finanční kalkulace	71
6	VÝVOJOVÉ TRENDY V INTEGRAČNÍCH TECHNOLOGIÍCH KAMEROVÝCH SYSTÉMŮ	74
6.1	VÝVOJ IP KAMER A KAMEROVÝCH SYSTÉMŮ	74
6.2	VÝVOJ INTEGRACE KAMEROVÝCH SYSTÉMŮ	76
	ZÁVĚR	78
	ZÁVĚR V ANGLIČTINĚ	79
	SEZNAM POUŽITÉ LITERATURY	80
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	83
	SEZNAM OBRÁZKŮ	84
	SEZNAM TABULEK	85
	SEZNAM PŘÍLOH	86

ÚVOD

Tato práce je věnována kamerovým systémům, integrovaným systémům a možností integrace kamerových systémů s dalšími poplachovými i nepoplachovými aplikacemi.

V současné době je ještě většina systémů separovaných a teprve nově instalovaná zařízení jsou v některých případech integrována do kompletního funkčního celku. Toto platí bez výjimky i pro kamerové systémy, které jsou pro tuto práci stěžejní, dokonce je možné říci, že u kamerových systémů dochází k integraci v ještě menším měřítku než u ostatních poplachových a nepoplachových aplikací.

Pravděpodobný hlavní důvod proč nejsou dříve instalované kamerové systémy integrovány s ostatními aplikacemi je patrný již z jejich platného označení CCTV systémy (closed circuit television), tedy uzavřený televizní okruh. Podle tohoto pravidla (tedy uzavřeně) jsou vystaveny starší kamerové systémy, tedy nejsou integrovány s ostatními aplikacemi.

Dnes již název uzavřený televizní okruh není zcela přesný, jelikož nové systémy zakládáné na IP kamerách a moderních videoserverech s možnostmi komunikace, jak přes internet, tak pomocí svých vstupů, výstupů a softwarových nástrojů, jsou bez problémů integrovatelné s mnoha poplachovými i nepoplachovými aplikacemi, které dnešní trh nabízí, tedy nejsou v žádném případě uzavřené (i když mohou být, pokud si to majitel bude přát).

Cílem a předpokládaným přínosem této práce je čtenáři přiblížit pojmy související s integrovanými systémy, možnosti kamerových systémů, požadavky na tyto systémy vycházející z aktuálních norem, dále nastínit možnosti hardwarové a softwarové integrace těchto systémů, vypracovat návrh integrovaného kamerového systému pro objekt komerčního typu a nakonec nastínit možnosti vývoje jak samotných kamerových systémů, tak jejich budoucích možností integrace s ostatními aplikacemi.

I. TEORETICKÁ ČÁST

1 INTEGROVANÉ POPLACHOVÉ SYSTÉMY

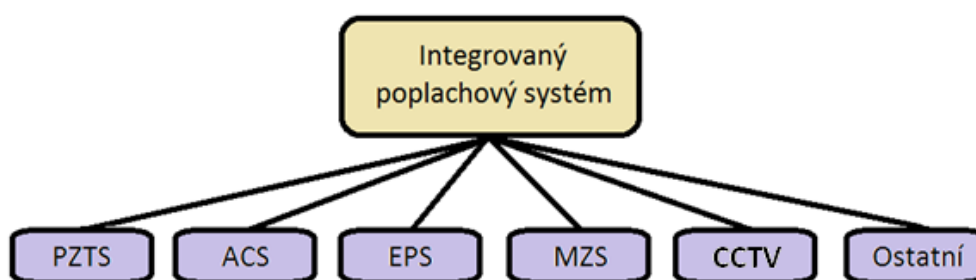
Integrovaný poplachový systém je systém mající jedno nebo více společných zařízení, alespoň jedním z nichž je poplachová aplikace. [1]

Důvodů proč navrhovat integrované poplachové systémy namísto používání oddělených aplikací je mnoho. Mezi hlavní důvody ovšem patří zvýšení bezpečnosti objektu, zvýšení uživatelského komfortu při užívání systému a redukce provozních nákladů. [2]

Integrované systémy, na rozdíl od běžných jednoúčelových systémů, jsou navrhovány a sestavovány prostřednictvím plného datového i funkčního propojení jeho jednotlivých částí. Díky tomuto řešení je možné, obvykle za pomoci grafického rozhraní, pohodlně ovládat využívat všechny spojené systémy, jenž by jinak bylo nutné ovládat zvlášť. [3]

Možné součásti integrovaného poplachového systému:

- PZTS - Poplachové zabezpečovací a tísňové systémy
- ACS - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích
- EPS - Elektrická požární signalizace
- MZS - Mechanické zábranné systémy
- CCTV - Kamerové systémy
- a další poplachové a nepoplachové aplikace



Obrázek 1 Součásti Integrovaného poplachového systému

1.1 Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy (PZTS) jsou základním prvkem, na němž je integrovaný poplachový systém vystaven. Jeho úkolem a tedy i hlavní funkcí je detekce a signalizace pokusu o vniknutí do střeženého prostoru. [4]

Systém PZTS je tvořen z

- ústředny,
- ovládací klávesnice,
- detektorů,
- koncových zařízení.

Dle tvaru a umístění střeženého prostoru dělíme detektory na:

- prvky perimetrické ochrany (obvod střeženého objektu - ploty, zdi),
- prvky plášťové ochrany (zdi, okna, dveře a další otvory střeženého objektu),
- prvky prostorové ochrany (jednotlivé místnosti a chodby střeženého objektu),
- prvky předmětové ochrany (jednotlivé předměty - trezor, umění atd.).

Pro detekci narušení střeženého prostoru se využívají čidla a detektory s různými principy detekce. Při projektování těchto systémů jsou nejčastěji využívány následující detektory:

- pasivní infračervený detektor pohybu,
- mikrovlnný detektor pohybu,
- detektor tříštění skla,
- magnetické kontakty.

1.2 Systémy kontroly vstupů

Elektronický systém kontroly vstupu (Access Control System – ACS), se využívá tehdy, pokud je třeba omezit, kontrolovat a evidovat pohyb osob v daném objektu. Pro ověřování totožnosti osob se využívá velká škála prvků od jednoduchých magnetických karet až po složité biometrické systémy (kontrola oční duhovky), někdy je využíváno i více prvků zároveň. [5]

System kontrolly vstupu lze samozřejmě uplatnit pouze tam, kde jsou jednotlivé prostory s různou přístupností odděleny mechanickou překážkou (zdi, dveře, závory, turnikety, brány apod.). [5]

Avšak pouze kontrola vstupu není vše, co nám tyto systémy nabízí, jeho součástí je obvykle i software, který kontroluje celý systém a archivuje záznamy o příchodech a odchodech, se kterými dále pracuje. To nám umožňuje zajistit nejen to, aby vstupovaly pověřené osoby, ale také například kontrolovat pracovní dobu všech zaměstnanců ve firmě, nebo osoby přesně lokalizovat v reálném čase.

Funkce přístupových systémů jsou:

- kontrola pracovní doby,
- rozčlenění do přístupových zón,
- sledování pohybu,
- otevření únikových cest při mimořádné události. [6]

1.3 Elektrická požární signalizace

Systémy elektrické požární signalizace (EPS) mají za úkol detekovat počáteční fáze požáru ve střeženém prostoru. Po detekci požáru může ústředna EPS přenášet informaci přímo k HZS (Hasičský záchranný sbor), nebo pokud není připojená na dohledové a poplachové přijímací centrum (DPPC) HZS, spouští poplach pomocí akustické signalizace. EPS může také ovládat další zařízení, jako například únikové dveře nebo zařízení pro odvod kouře a tepla. [7]

Požární detektory obvykle reagují na jeden či více z následujících projevů požáru:

- teplo - podle hraniční teploty (maximální), nebo podle rychlosti nárůstu teploty (diferenciální),
- světlo - podle světla, které vydávají plameny,
- kouř - podle plynů vznikajících při hoření, nebo podle zakrytí světelného paprsku kouřem.

1.4 Mechanické zábranné systémy

Mechanické zábranné systémy, jak už název napovídá, chrání objekt mechanicky, bez použití elektrické energie. Jejich úkolem je co možná nejvíce zkomplikovat pachateli

vstup do chráněného objektu a tím zvýšit dobu potřebnou k proniknutí alespoň na dobu potřebnou k příjezdu policie nebo zásahové jednotky bezpečnostní agentury.

Mely by být součástí každého kvalitního zabezpečovacího systému.

Tabulka 1 Mechanické zábranné systémy a jejich
zařazení do typu ochrany

Bezpečnostní dveře	plášťová ochrana
Bezpečnostní zámky	plášťová ochrana
Bezpečnostní mříže	plášťová ochrana
Bezpečnostní závory	perimetrická ochrana
Bezpečnostní skla	plášťová ochrana
Okenní zabezpečení	plášťová ochrana
Trezory	předmětová ochrana
Skříně na zbraně	předmětová ochrana

Dle výčtu různých prvků mechanického zábranného systému je vidět že je nejvíce využíván pro plášťovou ochranu objektu. [6]

1.5 Ostatní poplachové a nepoplachové aplikace

Vzhledem k tomu, že jednoúčelových aplikací, které může integrovaný poplachový systém obsahovat je velké množství, tak je zde nebudu jednotlivě rozepisovat, ale uvedu pouze výčet některých z nich.

- Systémy přivolání pomoci

Jedná se o poplachový systém, který poskytuje prostředky pro přivolání pomoci a je určen zejména osobám, které žijí nebo mohou žít v nebezpečí. Tento systém musí poskytovat 24 hodinovou pohotovost pro aktivaci poplachu, jeho identifikaci a přenos signálu, přijetí poplachu, jeho zaznamenání a hlasovou komunikaci, to vše k poskytnutí jistoty lidem žijícím v možném nebezpečí. [8]

- Ovládání osvětlení, rolet, topení

Pokud jsou na integrovaný systém napojeny ovladače topení, osvětlení (vypínače, tlumiče), topení (termostat), tak je systém při správném nastavení schopen reagovat na jednotlivé vlivy okolí a podněty, které mu uživatel dává (například otevření/zamčení dveří,

zastřežení/odstřežení zabezpečovacího systému, zvýšení teploty v místnosti atd.) a samovolně tyto zařízení ovládat. Jedná se zejména o funkce zvyšující uživatelský komfort při bydlení v objektu, který je integrovaným systémem vybaven.

- Ozvučovací systémy

Tyto systémy naleznou nejlepšího využití v objektech komerčního typu, jako jsou školy, rozlehlé kancelářské prostory, nákupní centra a v dalších podobných budovách. Využívají se pro informování pracovníků ve větších provozech, informování zákazníků v nákupních centrech a hudební produkci. Avšak jejich nejdůležitější funkcí je varování a informování osob nalézajících se v objektu o vzniku mimořádné události a koordinaci těchto osob při evakuaci, pokud je potřeba ji zorganizovat. [9]

- Systémy jednotného času

Jedná se o systém, který synchronizuje zařízení a umožní jim zobrazovat přesný čas. Opět hojně využívaný zejména u rozsáhlých objektů, kde je třeba, aby byl čas na všech ukazatelích přesný (velké provozy, nádraží a další). Tento čas je přijímán externím radiovým signálem z vysílače DCF (signál vysílače DCF77 je šířen v pásmu dlouhých vln na kmitočtu 77,5 kHz). Základem tohoto systému jsou hlavní hodiny přijímající signál z DCF a ty rozesílají signál dál sekundárním hodinám. Tohoto systému lze rovněž využít pro zobrazování dalších dat jako třeba datum, teplota a vlhkost vzduchu. [9]

Dílčí závěr

Integrovaný poplachový systém je systém mající jedno nebo více společných zařízení, alespoň jedním z nichž je poplachová aplikace.[13] Jedná se o systém využívající spojení dílčích aplikací ve prospěch jeho majitele (bezpečnost, komfort, redukce nákladů). Mezi nejčastěji využívané poplachové aplikace patří PZTS, CCTV, ACS a EPS, kdy je základním stavebním prvkem systému PZTS. Ke kombinaci vybraných poplachových aplikací jsou dále přidávány aplikace nepoplachové (ovládání osvětlení, topení, rolet, zavlažování atd.) a dohromady tvoří kompletní funkční celek, jehož účelem je maximalizace přínosů pro jeho uživatele.

2 KAMEROVÉ SYSTÉMY

Kamerové systémy, ČSN EN 50132 používá název CCTV sledovací systémy (Closed Circuit Television - uzavřený televizní okruh), jsou určeny k nepřetržitému sledování střeženého prostoru. Dříve byly tyto systémy velmi drahé a z toho důvodu zřídka využívané, ovšem v dnešní době, kdy pořizovací hodnoty kamer klesají a jejich kvalita stoupá, se kamerové systémy stále více využívají, a to ve všech možných odvětvích (například kontrola výroby a zaměstnanců, poplachové systémy, kontrola veřejného pořádku). [10]

Při zaměření se na kamerový systém využívaný v rámci integrovaného poplachového systému, je možné vyzdvihnout některé jeho vlastnosti, které jsou oproti běžné PZTS výhodou:

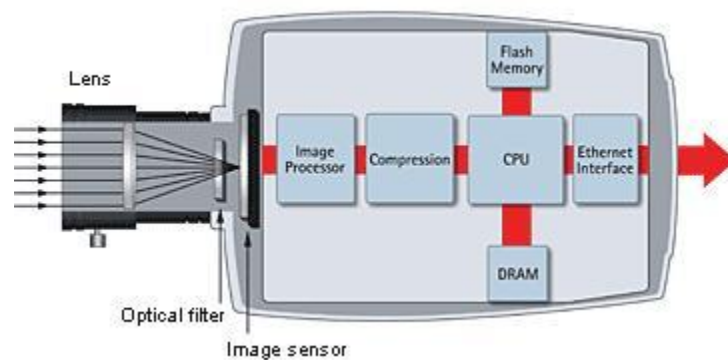
- při vzniku poplachu umožňuje zaznamenání celého incidentu,
- možnost identifikace pachatele,
- odstrašení pachatele (kamerové systémy jsou pro většinu pachatelů odstrašující, svědčí o tom i to, že jsou na některé objekty umístovány makety kamer pro prevenci před vloupáním). [11]

2.1 Skladba kamery

Vzhledem k tomu, že se při navrhování nových kamerových v dnešní době používají ve velké většině případů IP kamery, tak zde bude rozebrána skladba právě tohoto druhu kamer. IP kamera je v podstatě počítač a kamera zároveň, je připojena přímo k ethernetové síti, má vlastní IP adresu a vestavěné funkce starající se o síťovou komunikaci kamery s ostatními zařízeními. [12]

Součásti IP kamery:

- Čočky - zaměření obrazu do senzoru
- Optický filtr - oddělení infračerveného světla
- Senzor (CCD/CMOS) - konverze světla na elektrický signál
- Obrazový procesor - zpracování a komprese signálu
- CPU, flash paměť, DRAM - mozek IP kamery, obstarává komunikaci se sítí a webovým serverem
- Ethernetové rozhraní - rozhraní pro připojení do sítě



Obrázek 2 Skladba IP kamery [13]

2.2 Skladba kamerového systému

Skladbu kamerového systému je možné pojmout dvěma způsoby. Prvním způsobem je skladba systému dle technických norem, kdy je systém popisován teoreticky a nekonkrétně pro vyšší platnost normy bez potřeby aktualizace z důvodu rychlého vývoje těchto systémů. Dalším způsobem popisu skladby kamerového systému je popis jednotlivých komponent, které se v systému mohou vyskytovat a jejich návaznost na sebe navzájem.

2.2.1 Skladba kamerového systému dle normy ČSN EN 50132-1

Tato struktura kamerového systému vyhovuje zejména IP kamerovému systému. Dle normy ČSN EN 50132-1 je kamerový systém složen z následujících částí:

- video prostředí,
- management systému,
- bezpečnost systému.

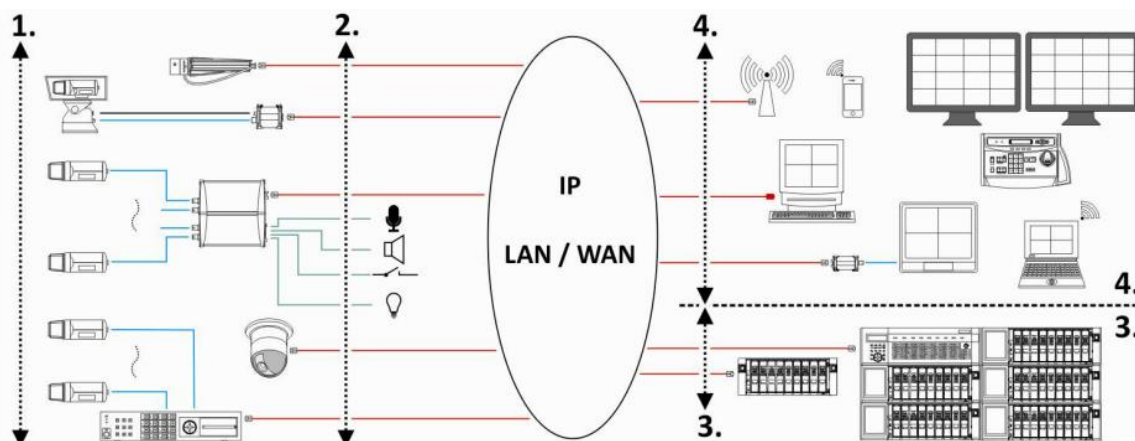
Video prostředí

Jedná se o prvky, vlastnosti a funkce, jenž může kamerový systém obsahovat. Samo video prostředí je dále rozděleno na 4 části, jimiž jsou:

- zachycení obrazu,
- přenos obrazové informace,
- zpracování obrazu,
- uživatelské rozhraní.

Tyto součásti jsou názorně vykresleny na obrázku 3.

Tyto součásti video prostředí ovšem nemusí být zvlášť obstarávány jednotlivými zařízeními. V dnešní době jsou již moderní kamery schopny zajišťovat více než jednu z těchto služeb. IP kamera s přístupem na internet a bezdrátovým připojením k PZTS systému může obstarávat jak zachycení obrazu, tak zpracování obrazu i přenos obrazové informace.



Obrázek 3 Schéma video prostředí [14]

Management systému

Pro management systému je velmi důležité uživatelské prostředí, které pomáhá pro orientaci v celém kamerovém systému a záznamech jím pořízených. Management systému lze rozdělit do dvou částí a to:

- management dat,

Kamerový systém může kromě obrazových dat také obstarávat zvuková data, či metadata získávaná z jiné aplikace či generovaná systémem samotným. Management dat zahrnuje zpracovávání těchto dat do přehledných a srozumitelných informačních rámců. Zajišťuje získávání dat, přenos dat mezi prvky systému, uchování obrazu a zobrazení dat. Tyto funkce zajišťují obvykle komponenty kamerového systému. [15]

- management aktivity.

Managementem aktivity jsou myšleny veškeré aktivity, které jsou vyvolávány událostmi působícími na kamerový systém (například výskyt požáru v pozorované oblasti, přijatý poplachový signál od PZTS, varování operátora na podezřelou aktivitu a další), nebo ovládáním systému uživatelem (například dočasné ruční ovládání kamery, export dat, zálohování dat a podobně). [15]

Bezpečnost systému

Bezpečnost systému zahrnuje integritu systému a integritu dat.

Integrita systému je ochrana jednotlivých komponent systému i systému jako prvku před poruchou prvků, softwaru a propojení, dále před fyzickým narušením a neautorizovaným přístupem. Při propojení kamerového systému s jinými aplikacemi musí být i toto propojení chráněno.

Integritou dat je myšlena ochrana dat, jež kamerový systém pořizuje, přenáší, zpracovává a zobrazuje před modifikací dat, neautorizovanému přístupu k nim. Dále také zajišťuje přesnou identifikaci zdrojů dat, času jejich pořízení a dalších podrobností. [15]

2.2.2 Skladba kamerového systému s popisem komponentů

Tento způsob popisu skladby kamerového systému je nejbližší, dnes již málo používaným, analogovým kamerovým systémům, které obvykle obsahují všechny níže zmíněné prvky jako samostatné zařízení. U IP kamerových systémů může být již většina zabudována přímo v kameře. Skladbu systému tedy tvoří:

- kamera,

Kamera je základním prvkem systému, který je určen pro zachycení obrazových dat, jejich zpracování na požadovaný typ signálu (analogový nebo digitální) a odeslání po přenosové cestě.

- přenosová cesta,

Signál, který je získán od kamery, je přenášen, dle typu přenosové cesty, buď kabelem, nebo bezdrátově k dalšímu zařízení pro zpracování obrazu. V některých případech může být signál i šifrovaný.

- záznamové zařízení,

Zařízení, které přijímá signál od přenosové cesty a ukládá jej pro pozdější použití na harddisk, nebo jiné paměťové médium.

- a zobrazovací zařízení. [16]

Obvykle jím bývá počítač či monitor, jež zobrazuje obrazovou informaci přímo (živý přenos) nebo z harddisku. Při použití počítače lze dále obraz pomocí softwaru dále analyzovat.

Dílčí závěr

Kamerové systémy jsou v důsledku jejich klesajících cen a zvyšující se kvality po všech stranách v poslední době stále více využívány a to i při integraci s dalšími aplikacemi, jak poplachovými, tak nepoplachovými. V poslední době se upouští od používání analogových kamerových systémů a přechází se spíše na IP kamerové systémy a to z důvodu jejich velké variability, jejich širokých programovatelných a detekčních schopností a možností praktického propojení s dalšími aplikacemi, které díky nim získávají další rozměr kvality a spolehlivosti. Vyspělá IP kamera dnes dokáže plnit funkci celého analogového kamerového systému vyjma zobrazení obrazové informace. Při instalaci PZTS systému je nespornou výhodou jej integrovat s kamerovým systémem, jelikož je schopen pořídit záznam celé události, která vyvolala poplach a díky tomu značně zvyšuje šanci na dopadení pachatele i po uprchnutí z místa nepovoleného vniknutí.

3 TECHNICKÉ POŽADAVKY NA INTEGRACI

Při návrhu integrovaných poplachových systémů je třeba dodržovat normy, které se pro tuto problematiku vztahují. Jako základní normu pro tuto kapitolu jsem určil ČSN CLC/TS 50398, dále pak normy ČSN EN 50132-1 a ČSN EN 50132-7 podle nichž jsem se při klasifikaci požadavků řídil.

3.1 Technické požadavky na integrované poplachové systémy

Před tím, než započneme navrhovat integrovaný systém, je třeba vypracovat soubor požadavků, který nám bude specifikovat celistvost systému a obsahovat alespoň následující informace:

- druhy použitých aplikací a požadavky na ně,
- cíle, kterých chceme kombinací a integrací těchto aplikací dosáhnout,
- charakteristika objektu, který bude integrovaným poplachovým systémem vybaven.

U integrovaných poplachových systémů musí veškeré zařízení odpovídat normám daným pro aplikaci, v níž je toto zařízení využíváno. Pokud je zařízení společné pro více aplikací, tak musí vyhovovat normám pro každou aplikaci, pro niž je využíváno (tedy nejpřísnějším požadavkům). Toto platí i pro veškeré další prvky integrovaného systému, jako například kabeláž, napájecí zdroje atd. [1]

3.1.1 Všeobecná klasifikace

Podle ČSN CLC/TS 50398 jsou integrované poplachové systémy rozděleny do tří základních skupin:

Typ 1 - zde se jedná o kombinaci a integraci jednoúčelových poplachových systémů s jednoúčelovými systémy nepoplachového typu,

Typ 2A - je použitelný pro kombinaci a integraci poplachových a nepoplachových systémů využívajících společné zařízení, vybavení a přenosové trasy. Porucha v jedné aplikaci nesmí mít vliv na jiné aplikace, aby toto bylo možné je třeba redundantních zařízení,

Typ 2B - stejně jako u typu 2A jde o integraci poplachových a nepoplachových systémů využívajících společné zařízení, vybavení a přenosové trasy, ovšem s tím

rozdílem, že pokud se vyskytne porucha v jedné aplikaci, tak může ovlivnit aplikace ostatní.

Aplikací, či jednoúčelovým systémem je myšleno zařízení využívané pro specifické účely, či jediný účel (např.: CCTV, ACS), společným zařízením je zařízení sdílené jednou nebo více aplikacemi (např.: elektronický zámek – může být sdílen systémem ACS a EPS), ústředním ovládacím zařízením (CCF) je zařízení používané k řízení, ovládání, signalizaci a konfiguraci jedné nebo více aplikací a obvykle ovládáno personálem (např.: počítač, ústředna PZTS). [1]

3.1.2 Systémové požadavky

V rámci integrovaného poplachového systému nesmí v normálním stavu žádná aplikace nepříznivě ovlivňovat funkci aplikace jiné. Povelové signály ovšem mohou být přenášeny z jedné aplikace do druhé nebo z ústředního ovládacího zařízení do aplikace (například otevření dveří elektrickou požární signalizací, kdy je obvykle má na starost přístupový systém). Ovšem zde je třeba dbát na to, aby takovýto povelový signál byl správně použit.

Pokud jsou v systému využita společná ovládací a signalizační zařízení, musí mít jednoduché ovládání a signalizace musí splňovat nejpřísnější požadavky, jež jsou definovány v normách. Při signalizaci by měly být určeny priority jednotlivých druhů poplachů následně (ovšem není to pravidlem, v některých situacích je vhodné pořadí pozměnit):

- priorita 1 - Poplachové signály vztahující se k ochraně života při požárním poplachu či napadení,
- priorita 2 - Poplachové signály vztahující se k ochraně majetku a proti nedovolenému vniknutí do objektu,
- priorita 3 - Poplachové signály z ostatních poplachových systémů,
- priorita 4 - Poruchové signály ze systémů ochrany života a majetku,
- priorita 5 - Poruchové signály z ostatních poruchových systémů,
- priorita 6 - Informace z nepoplachových systémů.

Pokud se jedná o software jednotlivých poplachových a nepoplachových aplikací, je doporučeno, aby při návrhu, dokumentaci a jednotlivých modulech byl navzájem

oddělen. Pokud je zde možnost vlivu softwarů jednotlivých aplikací navzájem, měl by být popsán ve zvláštním dokumentu. [1]

3.1.3 Požadavky na centrální ovládací zařízení

Centrální ovládací zařízení se dělí do dvou tříd, dle svých možností.

- Třída 1 - Pouze pro zobrazování informací, neustálá obsluha, signalizační zařízení umístěno ve stejné místnosti jako centrální ovládací zařízení
- Třída 2 - Kromě zobrazování informací lze použít i pro další činnosti (např. nastavení střežení systému), neustálá obsluha

Centrální ovládací zařízení musí:

- odpovídat správné třídě prostředí,
- být správně umístěno dle třídy prostředí,
- vyhrazeno pouze integrovanému poplachovému systému,
- opticky a akusticky signalizovat poruchy jednotlivých aplikací,
- detekovat výpadek monitorovací sekvence,
- monitorovat síťové připojení,
- signalizovat výpadek komunikace s některou z jednoúčelových aplikací,
- obsahovat záložní zdroj.

V případě poruchy centrálního ovládacího zařízení je třeba mít stanoven postup, díky kterému budeme schopni integrovaný poplachový systém ovládat i bez pomoci tohoto zařízení (postupy ovládání ústředěn příslušných jednotlivým systémům a jejich umístění).[1]

3.2 Technické požadavky na integraci kamerových systémů v bezpečnostních aplikacích

Kamerové systémy musejí, stejně jako všechny ostatní jednoúčelové aplikace splňovat požadavky normy ČSN CLC/TS 50398, ovšem pro konkretizaci požadavků na tyto systémy byla vydána další norma ČSN EN 50132 (Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích), kdy nejdůležitějšími částmi jsou ČSN EN 50132-1 (Část 1: Systémové požadavky) a ČSN EN 50132-7 (Část 7: Pokyny pro aplikace).

3.2.1 Stupně zabezpečení

Stejně jako u PZTS jsou i u kamerových systémů určeny čtyři stupně zabezpečení, od nichž se odvíjí požadavky na jednotlivá zařízení a jejich funkce:

Tabulka 2 Stupně zabezpečení pro kamerové systémy [15] a pro PZTS [17]

Stupeň 1 - Nízká rizika	Bez ochrany proti narušení a monitorování základních funkcí	Vetřelec má malou znalost PZTS a má omezený sortiment snadno dostupných nástrojů
Stupeň 2 - nízká až střední rizika	Jednoduchá ochrana proti narušení, bez monitorování základních funkcí	Vetřelec má omezené znalosti PZTS a má běžné nářadí a přenosné přístroje
Stupeň 3 - střední až vysoká rizika	Střední ochrana proti narušení, vyžadováno jednoduché monitorování základních funkcí	Vetřelec je obeznámen s PZTS a má rozsáhlý sortiment nářadí a přenosných elektronických přístrojů
Stupeň 4 - vysoká rizika	Vysoká ochrana proti narušení, vyžadováno stále monitorování základních funkcí	Vetřelec je schopen zpracovat podrobný plán vniknutí a má kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů PZTS

3.2.2 Funkční požadavky

Prvním požadavkem na kamerové systémy je schopnost správného zachycení obrazu a jednotlivých detailů v něm v závislosti na účelu, pro který byla kamera využita, tedy co vlastně má snímat a kontrolovat. Uvádí se 6 základních druhů snímání v závislosti na procentuální velikosti cíle na obrazovce.

- Prozkoumání - cíl zaujímá 400% výšky obrazu
- Identifikace - cíl zaujímá 100% výšky obrazu
- Rekognoskace - cíl zaujímá 50% výšky obrazu
- Pozorování - cíl zaujímá 25% výšky obrazu
- Detekce - cíl zaujímá 10% výšky obrazu
- Monitorování davu - cíl zaujímá 5% výšky obrazu [18]

Ovšem se zvyšující se kvalitou záznamu a různými typy rozlišení, v nichž jsou kamery schopny pořizovat záznam, již toto dělení není zcela vhodné, proto se upravuje vzhledem k jednotlivým rozlišením.

Podle jednotlivých stupňů zabezpečení jsou dále kladeny požadavky na následující funkce kamerového systému:

- propojení,
- zpracování obrazu,
 - zobrazení a analýza dat,
 - ukládání, archivace a zálohování dat,
- obsluhu systému,
- bezpečnost,
 - detekce poruch,
 - monitorování funkcí,
 - ochrana a detekce sabotáže,
 - zabezpečení dat. [15]

3.2.3 Integrace kamerových systémů v bezpečnostních aplikacích

Při integraci kamerového systému s dalšími aplikacemi musí být aplikovány obecné požadavky na integrované systémy (ČSN CLC/TS 50398) a veškerá společná zařízení musí splňovat požadavky všech aplikačních norem, jenž se na ně vzhledem k jejich funkci vztahují. Veškeré bezpečnostní požadavky, které jsou kladeny na kamerový systém dle normy ČSN EN 50132-1, musí být splněny i v případě, že bude ovládán jinou aplikací v rámci integrovaného systému. V tomto případě musí být aplikace ovládaná kamerovým systémem vnímána jako uživatel, který má jasně určeny přístupové práva. [15]

Kamerové systémy lze z hlediska bezpečnosti integrovat například s následujícími aplikacemi:

- poplachovými zabezpečovacími a tísňovými systémy,
- systémy kontroly vstupu,
- elektrickou požární signalizací,
- dalšími kamerovými systémy,
- dohledovými poplachovými a přijímacími centry,
- systémy inteligentní elektroinstalace.

Nejčastěji jsou však kamerové systémy integrovány se systémy kontroly vstupu nebo poplachovými zabezpečovacími a tísňovými systémy. Důležitými aspekty při integraci těchto systémů jsou zejména:

- definování způsobu propojení s těmito systémy (pomocí zásuvných modulů, driverů, vstupů a výstupů),
- možnost ovládání některých funkcí kamerového systému prostřednictvím externě aktivovaných událostí, časově závislých událostí, poplachových podmínek či manuální aktivací obsluhou,
- společná zařízení musí vyhovovat požadavkům všech aplikací, které zařízení využívají,
- rozhraní mezi jednotlivými aplikacemi mohou řídit přenos dat, vzájemné řízení systémů a společné databáze,
- kompatibilita z hlediska přenosu a řízení video streamu, datového objemu videosignálu a synchronizace času. [8]

Při integraci kamerových systémů můžeme brát v úvahu dvě možnosti jak postupovat.

- Celý integrovaný systém navrhnout od jednoho výrobce, čímž si zajistíme kompatibilitu jednotlivých zařízení, avšak se ochudíme o možnost použít nejvhodnější zařízení pro danou situaci, pokud jej vybraný výrobce nenabízí.
- Navrhnout systém, který bude kombinovat zařízení různých výrobců, díky čemuž dosáhneme optimálních výsledků a jsme schopni systém vytvořit přímo na míru. V tomto případě ovšem musíme jednotlivé prvky integrovat například pomocí driverů, zásuvných modulů, nebo otevřených rozhraní. Tyto komponenty pak musí být kompatibilní s ČSN EN 50132-5-2 (Poplachové systémy - CCTV dohledové systémy pro použití v bezpečnostních aplikacích - Část 5-2: IP video přenosové protokoly). [18]

Dílčí závěr

Stěžejními normami pro zjištění požadavků na integraci kamerových systémů jsou normy ČSN CLC/TS 50398, ČSN EN 50132-1 a ČSN EN 50132-7. Podle těchto norem je třeba se řídit při realizaci integrovaných kamerových systémů, kdy norma ČSN CLC/TS 50398 nám udává základní požadavky na veškeré integrované systémy, asi nejdůležitějším pravidlem, kterým je nutno se řídit, je že se jednotlivé aplikace nesmí navzájem nepříznivě ovlivňovat a že u společných zařízení je nutné, aby vyhovovalo požadavkům každé aplikace, pro niž je využíváno (tedy nejpřísnějším požadavkům).

Na kamerové systémy se také podle normy ČSN EN 50132-1 vztahují požadavky podle stupňů zabezpečení, rozdílné od PZTS stupňů zabezpečení. Pokud se tedy jedná o integraci těchto dvou aplikací, musí být v každé kategorii splněny veškeré požadavky. Kamerový systém musí být kompatibilní s ostatními prvky integrovaného systému a může jimi být částečně ovládán.

II. PRAKTICKÁ ČÁST

4 ZPŮSOBY INTEGRACE KAMEROVÉHO SYSTÉMU

Jako veškeré poplachové a nepoplachové systémy lze i kamerový systém integrovat mnoha způsoby, například do zabezpečení budovy, nebo do systémů inteligentní elektroinstalace.

První otázkou, která se naskytuje, pokud chceme kamerový systém integrovat s jinými aplikacemi, je jakým způsobem budeme tento záměr realizovat. V oboru integrovaných systémů existuje mnoho různých způsobů integrace, jež lze rozdělit do dvou základních kategorií a to hardwarová integrace a softwarová integrace.

Pokud se jedná o hardwarovou integraci, systémy jsou propojeny pomocí svých vstupů a výstupů a zejména u poplachových zabezpečovacích a tísňových systémů pomocí dalších nadstavbových modulů, jež jsou schopny ovládat i další poplachové a nepoplachové aplikace k nim připojené.

V případě, že se rozhodneme integrovat systémy pomocí softwaru je řešení obvykle takové, že jsou jednotlivé aplikace, poplachové i nepoplachové, připojeny na LAN (Local Area Network) síť, pomocí které komunikují se serverem, na němž je nainstalován integrační software, který řídí tyto aplikace a vztahy mezi nimi. [19]

Následuje výčet některých druhů integrace.

1) Hardwarová integrace

- IN/OUT integrace
- PZTS jako integrační prvek
- Integrace s využitím prvku kamerového systému
- Automatizační systém jako integrační prvek

2) Softwarová integrace

- Software ústředěn poplachových systémů
- Software pro uživatelskou správu
- Vizualizační software
- Integrační software systémů budov [8]

Výše uvedené druhy integrace jsou vhodné pro většinu typů poplachových a nepoplachových aplikací. Avšak pokud chceme zjistit, jestli lze tyto pravidla a metody aplikovat na kamerové systémy je třeba se pokusit je jejich praktické využití vzhledem ke kamerovým systémům.

4.1 Hardwarová integrace kamerového systému

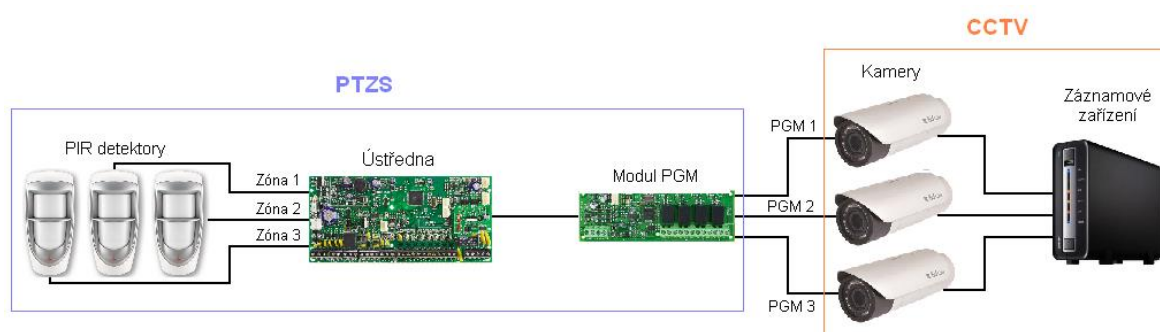
V následující podkapitole jsou popsány některé druhy hardwarové integrace kamerového systému s jinými aplikacemi na praktických příkladech. Na konci podkapitoly jsou zhodnoceny výhody a nevýhody jednotlivých druhů integrací a doporučeno řešení, které je, dle autorova názoru, nejefektivnější.

4.1.1 Integrace IN/OUT

Tento způsob integrace je vhodný při využití v menších budovách. Sice lze využít i rozsáhlých objektech, ale jeho konfigurace a instalace by byla velmi obtížná a uživatelský komfort pro správce či dohlížejícího pracovníka velmi nízký. [8]

Integrace IN/OUT je založena na propojování vstupů a výstupů jednotlivých systémů. Vzhledem k tomu, že některé IP kamery nabízejí poplachové vstupy a výstupy, mohou se tyto stát cestou k integraci kamery například s poplachovým zabezpečovacím a tísňovým systémem.

Jako příklad pro tento druh integrace jsem si vybral velmi jednoduchou variantu, kdy bude kamera ovládána ústřednou PZTS. Spolupráce bude probíhat ve chvíli kdy je vyhlášen poplach v prostoru, ve kterém se kamera nachází, ústředna vyše pomocí svého programovatelného výstupu signál pro zahájení záznamu, který kamera přijme svým poplachovým vstupem. Výhodou tohoto řešení je šetření místa na záznamovém zařízení z toho důvodu, že kamera nahrává pouze v případě poplachu. Schéma systému je zachyceno na obrázku 4.



Obrázek 4 Integrace IN/OUT pomocí PGM výstupů [20]

Detektory pohybu DG85 jsou rozmístěny v okolí zabezpečovaného objektu a připojeny ve smyčkách k ústředně SP6000 místního PZTS, který je vybaven modulem PGM4 pro rozšíření počtu programovatelných výstupů. Poblíž každého detektoru pohybu

je umístěna kamera WOB-100Ae, která je zapnutá, tudíž lze sledovat snímané prostory, ale nenahrává. Kamery jsou připojeny k jednotlivým programovatelným výstupům ústředny a při vzniku poplachu v dané lokalitě, je automaticky zahájen záznam, který se ukládá na záznamové zařízení VS-1004L. Oba systémy jsou navzájem oddělené a pracují samostatně, takže není problém zahájit záznam i jiným způsobem než při detekci pohybu v hlídání oblasti.

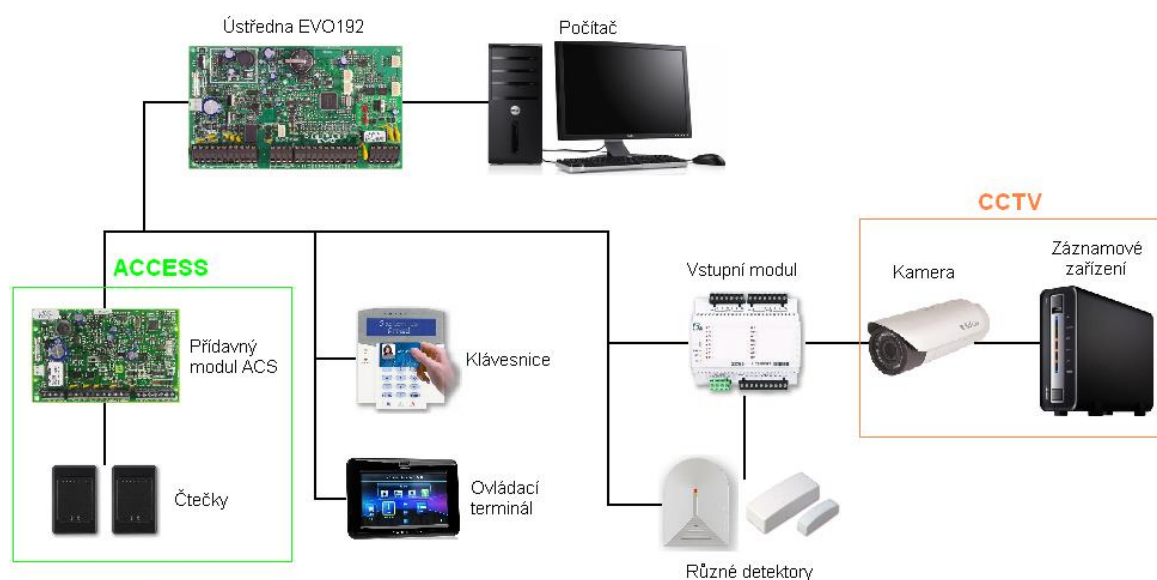
Podobně by šlo integrovat kamerový systém i se systémem přístupovým, kdy by kamera reagovala na vstup do místnosti a začala pořizovat záznam.

4.1.2 Ústředna PZTS jako integrační prvek

Pomocí integrace, kde hraje roli integračního prvku ústředna PZTS, je možné vystavět i velmi rozsáhlé systémy pro velké objekty, které ovládají nejen zabezpečovací prvky ale i prvky nepoplachových aplikací.

Tento způsob integrace je založen na připojení modulů jednotlivých ovládaných systémů na sběrnici, jejíž hlavním prvkem je ústředna PZTS.

Možností je opět velké množství, pro tento způsob integrace kamerového systému jsem si vybral případ, kdy jsou inteligentními kamerami nahrazeny detektory pohybu v objektu. Návrh systému je zobrazen na obrázku 5.



Obrázek 5 Integrace s ústřednou PZTS jako integračním prvkem [20]

Centrálním a zároveň integračním prvkem toho systému je ústředna Digiplex EVO192. Tato ústředna má na sběrnici připojený přídavný modul ACM12, který ovládá

přístupový systém, v další větvi má připojeny klávesnici K641R a ovládací terminál TM50, v další poté poplachové detektory (tříštění skla - DG457, magnetický kontakt – ZC1) a vstupní modul, který přijímá poplachové signály z poplachových detektorů a z kamer WOB-100Ae, jež jsou schopny detekovat pohyb a pomocí poplachového výstupu odesílat signál, čímž nahrazují běžné detektory pohybu. Kamery jsou dále připojeny k záznamovému zařízení VS-1004L.

Hlavním rozdílem v práci CCTV systému oproti případu s integrací IN/OUT, kterou jsem uváděl je směr komunikace. V prvním případě kamera přijímala signál od ústředny a reagovala na její podnět zapnutím nahrávání, zde naopak reaguje ústředna na podněty kamery vyhlášením poplachu v zóně kameře přiřazené. Zde již ovšem nejsou systémy na sobě nezávislé, jelikož ve chvíli kdy přestane fungovat systém CCTV, ztrácí ústředna PZTS schopnost detekovat pohyb v hlídaném prostoru.

4.1.3 Integrace s využitím prvku kamerového systému

Využití prvku kamerového systému jako integračního prvku je vhodné zejména u menších integrovaných systémů, které lze prakticky využít spíše v rodinných domech než v komerčních objektech.

Integračním prvkem může být IP kamera, nebo záznamové zařízení. Podmínkou je, aby tento prvek obsahoval digitální vstupy a výstupy, pomocí nichž bude komunikovat s ostatními zařízeními.

Pro příklad jsem si jako integrační prvek vybral IP kameru SONY SNC-RH124, která je vybaven 4 digitálními vstupy a 2 digitálními výstupy. Níže na obrázku 6 je vidět náčrt integrovaného systému, jehož integračním prvkem je tato IP kamera.

V tomto případě jsou využity tři digitální vstupy (1x detektor pohybu, 1x detektor tříštění skla a 1x magnetický kontakt umístěný na dveřích) a dva výstupy (siréna se světelnou a akustickou signalizací a světlo 12V). Jakmile jeden z detektorů zaznamená narušení chráněného prostoru, je rozepnut dveřní kontakt nebo kamera zachytí pohyb v oblasti (je také vybavena detekcí pohybu), začíná nahrávat video na záznamové zařízení, přičemž vysílá signál oběma digitálními výstupy pro aktivaci sirény a rozsvícení světla. Navíc, pokud je kamera připojena k internetu, má možnost odesílat obrázky na email nebo ftp server.



Obrázek 6 Využití IP kamery jako integračního prvku [20]

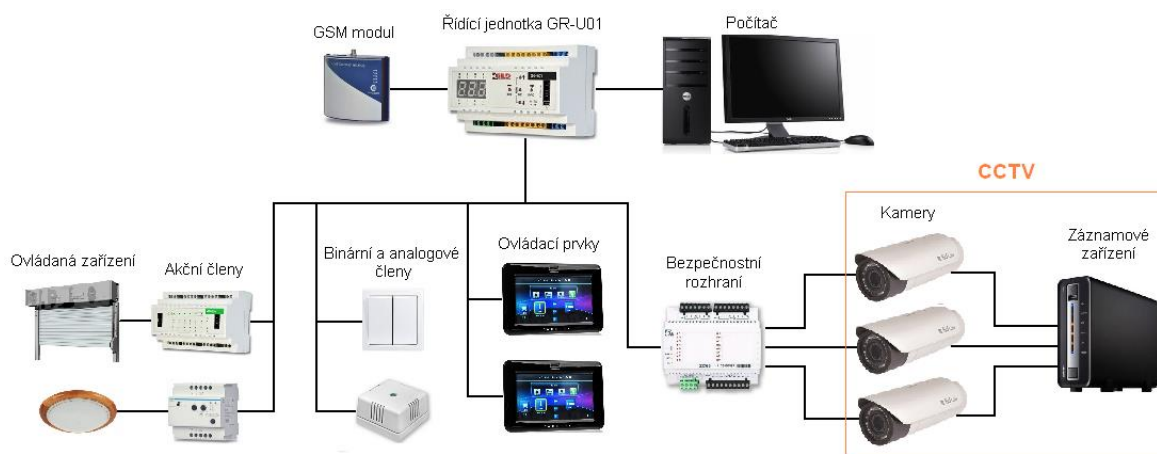
Při tomto druhu integrace je samozřejmě kamerový systém hlavním integračním prvkem. Kamera v tomto případě přijímá signál od detektorů, vysílá signál do ovládaných zařízení a zároveň může odesílat informace na internet a do záznamového zařízení. Systém ovšem může být nastaven různými způsoby, například kamera může v některých situacích hrát roli centrálního prvku a po podnětu od nějakého vstupního zařízení pouze vyslat signál do zařízení výstupního a sama na něj nereagovat (například při otevření dveří rozsvítit světlo).

4.1.4 Automatizační systém jako integrační prvek

Dále je možné integrovat pomocí automatizačního systému (systém inteligentní elektroinstalace), který ovládá technologie nacházející se v hlídaném objektu. Tento způsob integrace je vhodný zejména pro systém PZTS, nebo přístupové systémy. U kamerových systémů již tento druh integrace není natolik výhodný vzhledem k tomu, že podněty, na které reagují akční členy inteligentní elektroinstalace (teplota, světlo, přednastavený čas apod.) jsou pro kamerový systém obvykle jen málo důležité. Ovšem i zde lze pro kamerový systém najít uplatnění, zejména pokud podporuje inteligentní analýzu obrazu, především detekci pohybu.

Pro příklad uvádím dům s inteligentní elektroinstalací, v němž je místo PZTS systému využito zabezpečení na bázi kamerového systému. Tento systém je integrovaný s řídicí jednotkou GR-U01 inteligentní elektroinstalace pomocí bezpečnostního rozhraní. Ve chvíli kdy kamera snímající prostor pokoje zachytí pohyb, odešle signál centrální jednotce inteligentní elektroinstalace a počká na odezvu. Centrální jednotka vyhodnotí, zda

je majitel doma (a tudíž objekt odstřežen), nebo není (objekt je zastřežen). Pokud je majitel doma tak může například rozsvítit v dané místnosti světlo pomocí odpovídajícího akčního členu, a pokud není, poslat kameře příkaz k nahrávání a odeslat majiteli varovnou SMS pomocí modulu GSM.



Obrázek 7 Automatizační systém jako integrační prvek [20][21][22][23]

4.2 Softwarová integrace kamerového systému

Stejně jako pomocí hardware, lze i pomocí software integrovat kamerové systémy do jiných aplikací. Jsou různé programy pracující s kamerovými systémy, které jsou programovány dle účelu, ke kterému je třeba kamery využívat. V následující podkapitole jsou popsány některé způsoby softwarové integrace a softwarové nástroje, které lze využít pro práci s kamerovými systémy.

4.2.1 Způsoby softwarové integrace

Ještě před uvedením konkrétních příkladů jednotlivých softwarových nástrojů, vhodných pro integraci kamerových systémů, budou uvedeny obecné druhy softwarové integrace.

4.2.1.1 Software ústředěn poplachových systémů

Tyto typy softwarových nástrojů jsou vytvořeny zejména za účelem propojení ústředěn poplachových systému s počítačem, pomocí něhož jsou prováděny základní operace pro správu a konfiguraci systému. Programy jsou využívány zejména poskytovateli zabezpečení. Příkladem jsou programy WinLoad a BabyWare. [8]

Nástroje tohoto typu mohou mít vztah k integraci kamerových systémů v případě, že je celý systém založen na hardwarové integraci, kde je hlavním integračním prvkem ústředna PZTS.

4.2.1.2 Software pro uživatelskou správu

Software pro uživatelskou správu umožňuje uživateli spravovat nastavení centrálních jednotek systémů. Tato vlastnost uživateli umožňuje, vyjma běžného sledování a vyhodnocování práce systému, zejména následující funkce, které jsou praktické při práci se systémem samotným, ať už pro správce, či pro běžného uživatele:

- nastavování uživatelských profilů,
- vytváření popisů subsystémů, zón, terminálů,
- vytváření časových rozvrhů přístupu,
- přidělování a evidenci identifikátorů (karty, otisky prstů),
- filtrovat historii událostí (typ, čas, místo, osoba).

Posledním znakem těchto programů je, že obvykle nedisponují nástroji vhodnými pro vytvoření kvalitní vizualizace. [8]

Ačkoliv jsou tyto nástroje vyvíjeny zejména pro integraci PZTS systémů se systémy kontroly vstupu, jsou i takové, které splňují charakteristiku tohoto typu nástroje a pracují s kamerovými systémy. Příkladem takového softwaru je NetRex, který bude popsán níže.

4.2.1.3 Vizualizační software

Tento druh softwarové integrace navíc, oproti výše zmíněným typům, umožňuje vytvářet přehledné mapy systému založené na půdorysných plánech střežených objektů a v umístěných jednotlivých komponent systému (kamery, detektory pohybu, požární hlásiče, čtečky...).[19] Operátor, který kontroluje takovýto systém, má tak možnost v reálném čase sledovat veškeré procesy, které v systému probíhají v uživatelsky přehledném prostředí a zároveň je pomocí tohoto prostředí ovládat.

V tomto prostředí lze provádět následující akce:

- zapnutí/ vypnutí střežení subsystému nebo zóny,
- otevření dveří, zamknutí dveří,

- zapnutí kamery, zobrazení kamerou sledovaného prostoru, otočení kamery, aktivace inteligentních funkcí kamery (například sledování objektu)
- ovládání PGM výstupů. [8]

Jedná se o ideální typ softwarových nástrojů pro integraci kamerových systémů a to zejména pro jejich výbornou přehlednost, mnoho možností pro využití nadstandardních vlastností kamer a intuitivní ovládání.

4.2.1.4 Integrovaný software systémů budov

Jedná se o software využívaný při integraci bezpečnostních aplikací, ať už poplachových či nepoplachových, s inteligentní elektroinstalací budovy. Integrovaný software systémů budov má veškeré vlastnosti vizualizačního softwaru s rozšířením o možnost ovládání prvků budovy, které nemají důležitost z hlediska střežení objektu (topení, světla, rolety ... - ovládání těchto zařízení však může mít i bezpečnostní charakter, inteligentní elektroinstalace nabízí funkce jako je například simulace přítomnosti v objektu realizovaná náhodným rozsvěcováním světel, nebo prevence vzniku požáru realizovaná automatickým vypínáním určitých zásuvkových okruhů).

Stejně jako vizualizační software, je i tento typ integrace vhodný pro kamerové systémy, avšak vzhledem k tomu, že tyto nástroje zastřešují velké množství funkcí spojených se správou inteligentní elektroinstalace a ostatních systémů, je možné, že s jeho pomocí nebude možné využít veškeré možnosti, které nám některé vyspělé kamerové systémy poskytují.

4.2.2 Softwarové nástroje pro integraci kamerových systémů

Zde následuje popis vybraných softwarových nástrojů pro integraci kamerových systémů. Jsou zde zmíněny programy schopné integrovat kamerové systémy s dalšími poplachovými a nepoplachovými aplikacemi, čímž vytvářejí kompletní řešení pro provoz a zabezpečení jednotlivé budovy, či celé sítě budov.

4.2.2.1 VAR-NET Integral

Jedná se o software sestavený pro integraci systémů pro správu a bezpečnost budov, vizualizaci a celkové zvýšení efektivity jednotlivých aplikací i osob, které systém využívají. Pokud bych měl být zařazen mezi jeden z výše zmíněných způsobů softwarové integrace, tak se jedná o integrovaný software systémů budov.

Velkou výhodou programu VAR-NET Integral je přehlednost a rozsáhlý sortiment systémů, které je schopen integrovat a ovládat. Další výhodou programu je modularita celého systému, tudíž pokud si jej hodláme pořídit, nemusíme platit za funkce, které jsou pro nás zbytečné a které nijak nevyužijeme.

Zde je výčet modulů, které lze využívat při pořízení základní verze programu:

- komunikační okruh PZTS,
- komunikační okruh CCTV (10 kamer),
- rozšiřující licence CCTV o 10 kamer,
- komunikační okruh Access - přístupu/docházka,
- komunikační okruh EPS,
- komunikační okruh ENVIRO,
- mapové rozhraní - vizualizace a ovládání připojených technologií z mapového rozhraní + integrovaný vývojový nástroj, 2000 prvků bez omezení počtů map,
- docházka s limitem 25/50/100/150/200/400 osob,
- přístup Access s limitem 25/50/100/200/400/600/800 osob,
- export docházky - export docházkových dat do mzdových systémů,
- grafické plánování docházky,
- stravování – stravovací modul, kalkulace výdeje stravenek,
- modul návštěvy – správa návštěv (recepce, vrátnice),
- notifikace – zasilání vybraných událostí a požadavků prostřednictvím SMS nebo emailu,
- PDA klient – ovládání aplikace z mobilního telefonu. [24]

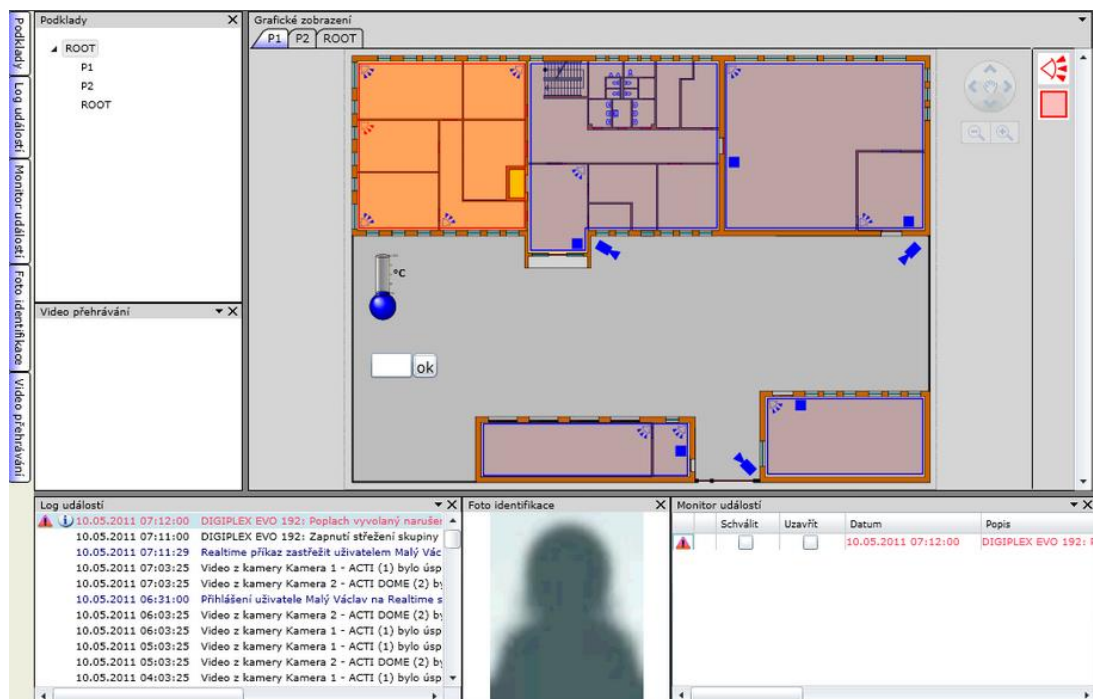
Pokud chceme dosáhnout co nejlepší cenové dostupnosti, jsou zde určeny následující limity:

- okruhů, přičemž 10 kamer se počítá jako jeden okruh,
- 2 okruhy CCTV (max. 20 kamer),
- 2000 prvků celkem na neomezeném počtu obrazovek,
- 800 osob pro správu přístupu,
- 400 osob s docházkou. [24]

Tento program se zdá jako ideální řešení pro využití při softwarové integraci různých poplachových a nepoplachových aplikací a to jak z důvodu rozsáhlých možností, tak z důvodu přehlednosti. Na obrázku 8 je zobrazeno schéma propojení aplikací pomocí systému VAR-NET Integral a na obrázku 9 je vyobrazen poplach podsystemu v uživatelském prostředí tohoto programu.



Obrázek 8 Propojení aplikací pomocí systému VAR-NET Integral [25]



Obrázek 9 Prostředí programu VAR-NET Integral – vyhlášení poplachu [26]

4.2.2.2 Software firmy Milestone

Softwarové nástroje firmy Milestone jsou primárně určeny pro prvotřídní digitální správu a zpracování videoaplikací v instalacích založených na počítačových sítích. [27] U tohoto nástroje je problém se zařazením, jelikož kombinuje velké množství funkcí a obsahuje mnoho možností. Avšak vzhledem k tomu, že se zajímá zejména o správu systému se základem v počítačových sítích, má nejbliže k softwaru pro uživatelskou správu.

Milestone nabízí 7 základních typů programu, které jsou omezeny dle rozsahu kamerového systému:

- XProtect Go – až 8 kamer, 1 server,
- XProtect Essential – až 26 kamer, 1 server,
- XProtect Express – až 48 kamer, 1 server, podpora integrace,
- XProtect Professional – až 64 kamer, až 5 serverů, podpora integrace,
- XProtect Enterprise – neomezený počet kamer, více serverů, podpora integrace,
- XProtect Expert – neomezený počet kamer, centrální správa, více serverů, podpora integrace,
- XProtect Corporate – neomezený počet kamer, centrální správa, sdružené sítě, podpora integrace. [27]

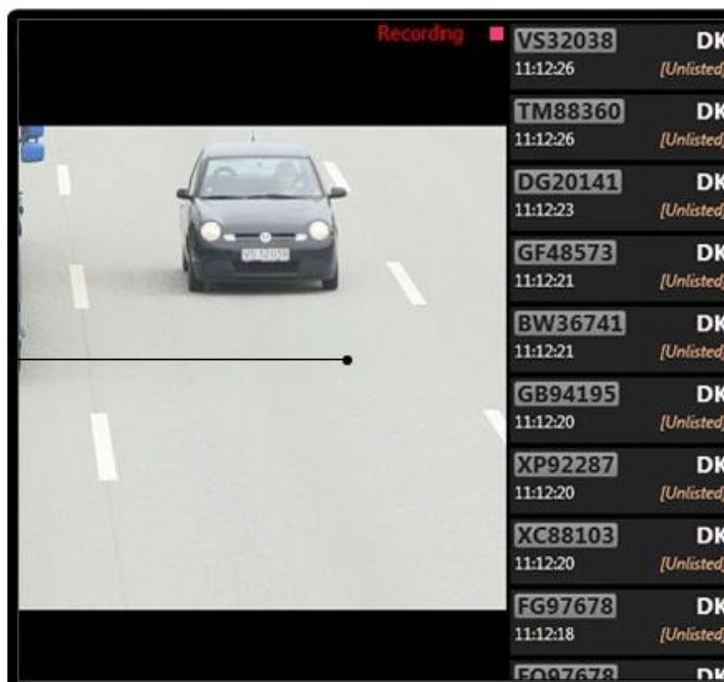
Podporou integrace je zde míněna možnost využít daný druh softwaru pro integraci s dalšími poplachovými a nepoplachovými aplikacemi. Z výčtu softwarových produktů lze tedy vidět, že první dva typy produktů nejsou vhodné pro integraci, tedy je třeba použít minimálně software typu XProtect Express abychom jej mohli využívat jako integrační software.

K těmto verzím lze přidávat další rozšiřující moduly, které jsou zaměřené na určitý typ analýzy videozáznamu, nebo integraci s dalšími aplikacemi.

Přídavné moduly

XProtect LPR

Tento modul umožňuje detekci RZ vozidel, kdy rozpoznané značky spolu s časem průjezdu ukládá do paměti spolu s videozáznamem. Zajímavou možností je nastavení určité RZ, na kterou systém majitele v případě průjezdu upozorní například zasláním SMS.



Obrázek 10 XProtect LPR – rozpoznávání RZ [28]

XProtect Retail a XProtect Transact

Tyto moduly lze využít zejména v obchodech, kde pomáhají při zjišťování podvodů a krádeží. Kamera je připojena na kasu a přitom snímá prostor kolem ní. Kdykoliv je zpětně možné podle zadané platby a jejího času rychle dohledat videozáznam. Tento systém lze integrovat také s bankomaty.

XProtect Screen Recorder

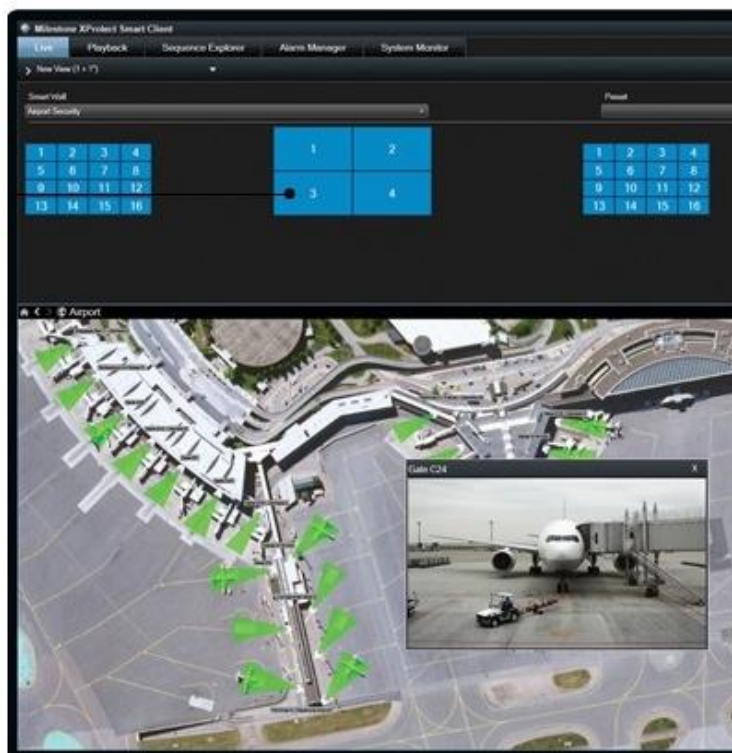
V tomto případě se jedná o program, který nahrává obrazovku terminálu kasovního systému, nebo počítače s operačním systémem Microsoft Windows. Záznamy jsou ukládány do databáze a spravovány stejně jako nahrávky z běžných kamer.

XProtect Utilities

Jedná se především o podpůrné nástroje, zejména pro instalační účely, správu a pro účely údržby softwaru firmy Milestone.

XProtect Smart Wall

Tento modul se zaměřuje především na zvýšení efektivity při kontrole kamerových systémů operátory. Zajišťuje intuitivní prostředí s vhodně rozmístěnými obrazy z jednotlivých kamer pro co nejefektivnější pozorování. Je praktický zejména při využití v dohledových centrech monitorujících velké množství kamer.



Obrázek 11 XProtect Smart Wall [29]

XProtect Plug-ins

Tyto pluginy jsou vyvinuty zejména pro integraci s dalšími zařízeními. V tomto modulu lze nalézt Input Unit Plug-ins a Software Plug-ins. Input Unit Plug-ins jsou využívány zejména pro připojení externích klávesnic, joysticků a podobných zařízení, které zjednoduší a zefektivní práci s kamerovým systémem. Software Plug-ins jsou určeny zejména k integraci se systémy třetích stran, tedy s dalšími poplachovými a nepoplachovými aplikacemi.

Programy firmy Milestone jsou základem celého kamerového systému a nabízí velké množství možností práce s kamerami a obrazem. Pomocí toho systému lze vytvořit zabezpečení založené kompletně na kamerových systémech, které bude zastupovat systém PZTS v mnoha ohledech. Samozřejmě tento systém nebude moci poskytnout stejné možnosti jako kvalitní PZTS, ale bude schopen detekce narušení pomocí detekce pohybu, nebo zvukové spouště alarmu. Velkou výhodou tohoto systému je možnost správy celé řady budov a přístupu k jejich zabezpečení pomocí internetu odkudkoliv na světě.

I přesto, že je tento program vyvíjen zejména pro práci s kamerami a počítačovými sítěmi, obsahuje i možnosti integrace s dalšími poplachovými a nepoplachovými

aplikacemi. Distributor uvádí integraci s přístupovými systémy, systémy inteligentní elektroinstalace a s kontrolními systémy užívanými v průmyslové výrobě.

4.2.2.3 *Omnicast, Genetec Security Center a Integra*

Omnicast

Softwarový nástroj Genetec Security Center je vylepšením dřívějšího nástroje s názvem Omnicast, který má velmi podobné možnosti jako výše zmiňované softwary firmy Milestone, jako třeba:

- přístup přes internet,
- analytické zpracování obrazu (tato možnost je u systému Omnicast ještě o trochu propracovanější, vzhledem k častému využívání například na letištích, kde lze nastavit například funkci jako detekce opuštěného zavazadla apod.),
- automatická detekce pohybu
- rychlé vyhledávání v záznamech (například vyhledávání záznamů spojených s určitou RZ).

Genetec Security Center

Pokud se jedná o samotný Genetec Security Center, obsahuje všechny funkce Omnicastu s důležitým vylepšením, a to možností integrace s dalšími poplachovými a nepoplachovými aplikacemi. Nejširší možnosti nabízí Genetec Security Center při integraci s přístupovým systémem, kdy je systém schopen, například sledovat pohyb osoby, která neprokázala svou totožnost při vstupu do hlídaného prostoru, po budově formou předávání informací od jedné kamery ke druhé.

Výpis některých funkcí Genetec Security Center, které uvádí výrobce:

- architektura zaměřená na dosažení co nejvyšší spolehlivosti,
- funkce produktu Omnicast,
- nástroje pro rychlé vyhledávání záznamů podle událostí,
- automatické vyvolávání a řízení poplachů,
- dobrá ovladatelnost pro uživatele,
- možnost rozdělení areálu do zón s různými režimy,
- možnost střežení několika areálů zároveň,

- vedení databáze uživatelů a jejich vstupních práv,
- přebírání identit uživatelů z Microsoft Active Directory,
- možnost připojit téměř jakoukoliv kameru,
- snadné rozšiřování systému o další kamery a jiná zařízení,
- možnost přístupu pomocí počítačů, tabletů a mobilních telefonů,
- zabezpečená šifrovaná komunikace. [30]



Obrázek 12 Prostředí programu Genetec Security Center [31]

Firma Integoo s.r.o., dodavatel těchto nástrojů, dále uvádí možnost integrace s dalšími systémy při spolupráci Genetec Security Center se softwarem Integra 3, jehož je také dodavatelem.

Integra 3

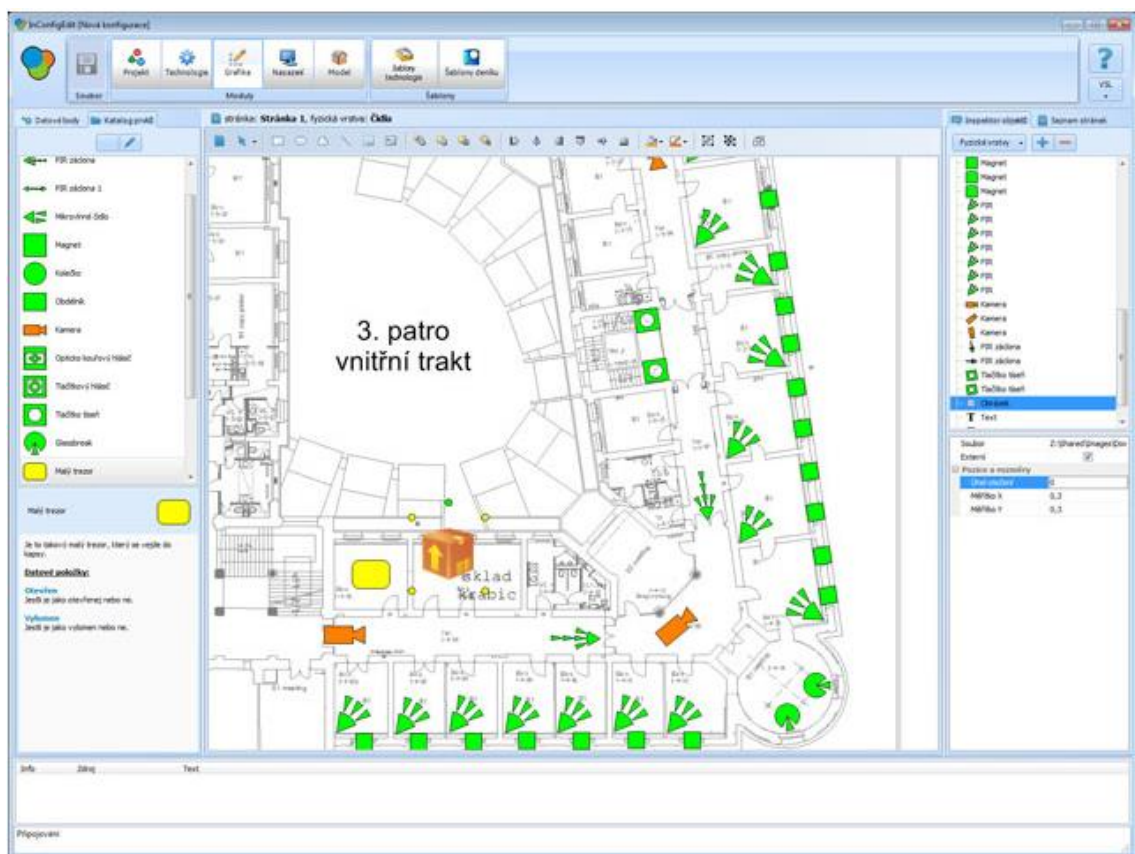
V sortimentu firmy Integoo s.r.o. se jedná o nástroj s nejrozsáhlejšími integračními možnostmi vzhledem dalším poplachovým aplikacím, určeným konkrétně pro ochranu před narušením střeženého prostoru.

Systém podporuje spolupráci poplachových zabezpečovacích a tísňových systémů, elektrické požární signalizace, Access systémů, kamerových systémů (Genetec Security

Center) a dalších nepoplachových aplikací připojitelných pomocí rozhraní I/O, MODBUS, OPC, TECO. [32]

Integra 3 je vhodná pro správu větších objektů. Pro kvalitní zabezpečení a kontrolu objektů je výborně vybavena (vizualizace, intuitivní ovládání a v podstatě veškeré vlastnosti, které byly popsány v souvislosti se systémem VAR-NET Integral). Spolupráce s Gentec Security Center jí přináší rozšíření o možnost správy pomocí připojení přes internet a možnosti inteligentní analýzy obrazu.

Poslední důležitou informací, kterou je nutno zmínit v souvislosti se softwarem Integra 3, je její velká variabilita vzhledem k aplikacím které spojuje, tedy je schopna zpracovávat data od zařízení téměř jakéhokoliv výrobce, ať už se jedná o PZTS, kamerový systém, systém kontroly vstupu, EPS, či další zařízení, která jsou vybavena vstupními a výstupními moduly.



Obrázek 13 Prostředí nástroje Integra 3 [33]

4.2.2.4 NetRex

Systém NetRex je rozdílný od výše zmíněných softwarových nástrojů. Jeho hlavním rozdílem je absence potřeby instalace softwaru a provozování serverů, které řídí kamerový systém. Celý systém je totiž provozovaný na serverech firmy NetRex s.r.o., ke kterým se zákazníci připojují pod svými uživatelskými jmény pomocí zabezpečeného internetového spojení. Vše co uživatel potřebuje ke správě svého kamerového systému je zařízení s připojením internetu (počítač, notebook, tablet, telefon ...) a uživatelské jméno a heslo. Jakmile je připojen má, kromě možnosti sledování záznamu (záznam uložený na serveru má nižší kvalitu než na lokálních záznamových zařízeních) či obrazu ze svých kamer, také možnost systém ovládat, například odesláním SMS zprávy v předdefinovaném formátu rozsvítit světlo připojené ke kameře u brány svého rodinného domu. [34]

Další velkou výhodou tohoto systému je jednoduchost připojení zařízení v terénu. Záznamové zařízení či IP kamery, které chceme provozovat, jednoduše připojíme k internetu a služba začíná být aktivní.

NetRex zároveň monitoruje připojená zařízení a při zjištění nějaké chyby, poruchy či narušení hlídaného prostoru může pomocí svého GSM modulu instalovaného u serveru odeslat SMS, která o tomto stavu ihned podá uživateli informace. Stejně takto může odesílat informace i na DPPC.

Poslední možností, kterou NetRex nabízí, je služba počítání lidí, která je pro bezpečnostní aplikace jen zřídka využitelná, avšak při instalaci kamer v obchodě může být použita pro analýzu produktivity prodeje (návštěvnost prodejny, přehled o počtu nakupujících oproti počtu návštěvníků) a měření efektivity marketingu (sledování vlivu uspořádání prodejny a skladby zboží na návštěvnost, vyhodnocení účinnosti marketingových akcí). [35]

Tento systém je vhodný zejména pro menší objekty, či při využití pouze jednotlivých kamer, pro větší objekty bude pravděpodobně neekonomický.



Obrázek 14 Prostředí systému NetRex [36]

Dílčí závěr

Kamerové systémy lze integrovat mnoha způsoby. Efektivnost jednotlivých druhů řešení závisí na tom, jaké představy o fungování systému má uživatel a o jaký typ a velikost objektu se jedná.

Pro malé objekty typu rodinných domů je pravděpodobně nejvýhodnější integrace IN/OUT, integrace s využitím prvku kamerového systému, nebo využití integračního softwarového nástroje NetRex.

Pro středně velké objekty jako jsou obchody nebo kancelářské prostory je také možné využít řešení integrací IN/OUT, dále pak variantu, kde hlavním integračním prvkem je ústředna PZTS, nebo využití některého z integračních softwarů jako je VAR-NET Integral, Integra, Gentec Security Center nebo XProtect Express.

Pro opravdu rozsáhlé objekty, či dokonce skupiny objektů je ideální využít zejména rozšířené verze programu XProtect.

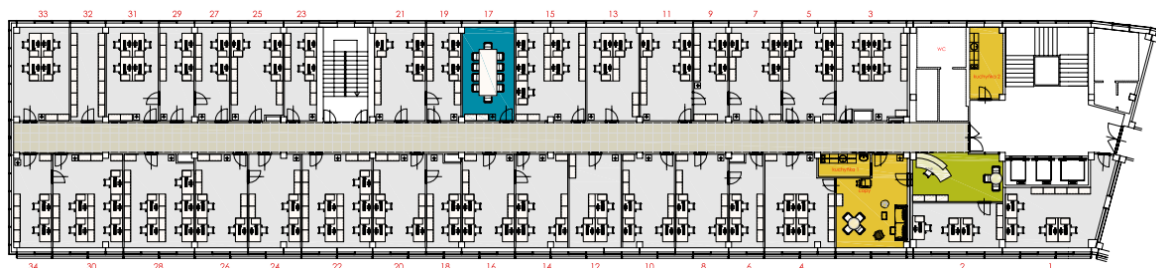
5 NÁVRH INTEGROVANÉHO KAMEROVÉHO SYSTÉMU

V další části práce jsem se rozhodl navrhnout integrovaný kamerový systém pro kancelářské prostory, jenž jsou pronajímány firmou XY a umístěné ve středu Brna, konkrétně v administrativní budově ABC na Botanická 597, Brno-střed, 602 00 Brno (názvy ani adresa neodpovídají skutečnosti, jsou použity pouze pro tento příklad návrhu systému). Firma XY zde pronajímá pouze část objektu, který je zobrazen na následujícím obrázku 15.



Obrázek 15 Fotografie objektu [37]

Kancelářské prostory, o které se budu zajímat při návrhu integrovaného kamerového systému, jsou ve čtvrtém patře sedmipatrové budovy, konkrétně v její části která se nalézá v křídle viditelném na obrázku 15. Plán kancelářských prostor je následně vidět na obrázku 16.



Obrázek 16 Plán kancelářských prostor [37]

V této části budovy se nalézají 32 kanceláří, zasedací místnost, čekárna pro zákazníky, 2 kuchyňky, sklad, toalety a recepce.

5.1 Bezpečnostní posouzení objektu

Důvodem zpracování bezpečnostního posouzení objektu je návrh integrovaného kamerového systému, který by měl zvýšit úroveň zabezpečení a celkově zvýšit komfort a úroveň celého kancelářského zařízení. Součástí systému by měl být také přístupový systém, který zjednoduší vedoucím pracovníkům dohled nad svými podřízenými a zároveň zabezpečí, že zaměstnanci nebudou navštěvovat prostory, které jim nejsou přímo určeny.

5.1.1 Zabezpečované hodnoty

Druh majetku

Pokud se jedná o druh chráněného majetku, tak většina cenných předmětů, jenž se v objektu nachází, jsou zejména počítačové sestavy. Vzhledem k tomu, že je zde až 32 využívaných kanceláří, ve kterých se nachází od dvou až po pět počítačových sestav na kancelář, je objem majetku opravdu značný. Kromě samotných počítačových sestav mají vysokou hodnotu také servery v serverovně, tiskárna v čekárně a projektor umístěný v zasedací místnosti. Zbylý majetek, jako například kuchyňské vybavení, kancelářské potřeby, nábytek a podobně, mají proti elektronice jen malý podíl na celkové hodnotě.

Další důležitou částí majetku jsou dokumenty, které budou používány firmou, jenž si bude prostory pronajímat. Zde se nejedná ani tak o hmotný majetek, jako spíše o majetek typu know how, interní firemní informace, diskrétní informace o zákaznících a zaměstnancích a podobně.

Objem majetku

Pokud začneme uvažovat o majetku z pohledu zloděje, zjistíme, že nejatraktivnější hmotnou položkou na seznamu se jistě stanou počítačové sestavy, kterých je zde mnoho a mají vysokou hodnotu. Nevýhodou pro zloděje je zde samozřejmě objem tohoto majetku. Pokud by se jednalo o krádež jednotlivého zařízení, je zloděj schopen jej odnést, ovšem pokud by se jednalo o zařízení více, muselo by se již účastnit více lidí. V tomto případě je zde mnohem vyšší pravděpodobnost neúspěchu pachatelů.

Dalším možným cílem pachatele může být nehmotný majetek umístěný ve formě informací a smluv jak v počítačových pamětech, na serverech, nebo uložené v kancelářích v papírové podobě. Tento druh majetku může mít pro pachatele různou hodnotu, dle toho o

jakého pachatele se jedná. Pokud se jedná o typického zloděje, kterému jde o majetek, tak je pro něj hodnota tohoto majetku nulová, avšak pokud se jedná o pachatele, jenž se chce nabourat do firmy pomocí zisku interních informací, smluv, či pokud ji chce pouze učinit problémy zničením tohoto majetku, můžeme jej považovat za hlavní cíl. Navíc vzhledem k jeho velmi malému objemu není problém jej odnést. [38]

V následující tabulce je přehledně uveden objem majetku a jeho atraktivita pro případného zloděje, kdy 1 je pro zloděje nejpříhodnější a 5 nejméně atraktivní. Hodnota v závorce je určena pro zloděje, který postrádá znalosti o tom, jak zpeněžit tento druh majetku.

Tabulka 3 Hodnocení majetku

Druh majetku	Hodnocení objemu majetku	Hodnocení atraktivnosti pro případného zloděje
Elektronika	3	2
Informace v papírové formě	2	1 (5)
Informace v datové formě	1	1 (5)
Nábytek	5	4
Kancelářské potřeby a kuchyňské vybavení	3	5

Poškození

Jelikož se budova nachází v rušné části prachy, tak by mohlo dojít k jejímu poškození vlivem vandalství, avšak vzhledem k tomu, že zájmová část této budovy je až ve čtvrtém patře jsem tuto možnost vyloučil z důvodu velmi malé pravděpodobnosti.

5.1.2 Budova

Konstrukce

Jedná se o standardní zrekonstruovanou vícepodlažní panelovou budovu. Střecha domu je betonová. Podlahy jsou betonové, na nichž je položena dlažba. Kabeláž ke světlům a jiným prvkům je tažena nově vybudovanými podhledy.

Otvory

I když má budova velké množství různých otvorů (několik vchodových, zadní a střešní dveře, velké množství oken), které skýtají mnoho možností pro přístup pachatele, tak se v našem návrhu budeme zajímat pouze o otvory, které tvoří přímý přístup do zájmového prostoru kanceláří. Zde se jedná hlavně o okna, dveře spojující kancelářský

prostor s dalším křídlem budovy, hlavní vstupní schodiště a evakuační schodiště a dveře k nim vedoucí.

Provozní režim objektu

V objektu se v pracovních dnech během dne běžně pohybuje velké množství pracovníků, zákazníků a dalších osob. Ve večerních a nočních hodinách a také ve dnech pracovního volna je objekt téměř prázdný s výjimkou jednoho postaršího strážného, který sedí v nejnižším patře budovy a jednou za hodinu objekt projde.

Lokalita

Pokud se jedná o lokalitu, ve které se objekt nachází, je to širší centrum Brna, tudíž je v okolí objektu velký počet pohybujících se osob a relativně vysoké riziko vloupání či vandalizmu. Poblíž objektu je mnoho různých cest, případně zastávek autobusu či tramvaje, které mohou tvořit únikovou strategii pachatele. Vzhledem k anonymitě života ve velkoměstě a velmi malé možnosti pachatele vypátrat a chytit po opuštění místa činu je ideálním prostředkem pro ochranu právě kamerový systém, který celý čin zaznamená. Přesné umístění objektu je vidět na obrázku 17.



Obrázek 17 Umístění zabezpečeného objektu [39]

Stávající zabezpečení

V současné době se v kancelářských prostorech nenachází žádný prvek zabezpečení. Jediným ochraným faktorem, který je v budově přítomen je strážný, který

hlídá budovu v hodinách volna. Avšak vzhledem k tomu, že většinu času tento strážný přebývá v nejnižším patře budovy, považují toto zabezpečení za téměř nulové.

Historie krádeží, loupeží a výhružek

Za poslední dva roky fungování této budovy zde došlo ke třem vloupáním, kdy se jednalo převážně o krádeže elektronického zařízení. Také zde došlo k několika vandalským útokům, které ovšem směřovaly pouze na první dvě patra budovy.

5.1.3 Vlivy působící na integrovaný systém a mající původ ve střeženém objektu

Vodovodní potrubí

Vodovodní potrubí nemůže mít žádný vliv na mikrovlnné detektory. Hlavním důvodem je absence vodovodního potrubí ve většině zabezpečovaných prostor. Jedinou částí kancelářských prostor, kam je potrubí dovedeno, jsou kuchyňky a toalety. Ovšem v blízkosti těchto prostor se neplánuje umístění žádných technických prostředků, na které by tento element mohl mít vliv.

Vytápění, vzduchotechnika, klimatizace

Vytápění je v budově realizováno pomocí elektrického topení umístěného v každé kanceláři u oken. Tyto zdroje tepla by mohly mít neblahý vliv na pasivní infračervené detektory pohybu, proto se v návrhu snažím vyvarovat nasměrování detektorů jejich směrem.

Zdroje světla

Pro osvětlení kancelářských prostor a přilehlých chodeb a schodišť jsou použity zářivky instalované do podhledů. Zářivky mohou mít neblahý vliv na funkci některých detektorů pohybu, z toho důvodu jsou pro použití uvažovány zejména detektory pohybu využívající alespoň dva typy detekce – duální detektory pohybu (pasivní infračervený + mikrovlnný detektor pohybu).

Pokud se zaměříme na vliv na kamery, tak vnitřní zářivkové osvětlení by pro kamery nemělo být problémem, naopak jedná se ideální typ osvětlení.

Elektromagnetické rušení

Vzhledem k tomu, že je plánováno celý systém realizovat s drátovým přenosem dat a informací by neměl být problém s elektromagnetickým rušením.

5.1.4 Vlivy působící na integrovaný systém a mající původ vně střeženého objektu

Dlouhodobě působící faktory

V okolí objektu se nachází mnoho pozemních komunikací, ať už větších, či menších, po nichž se pravidelně pohybují vozidla, avšak nepředpokládá se zde pravidelný pohyb velmi těžkých vozidel, který by měl za následek nežádoucí otřesy a vibrace v tomto objektu.

Krátkodobě působící faktory

V blízkosti objektu nejsou naplánovány žádné stavby domů, opravy pozemních komunikací ani jiné stavební práce. Pokud se jedná o přerušení dodávky elektrického proudu, tak tato hrozba je řešena dieselaagregátem umístěným na střeše budovy. Vzhledem k tomu, že samotný systém bude také disponovat záložním zdrojem napětí, se jeví výpadek proudu jako velmi malé riziko.

Zdroje světla

Sluneční světlo, které během dne vychází z oken, kterých je v tomto objektu velké množství, bude dělat problém, jak PIR detektorům pohybu (změny teploty), tak umístěným kamerám (neblahý vliv na záznam). Z tohoto důvodu musí být tyto komponenty umístěny tak, aby nesnímaly plochu oken.

Vlivy počasí

V lokalitě, ve které je objekt umístěn, není nebezpečí sesuvu půdy, zemětřesení ani jiných živelných pohrom s výjimkou povodní, ovšem vzhledem k tomu, že bude systém umístěn až ve čtvrtém patře budovy, můžeme i tuto hrozbu vyloučit. Jako další možné ohrožení se u takto vysoké budovy jeví zásah bleskem, avšak budova je proti tomuto jevu ochráněna kvalitními bleskosvody.

Vlivy klimatických podmínek

Na místě, kde je objekt umístěn, nedochází k závažným teplotním výkyvům. Teplota se zde během roku pohybuje v rozmezí od -20°C do $+40^{\circ}\text{C}$.

5.1.5 Stanovení stupně zabezpečení

Pokud vezmeme v potaz bezpečnostní posouzení, tak z něj vyplývá, že chráněný objekt může být narušen zejména dvěma druhy pachatelů – zloději, kteří mají v úmyslu ukrást hmotný majetek v co nejvyšší peněžní hodnotě, a lidé najmutí konkurenčními

podniky, jenž se snaží odcizit či zničit důvěrné firemní informace v datové či papírové podobě.

Z hlediska ochrany objektu je pro systém nebezpečnější člověk, jež se snaží ukrást informace, a to z toho důvodu, že můžeme předpokládat jeho velmi dobrou připravenost na prováděný čin a také dobrou vybavenost technickými prostředky a znalost zabezpečovacích, kamerových i přístupových systémů.

Z těchto důvodů byl stanoven druhý stupeň zabezpečení (nízké až střední riziko) jak pro kamerový systém, tak i pro PZTS.

5.1.6 Stanovení tříd prostředí

Vzhledem k tomu, že je celý objekt trvale vytápěn a komponenty systému budou uvnitř budovy v pokojích, nanejvýše na chodbách, byla stanovena 1. třída prostředí pro kanceláře, kuchyňky, zasedací místnost, čekárnu pro zákazníky, recepci i chodbu, a 2. třída prostředí pro evakuační schodiště.

5.2 Návrh zabezpečení

Kamerový systému jsem se rozhodl integrovat se systémy PZTS, Access a EPS. V tomto případě se bude jednat o integraci pomocí softwaru, jenž bude všem systémům nadřazen. Tímto softwarem bude VAR-NET Integral, jenž bude integrovat bezpečnostní technologie do jednotného prostředí s požadavkem na komplexní přehled a evidenci všech zásahů a činnosti ve střeženém prostoru.

Jednotlivé systémy:

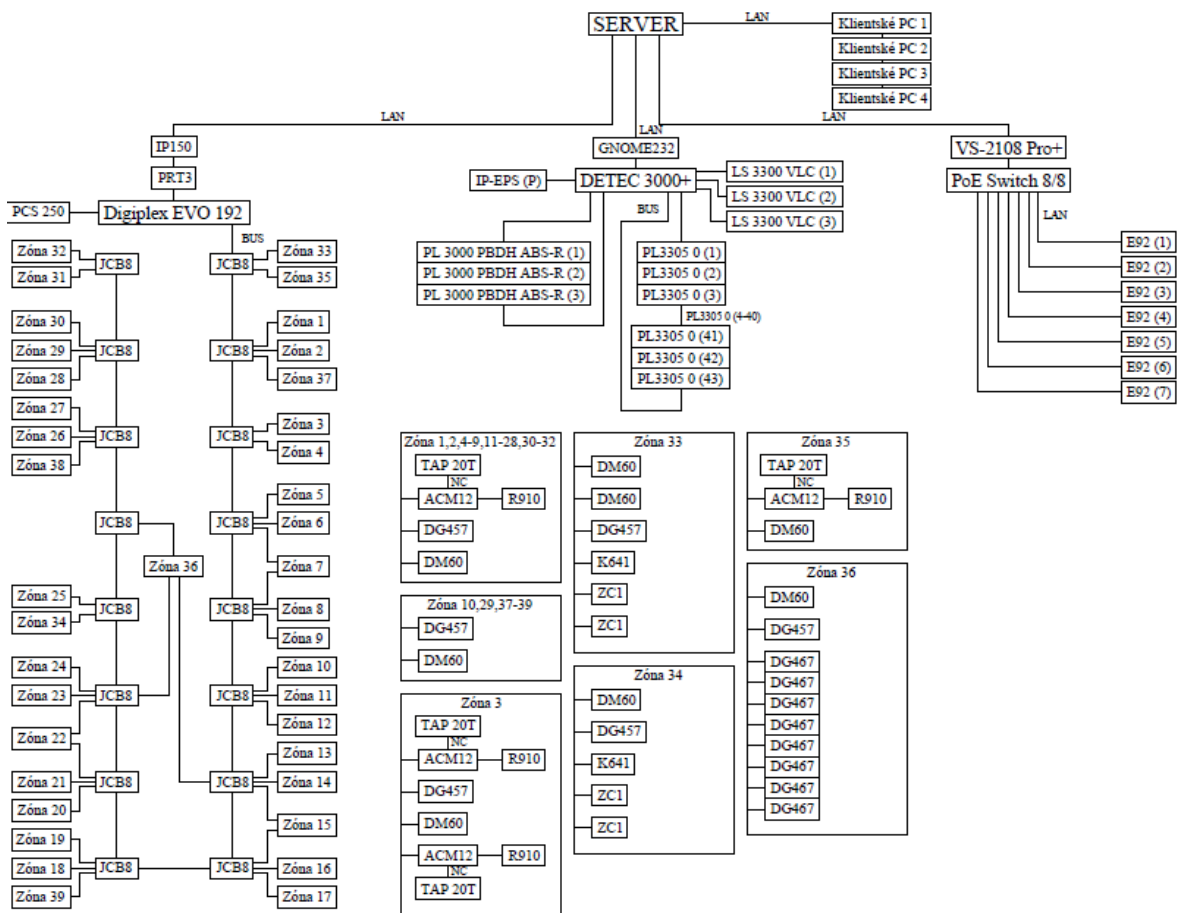
- CCTV, jenž bude zastoupena kamerami značky ACTi
- PZTS, jehož ústřednou je EVO192
- Access, který je řešen v rámci ústředny EVO192
- EPS, zastoupenou požární ústřednou Detect 3004+

Tyto jednotlivé celky budou fungovat jako samostatné systémy s tím rozdílem, že budou propojeny LAN sítí připojenou na server a klientské PC stanice. Úkolem serveru je nepřetržitě provozovat integrační a vizualizační software. Pomocí klientských stanic je možné se do systému kdykoliv připojit pomocí uživatelského účtu, kontrolovat a spravovat jej, dle možností a práv daného účtu.

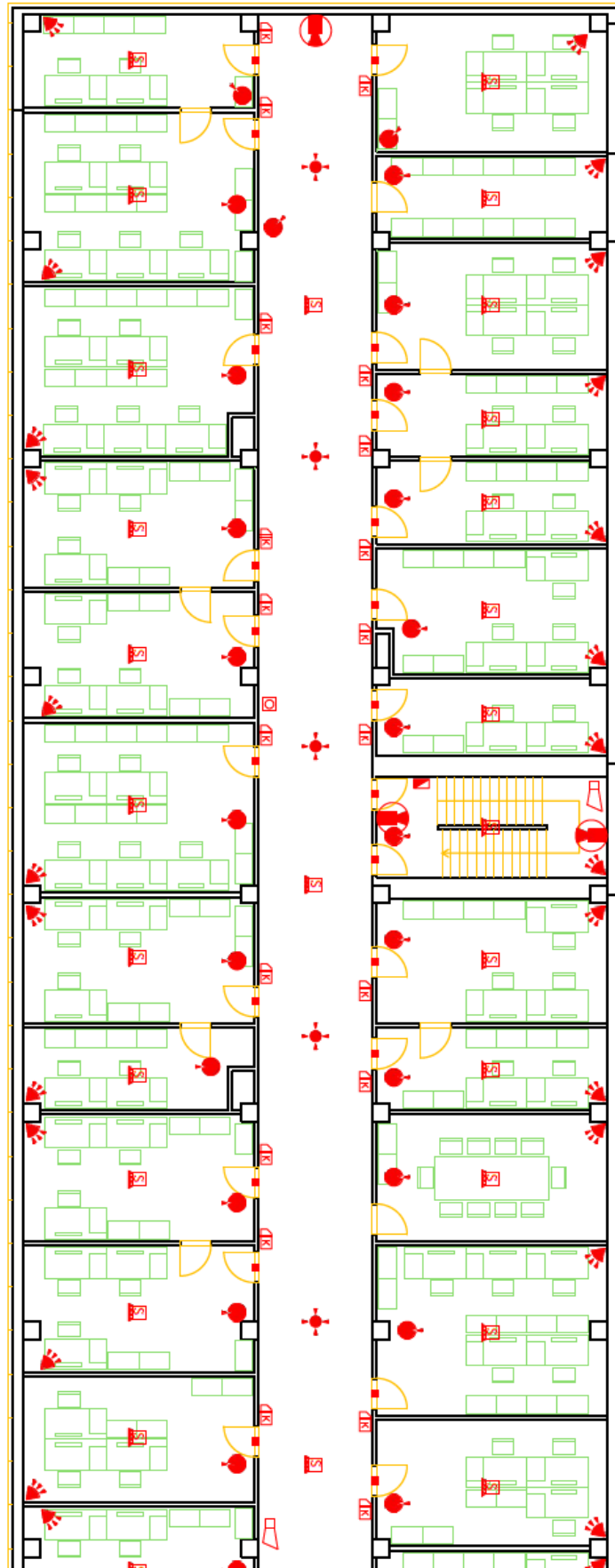
5.2.1 Náskres zabezpečení

V této části návrhu je postupně zobrazeno:

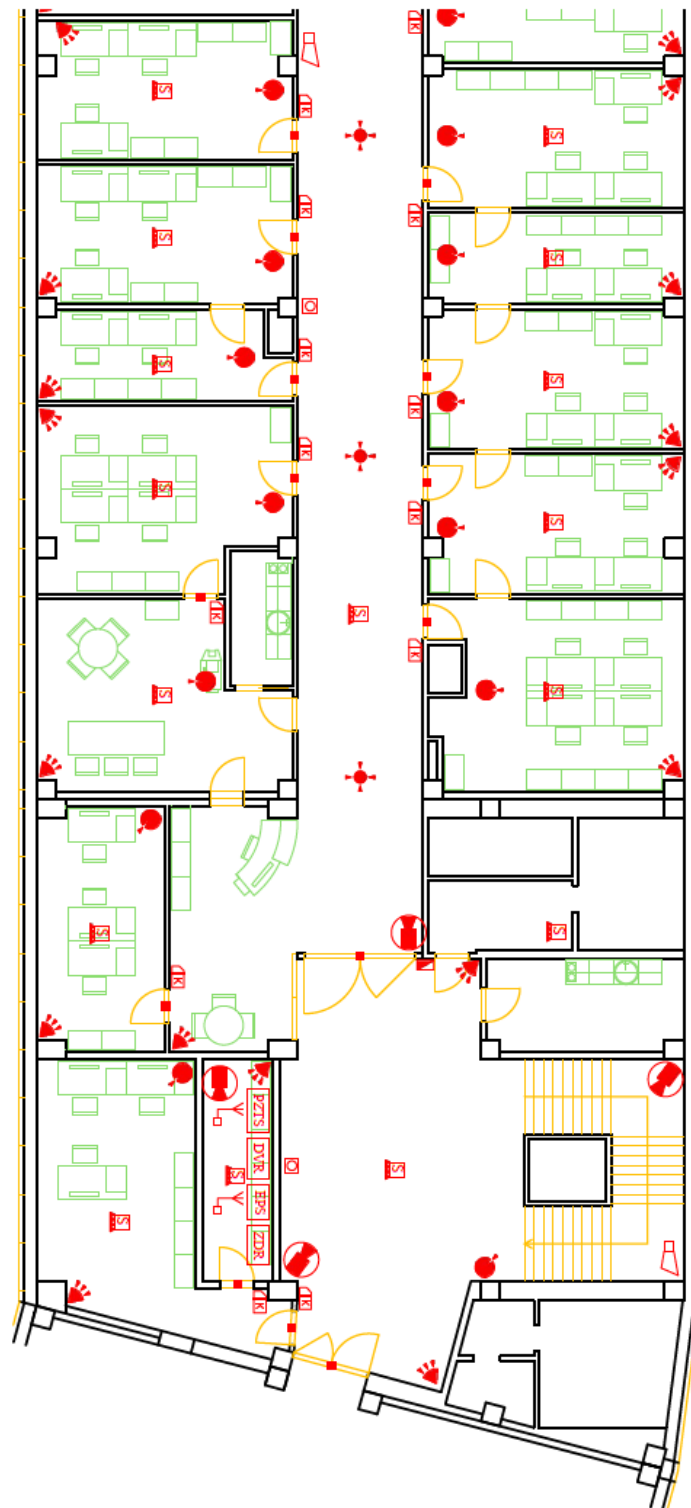
- schematické znázornění integrovaného kamerového systému
- schéma zakreslení použitých prvků v půdorysu
- legenda schéma zakreslení použitých prvků v půdorysu


















Obrázek 18 Schematické znázornění integrovaného kamerového systému



Obrázek 19 Zakreslení použitých prvků v půdorysu



Obrázek 20 Zakreslení použitých prvků v půdorysu

	Ústředna PZTS
	Záznamové zařízení systému CCTV
	Ústředna EPS
	Záložní zdroje
	IP dome kamera
	Stropní PIR detektor pohybu
	PIR detektor pohybu
	Detektor tříštění skla
	Magnetický kontakt
	Ruční požární detektor
	Bezdotyková čtečka s Access modulem
	Optickokouřový požární detektor
	Siréna
	GSM modul
	Klávesnice PZTS

Obrázek 21 Legenda pro nákres zabezpečení

5.2.2 Zvolené technické prvky

Integrační software

Jako integrační software byl zvolen systém VAR-NET Integral a to z toho důvodu, že je schopen integrovat všechny požadované aplikace, je i vizualizačním softwarem, což zvyšuje jeho efektivní využitelnost, a zároveň obsahuje mnoho modulů, které lze využívat dle potřeb zabezpečovaného objektu. Pro tento objekt byla vybrána verze obsahující:

- komunikační okruh PZTS,
- komunikační okruh CCTV (10 kamer),
- komunikační okruh Access - přístupu/docházka,
- komunikační okruh EPS,

- mapové rozhraní - vizualizace a ovládání připojených technologií z mapového rozhraní + integrovaný vývojový nástroj, 2000 prvků bez omezení počtů map,
- přístup Access s limitem 200 osob,
- notifikace – zasilání vybraných událostí a požadavků prostřednictvím SMS nebo emailu,
- PDA klient – ovládání aplikace z mobilního telefonu. [24]

Software bude nainstalován na serveru umístěném v serverovně. Klientské aplikace budou nainstalovány na počítačích, které si určí majitel. PDA klient bude nainstalován v mobilním telefonu vedoucího tohoto kancelářského úseku.

Poplachový zabezpečovací a tísňový systém

Všechny následující prvky poplachového zabezpečovacího a tísňového systému vyhovují určeným třídám prostředí i stupni zabezpečení.

Ústředna Digiplex EVO 192

Jedná se o řídicí prvek celého PZTS a Access systému. Tato ústředna byla vybrána hned z několika důvodů, a to:

- je vhodná pro střední a velké aplikace
- obsahuje nadstavbu přístupového systému
- kompatibilita se softwarovým nástrojem VAR-NET Integral

Ústředna je vybavena konfiguračním softwarem WinLoad, dále pak při verzi s nadstavbovým přístupovým systémem, která je zde použita, ještě softwarem NeWare Access. V případě, že nastane problém s hlavním integračním softwarem, jsou k dispozici tyto nástroje, které zajistí chod PZTS a Access systémů. Na desce ústředny je v základu 8 vstupů, kdy zde lze nastavit maximálně 16 adresovatelných zón. Vzhledem k tomuto faktu je jasné, že bude potřeba v systému využít expandéry. Dále je ústředna vybavena 5 PGM výstupy, z nichž 4 jsou opto-relé do 50mA a jeden je relé do 5A.

Jako řídicí prvek celého PZTS je ústředna umístěna v serverovně. Jedná se pravděpodobně o nejbezpečnější místo v budově z hlediska možnosti sabotáže.

Klávesnice K641

Jedná se standardní typ klávesnice s dvouřádkovým displejem a jednoduchým ovládáním.

V objektu jsou umístěny dvě klávesnice, kdy první klávesnice je na zdi u hlavních vstupních schodů a druhá vedle dveří u evakuačního schodiště.

Detektor pohybu DM60

Jedná se o quad detektor pohybu (detektor pohybu se čtyřnásobným prvkem), jehož dosah je 12 metrů a úhel záběru 110°.

Tento druh detektoru pohybu je využit zejména v jednotlivých kancelářích, kde jich je dohromady umístěno 34. Dva jsou umístěny u vstupního schodiště, jeden u evakuačního schodiště, jeden v serverovně, jeden v zasedací místnosti a jeden u recepce. Celkem je jich tedy v objektu 40.

Detektor pohybu DG467 Paradome

DG 467 Paradome je stropní duální detektor pohybu, který má elipsovitou charakteristiku snímání. Zorné pole tohoto detektoru má tvar elipsy o rozměrech 3 x 4 metry při montáži ve výšce 2,4 metrů (běžná výška patra v patrové budově).

V objektu je jich umístěno celkem 8 a to na chodbě vedoucí ke kancelářím. Jeden je dále umístěn v prostoru u recepce.

Detektor tříštění skla DG457 Glasstrek

Vzhledem k velkému množství oken jsou samozřejmě také využity detektory tříštění skla. Lze zapojit do standardní smyčky i na sběrnici. Dosah detektorů při nastavení vysoké citlivosti je 9 metrů, což je pro náš účel dostačující. Úhel záběru tohoto detektoru je 90° vertikálně a 70° horizontálně.

Detektory tříštění skla jsou umístěny v každé kanceláři (celkově 38 detektorů), navíc je jeden umístěn na chodbě vedoucí ke kancelářím, jeden u evakuačního schodiště a jeden v prostoru recepce.

Magnetický kontakt ZC1

Jedná se o sběrnice magnetické kontakty, které jsou využívány pro systém PZTS. Dva magnetické kontakty jsou umístěny u dveří k evakuačnímu schodišti, jeden na dveřích

mezi chodbou ke kancelářím a hlavním přístupovým schodištěm a jeden na dveřích vedoucích do další části budovy. Celkově se tedy jedná o 4 magnetické kontakty.

GSM/GPRS komunikátor PCS250

Pro přenos poplachového signálu na DPPC byl vybrán tento GSM/GPRS komunikátor. Kromě komunikace s DPPC přidává možnosti jako odesílání SMS při vykonání určených akcí ústřednou PZTS (poplach – včetně popisu zón, zapnutí, vypnutí, porucha).

GSM/GPRS komunikátor je umístěn stejně jako ústředna PZTS v serverovně.

Modul IP150

Pomocí tohoto modulu lze ústřednu propojit s počítačem po běžné LAN síti.

Modul IP150 je v objektu jeden a je umístěn stejně jako ústředna PZTS v serverovně.

Integrační modul PRT3

Jedná se o modul, pomocí něhož bude PZTS integrován s dalšími využívanými aplikacemi.

Integrační modul je umístěn stejně jako ústředna PZTS v serverovně.

Přístupový systém

Modul ACM12

Jako hlavní prvek přístupového systému je zde Modul ACM12, který je určen k vytvoření přístupového bodu. Tento modul lze využít k vytvoření jednoho přístupového bodu, tedy pro jedny dveře. Modul obsahuje vstup pro 1 čtečku a 2 detektory, které monitorují průchod dveřmi (magnetický kontakt, PIR detektor), dále pak relé pro odemykání elektronického zámku.

Moduly jsou umístěny u každých monitorovaných dveří, je jich tedy v objektu umístěno celkově 32.

Čtečka karet R910

Jedná se o čtečku karet pro vnitřní i venkovní využití. Pomocí identifikační karty přiložené k této čtečce může tedy její majitel procházet předem nadefinovanými dveřmi, dle svých přístupových práv v systému.

Čtečky jsou, stejně jako moduly ACM12 umístěny u každých monitorovaných dveří, tudíž jich v objektu nalezneme 32.

Magnetický kontakt TAP 20T

Magnetický kontakt je instalovaný na každých dveřích v objektu monitorovaných přístupovým systémem, tedy 32. Tento magnetický kontakt je určen přímo pro nastavbu Access z důvodu, že je u něj využíváno zapojení NC (normal closed).

Karta C706

Bezkontaktní karta pro průchod dveřmi zabezpečenými přístupovým systémem.

Jejich počet se odvíjí od počtu zaměstnanců a lidí oprávněných vstupovat do střežených prostor, jejich počet je tedy odhadnut na 70, kdy je uvažována určitá rezerva.

Kamerový systém

Záznamové zařízení VS-2108 Pro+

Centrálním prvkem kamerového systému je toto záznamové zařízení. Je určeno až pro 8 IP kamer, což nám v tomto případě bude stačit. Bylo vybráno zejména z těchto důvodů:

- počet připojitelných kamer,
- možnost vzdáleného i lokálního přístupu,
- inteligentní videoanalýza obrazu,
- nízká spotřeba,
- možnost vytváření RAID pole,
- vestavěný operační systém Linux.

Záznamové zařízení bude umístěno, stejně jako ústředna PZTS a Access v serverovně pro ochranu před sabotáží.

IP kamera E92

Jedná se o minidome kameru, která bude svým designem i velikostí vhodná pro využití v hlídaném objektu. Tato kamera je schopná nahrávat až rychlostí 30 snímků za sekundu v rozlišení 1920 x 1080 px nebo 1280 x 720 px, nadále pak rychlostí 15 snímků za sekundu v rozlišení 2048 x 1536 px. Podporuje automatické funkce AGC (redukce šumu a zrnění), AWB (vyvážení bílé barvy), BLC (eliminace protisvětla), WDR FL (eliminace protisvětla), DNR (redukce šumu a zrnění), detekci pohybu a odesílání obrázků na email.

Nastavení je možné pomocí internetového prohlížeče Internet Explorer verze 8.0 a vyšší. Také má možnost využívat své vlastní paměti k záznamu obrazu, pokud je využita Micro SD karta, avšak vzhledem k tomu, že v objektu využíváme záznamové zařízení VS-2108 Pro+, nebudeme ji pořizovat. Kamera vyhovuje požadavkům normy ČSN EN 50132-7 pro rekognoskaci do 40 metrů vzdálenosti od kamery a pro identifikaci do 20 metrů do vzdálenosti od kamery (při rozlišení 1920 x 1080px), tudíž je pro využití v tomto objektu vhodná.

Kamery jsou rozmístěny v objektu tak, aby jejich oblast snímání neobsahovala okna, čímž je zajištěno, že záznam nebude negativně ovlivněn slunečním světlem vycházejícím z oken. Dále byl při umisťování kamer kladen důraz na to, aby mohly sledovat veškerý pohyb na přístupových schodištích a chodbách vedoucím k jednotlivým kancelářím. Navíc je jedna kamera umístěna v serverovně z důvodu větší kontroly centrálních zařízení. Celkově se zde nalézají 7 kamer.

PoE Switch 8/8

Jedná se o zařízení, které umožňuje na záznamové zařízení připojit až 8 kamer, které budou napájeny po síti podle normy IEEE 802.3af.

Switch je umístěn stejně jako všechny centrální prvky v serverovně.

Elektrická požární signalizace

Ústředna DETECT 3004+

Tato ústředna je centrálním prvkem elektrické požární signalizace ve střeženém prostoru. Je určena pro vnitřní prostředí, je vybavena dvěma vstupy pro kruhové smyčky o až 126 detektorech (mezi tyto prvky lze zařadit i další sirény, nebo majáky) a jedním výstupem pro sirénu.

Ústředna EPS je umístěna stejně jako ústředna PZTS a záznamové zařízení kamerového systému v serverovně.

Modul IP-EPS (P)

Tento modul umožňuje ústředně EPS vyslat poplašnou zprávu na DPPC hasičského záchranného sboru.

Umístěn, stejně jako ústředna EPS v serverovně.

Detektor PL3305 O

Jedná se o základní adresovatelný opticko-kouřový požární detektor kompatibilní s ústřednou DETECT 3004+. Lze u něj nastavit 5 stupňů citlivosti, jeho detekční plocha je 70 m² a je vybaven detekcí poruch a zaprášení komory. Byl vybrán právě tento detektor, protože je designově vhodný pro instalaci do podhledů.

Detektory jsou rozmístěny ve všech kancelářích a ve větších prostorech jako jsou chodby v patnáctimetrových rozestupech. Celkem se zde tedy nachází 43 detektorů.

Tlačítko PL 3000 PBDH ABS-R

Jedná se o tlačítko určené k manuální detekci požáru.

V objektu jsou umístěny tři, jedno v prostoru u vstupního schodiště a dvě na chodbě vedoucí ke kancelářím.

Siréna LS 3300 VLC a kryt AD

Siréna je využívána pro akustickou signalizaci detekce požáru. U tohoto modelu je třeba zvlášť dokoupit kryt, proto je v názvu uvedeno i jeho označení.

Sirény jsou ve střeženém prostoru umístěny celkem 3, kdy jedna je na chodbě vedoucí ke kancelářím, druhá u evakuačního schodiště a třetí u hlavního vstupního schodiště.

Záložní napájecí zdroje*AKKU HSS 12V/26Ah*

Jedná se o baterii s dlouhou životností a vysokou kapacitou.

V objektu budou využity 4 tyto záložní napájecí zdroje. Dva budou určeny pro ústřednu EPS, jeden pro ústřednu PZTS a Access a jeden pro záznamové zařízení kamerového systému.

5.2.3 Konfigurace systému

Celý integrovaný systém bude mít pouze 2 režimy, zastřeženo a odstřeženo, ve kterých budou jednotlivé aplikace nakonfigurovány níže popsaným způsobem.

Režim odstřeženo

Do režimu odstřeženo je systém převeden pomocí zadání šestimístného číselného kódu do jedné z klávesnic za současného použití čipové karty s odpovídajícími přístupovými právy.

Režim zastřeženo

Do režimu zastřeženo je systém převeden, stejně jako u režimu odstřeženo, pomocí zadání šestimístného číselného kódu do jedné z klávesnic za současného použití čipové karty s odpovídajícími přístupovými právy. Do tohoto režimu však nelze systém přepnout, pokud se v objektu nalézá ještě nějaká další osoba (o tom rozhoduje přístupový systém).

Dále může mezi režimy přepínat osoba s odpovídajícími právy pomocí integračního softwaru VAR-NET Integral.

Pokud se jedná o podrobné nastavení chování systému, bude rozčleněno do jednotlivých částí, podle typu aplikace, v nichž budou vždy definovány možné vzniklé události a odpovídající reakce systému.

Rozčlenění zón

Následující tabulka přehledně ukazuje rozdělení objektu do jednotlivých zón, jejich popis a nastavení. Zóny, které jsou nastaveny, jako okamžité vyhláší poplach ihned po detekci podezřelého chování v tomto prostoru. Zóny nastavené jako zpožděné mají nastaven limit 30 sekund po detekci poplachu, během kterého lze odstřežit systém pomocí přístupové karty a klávesnice v zóně umístěné a tím zrušit poplach. Zóny definované jako 24 hodinové jsou zapnuty nepřetržitě.

Tabulka 4 Nastavení zón

Zóna	Popis	Nastavení
1-32	Kancelářské prostory 1-32	Okamžitá
33	Vstupní schodiště a chodba	Zpožděná
34	Evakuační schodiště	Zpožděná
35	Serverovna	Okamžitá
36	Chodba ke kancelářím	Okamžitá
37	Čekárna pro zákazníky	Okamžitá
38	Zasedací místnost	Okamžitá
39	Sklad kancelářských potřeb	Okamžitá
40	Požární hlásiče	24 hodinová

5.2.3.1 Konfigurace kamerového systému

Režim odstřeženo

V případě, kdy je systém odstřežen, jsou kamery aktivní a pořizují záznam (na záznamech lze identifikovat osoby podezřelé ze spáchaných útoků na objekt, či osoby, jenž se pokusily o odcizení informací pomocí metod sociálního inženýrství). Vzhledem k faktu, že je záznam pořizován v tomto režimu neustále, není třeba uvádět přehled událostí a reakcí kamerového systému.

Režim zastřeženo

Při zastřeženém stavu systému kamery nepořizují záznam. Kamery v tomto režimu snímají danou oblast a jsou nastaveny na detekci pohybu. Pokud je v objektu šero, automaticky se aktivuje jejich vestavěný přísvit.

Pokud je některou z kamer detekován pohyb, nebo kteroukoliv součástí PZTS detekováno narušení chráněného prostoru, začínají kamery automaticky pořizovat záznam. V situaci kdy pohyb detekovala kamera, je odeslána informace o detekci pohybu, spolu s adresou kamery, která pohyb detekovala, ústředně PZTS, která tuto informaci dále vyhodnocuje (vyhlašuje poplach, nebo pokud se jedná o kameru ve zpožděné zóně, čeká na přihlášení uživatele a zadání kódu na klávesnici).

5.2.3.2 Konfigurace PZTS

Režim odstřeženo

V tomto režimu bude přístupový systém aktivní, PZTS bude aktivní pouze v zónách, ve kterých se podle přístupového systému nikdo nenachází (v místech, které nejsou monitorovány přístupovým systémem, jako je například sklad kancelářských potřeb, budou komponenty PZTS neaktivní).

Výskyt možných událostí v režimu odstřeženo a reakce na ně lze nalézt v následující tabulce.

Tabulka 5 Události a reakce – PZTS, stav odstřeženo

Událost	Reakce systému
Detekce pohybu v prázdné místnosti	Odeslání poplachové zprávy na DPPC, odeslání SMS řediteli
Detekce tříštění skla v prázdné místnosti	Odeslání poplachové zprávy na DPPC, odeslání SMS řediteli
Neoprávněný vstup – zpráva od přístupového systému	Odeslání poplachové zprávy na DPPC, odeslání SMS řediteli
Požární poplach – zpráva od EPS	Odeslání poplachové zprávy na DPPC HZS, odeslání SMS řediteli

Režim zastřeženo

Při zastřeženém stavu systému, jsou aktivovány veškeré prvky PZTS. V tabulce 5 lze vidět možné události a odpovídající reakce systému.

Tabulka 6 Události a reakce – PZTS, stav zastřeženo

Událost	Reakce systému
Detekce pohybu	Odeslání poplachové zprávy na DPPC, odeslání SMS řediteli
Detekce tříštění skla	Odeslání poplachové zprávy na DPPC, odeslání SMS řediteli
Detekce otevření dveří	Odeslání poplachové zprávy na DPPC, odeslání SMS řediteli
Požární poplach – zpráva od EPS	Odeslání poplachové zprávy na DPPC HZS, odeslání SMS řediteli

5.2.3.3 Konfigurace přístupového systému

Režim odstřeženo

Přístupový systém je aktivní pokud je systém odstřežen. Všichni uživatelé v systému vlastníci kartu mají možnost procházet dveřmi, pro které mají oprávnění. V tabulce 7 je uveden seznam uživatelů a jejich přístupová práva a zároveň práva k ovládání systému a v tabulce 8 reakce přístupového systému na jednotlivé události.

Tabulka 7 Uživatelská práva

Uživatel	Práva
Pracovník v kanceláři	Průchod dveřmi do své kanceláře
Uklízečka	Průchod veškerými dveřmi, kromě dveří do serverovny
Ředitel	Průchod veškerými dveřmi, odstřežení systému
Správce počítačové sítě	Průchod veškerými dveřmi
Recepční	Odstřežení systému
Návštěva	Podle druhu návštěvy jsou nadefinována různá přístupová práva

Tabulka 8 Události a reakce – přístupový systém, stav odstřeženo

Událost	Reakce systému
Neoprávněný vstup – otevření monitorovaných dveří bez použití přístupové karty	Nahlášení neoprávněného vstupu ústředně PZTS
Vstup mimo pracovní dobu – uživatel má do těchto prostor přístup, ale vstupuje zde mimo svou pracovní dobu	Upozornění zaslané integračnímu softwaru
Pokus o neoprávněný vstup – uživatel se pokusil o vstup do prostor, pro které nemá definována přístupová práva	Upozornění zaslané integračnímu softwaru
Požární poplach – informace od EPS	Odemčení zámků u všech ovládaných dveří s výjimkou serverovny, pokud se v ní nikdo nenachází

Režim zastřeženo

V tomto režimu je detekován jakýkoliv průchod dveřmi jako neoprávněný a je odeslána poplachová zpráva ústředně PZTS, která následně vyhláší poplach.

5.2.3.4 Konfigurace EPS

Elektrická požární signalizace a všechny k ní připojené zařízení jsou aktivní 24 hodin denně. Jejich reakce na události jsou vypsány v následující tabulce.

Tabulka 9 Události a reakce – EPS

Událost	Reakce systému
Detekce požáru	Odeslání poplachové zprávy na DPPC HZS, odeslání SMS řediteli, odeslání informace přístupovému systému a systému PZTS, aktivace sirén
Aktivace tlačítka pro ruční detekci požáru	Odeslání poplachové zprávy na DPPC HZS, odeslání SMS řediteli, odeslání informace systému PZTS aktivace sirén

5.2.4 Hlášení poplachuPoplach zabezpečovacího systému

Ohlášení poplachu probíhá pomocí GSM/GPRS komunikátoru PCS250. Při vzniku poplachové události komunikátor nejprve zahájí předávání informací na DPPC. Dále systém bude postupovat v rozeslání poplachových textových zpráv SMS majitelům objektu popřípadě hlasových zpráv. Pokud během předávání poplachových informací z komunikátoru dojde ke zrušení poplachu uživatelem, je činnost komunikátoru přerušena. Komunikace na DPPC se uskuteční vždy kompletně.

GSM/GPRS komunikátor PCS250 má kromě odesílání poplachových zpráv na DPPC ještě další možnosti jako odesílání SMS, ve kterých je přesně popsán typ poplachu a zóna ve které poplach nastal (bude využito), dále SMS o zastřežení, odstřežení, poruše, či obnově systému. Dále lze připojit hlasový modul pro přenos hlasových zpráv (nebude využit).

Druhy poplachů jsou následující:

- poplach po zapnutí napájení,
- poplach v okamžité smyčce,
- poplach ve zpožděné smyčce,
- požární poplach (pouze prostřednictvím EPS),
- sabotáž,
- překročení počtu pokusů o zadání kódu,
- porucha zařízení.

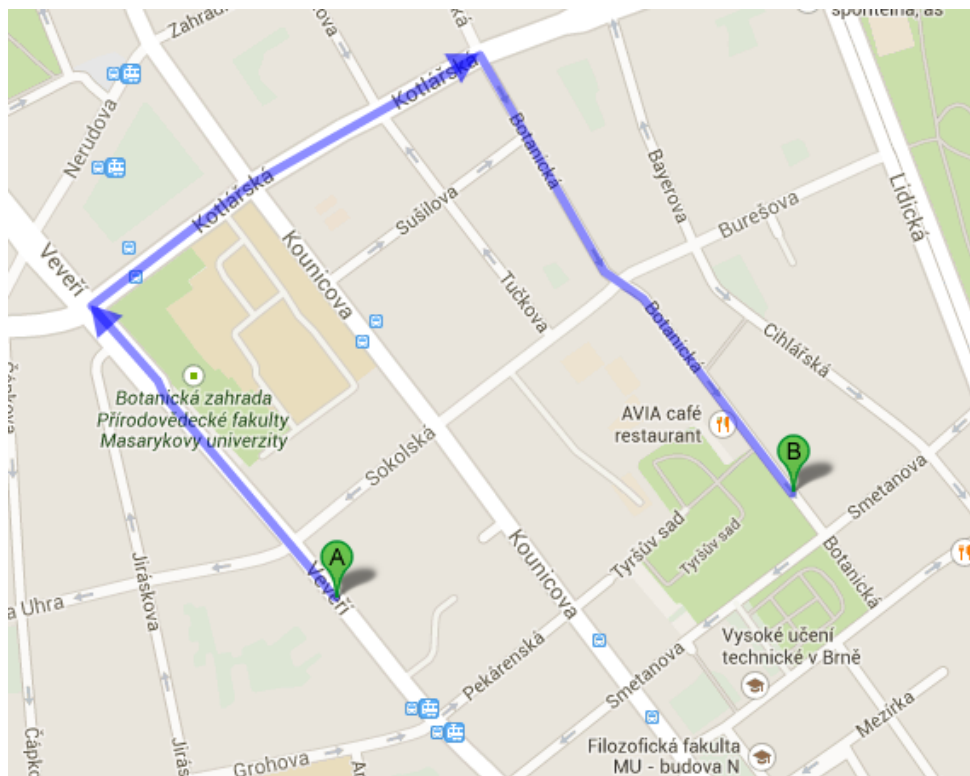
Požární poplach

Systém EPS je vybaven modulem IP-EPS (P), který je určen pro přenos poplachové zprávy na DPPC HZS. Tento poplach je vyhlášen jak po detekci požáru jakýmkoliv z detektorů PL3305 O, tak po ruční aktivaci jednoho z tlačítek PL 3000 PBDH ABS-R.

Při vyhlášení požárního poplachu, je pro jistotu navolena volba odeslání informace o požárním poplachu systému PZTS, který jej následně také může vyhlásit. Tato redundance je použita z důvodu maximální spolehlivosti (pokud by z nějakého důvodu modul IP-EPS (P) zprávu neodeslal, tak ji odešle komunikátor PCS250.

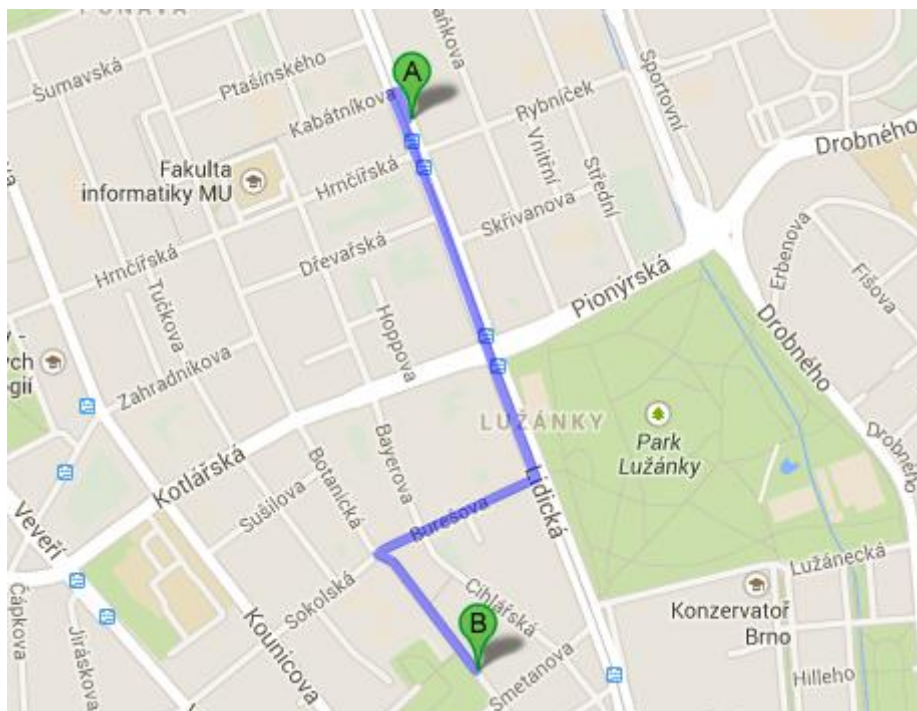
5.2.5 Zásah

Pro monitorování poplachu zabezpečovacího systému a případnou realizaci zásahu byla vybrána firma ALARM Comp, která je schopna zajišťovat monitoring objektů po celé republice. Společnost spolupracuje s PČR, jejíž sídlo se v Brně nachází pouze 1,3km od chráněného objektu (vzdálenost po pozemní komunikaci). Překonání této vzdálenosti by policii mělo trvat za mírného provozu 3 minuty a za hustého provozu nejvýše 6 minut.



Obrázek 22 Trasa od PČR (A) ke chráněnému objektu (B) [39]

Při aktivaci požárního poplachu bude zásah velmi rychlý, vzhledem k tomu, že se budova hasičského záchranného sboru nachází pouze 1,2km daleko (vzdálenost po pozemní komunikaci). Na následujícím obrázku je vidět trasa od budovy HZS k chráněnému objektu. Cesta by měla trvat asi 3 minuty při nízkém provozu, takže pokud budeme počítat i s provozem vysokým, tak by měly jednotky HZS k objektu dorazit do 6 minut.



Obrázek 23 Trasa od HZS ČR (A) ke chráněnému objektu (B) [39]

Pokud se jedná o cenu a typ monitoringu chráněné budovy, byla vybrána od společnosti ALARM Comp služba Dálkové střežení Fast Response pro objekty pro komerční využití. Společnost si za tuto službu bude pro chráněný objekt účtovat 3500 Kč měsíčně.

5.2.6 Údržba systému

Vzhledem k tomu, že se jedná o relativně rozsáhlý systém, který obsahuje velké množství prvků, je doporučeno si pro něj zařídit celoroční, pravděpodobně měsíčně placený, servis zajišťovaný specializovanou firmou. Nejlepší možností je zvolit firmu, která bude celý systém instalovat.

5.2.7 Finanční kalkulace

V následující tabulce je přehledně uvedena kalkulace návrhu integrovaného systému se všemi jeho součástmi. Jedná se pouze o systém, tedy součástí této kalkulace nejsou tarify za jeho údržbu a monitoring.

	Prvek	Počet kusů	Cena za kus	Cena za sadu
1	Software VAR-NET Integral	1	-	51992
2	Digiplex EVO 192 + K641+Box	1	5999	5999
3	Klávesnice K641	1	2699	2699
4	Detektor pohybu DM60	40	699	27960
5	Detektor pohybu DG467	8	699	5592
6	Detektor tříštění skla DG457	38	499	18962
7	Magnetický kontakt ZC1	4	699	5592
8	Modul IP150	1	3333	3333
9	GSM/GPRS komunikátor PCS250	1	4199	4199
10	Integrační modul PRT3	1	3599	3599
11	Modul ACM12	32	2699	86368
12	Čtečka karet R910	32	2499	79968
13	Magnetický kontakt TAP 20T	32	55	1760
14	Karta C706	70	139	9730
15	Záznamové zařízení VS-2108 Pro+	1	23599	23599
16	IP kamera E92	7	6399	44793
17	Ústředna DETECT 3004+	1	19999	19999
18	Modul IP-EPS (P)	1	4690	4690
19	Detektor PL3305 O	43	1775	76325
20	Tlačítko PL 3000 PBDH ABS-R	3	1499	4497
21	Siréna LS 3300 VLC a kryt AD	3	2299	6897
22	AD kryt ploché sirény	3	77	231
23	Svorkovnice SDB 3000	46	139	6394
24	AKKU HSS 12V/26Ah	4	1599	6396
25	Svorkovnice JCB8	16	399	6384
26	GNOME232	1	3375	3375
27	PoE Switch 8/8	1	3799	3799
28	Kabeláž	-	-	12297
29	Montážní a konfigurační práce	-	-	150000
Cena celkem:				677429

Dílčí závěr

Pro určenou budovu bylo zpracováno bezpečnostní posouzení a v návaznosti na něj navrhnout integrovaný systém.

Tento systém, pomocí softwaru VAR-NET Integral, integruje kamerový systém, poplachový zabezpečovací a tísňový systém, přístupový systém a elektrickou požární signalizaci. Z důvodu kompatibility jsou téměř všechny prvky systému vybrány u jednoho dodavatele, firmy VARIANT plus s.r.o., který zároveň poskytuje i využívaný integrační software.

Vzhledem k tomu, že jsou v tomto návrhu integrovány čtyři aplikace a střežený prostor je rozlehlý, je také cena tohoto systému značná.

6 VÝVOJOVÉ TRENDY V INTEGRAČNÍCH TECHNOLOGIÍCH KAMEROVÝCH SYSTÉMŮ

Následující kapitola obsahuje, kromě faktů, zejména osobní názor autora a jeho náhled do budoucnosti kamer, kamerových systémů a jejich možností integrace s ostatními aplikacemi.

6.1 Vývoj IP kamer a kamerových systémů

Dříve byly v kamerových systémech používány analogové kamery, dnes se od analogových kamer upouští a ve větší míře se, díky svým pokročilým možnostem, začínají využívat spíše IP kamery.

IP kamery a kamerové systémy se rychle vyvíjí, jde to znát i na faktu, že první IP kamera byla sestrojena v roce 1996 Martinem Grenem z Axis Communications. Od té doby uběhlo pouze 18 let a tyto kamery prošly opravdu velkou modernizací. V následující tabulce je vidět porovnání několika základních vlastností dnešní běžně využívané IP kamery (ACTi E53) a první IP kamery (Axis Neteye 200).

Tabulka 10 Porovnání IP kamer [40]

<i>Typ kamery</i>	<i>Nejvyšší rozlišení [px]</i>	<i>Snímkovací frekvence [snímky/s]</i>	<i>Minimální osvětlení [lux]</i>	<i>Rozměry[mm]</i>
Axis Neteye 200	352 x 288	0,05	10	155 x 125 x 48
ACTi E53	2048 x 1536	15	0,1	Ø128 x 99

Kromě toho, že dnešní IP kamery disponují mnohonásobně lepšími parametry, než kamery dřívější, mají také některé zabudovány inteligentní funkce analýzy obrazu, které byly již výše zmíněny.

Toto porovnání zde bylo uvedeno z toho důvodu, aby si čtenář udělal obrázek o rychlosti vývoje těchto systémů. Je velmi pravděpodobné, že za dalších deset let budou běžně užívané IP kamery disponovat parametry v řádech desítek Mpx, s rozsáhlými možnostmi zoomu a pokročilých inteligentních funkcí pro zpracování obrazu.

Další možností vývoje je zmenšování rozměrů kamer, ovšem tento scénář již nemá tak vysokou pravděpodobnost, jelikož pokud se ohlédneme zpět k porovnání první IP kamery Axis Neteye 200 a dnešní kamery ACTi E53, jejich rozměry se nijak výrazně nezměnily, což svědčí o tom, že tato velikost je pro kameru ideální.

Každopádně vlastností, na kterou se vývojáři IP kamer s největší pravděpodobností v budoucnu zaměří, budou jejich inteligentní a analytické funkce pro zpracování videozáznamu. Již v dnešní době se jedná u některých těchto funkcí o novinky a v tomto trendu bude vývoj nejspíše pokračovat.

Příklady moderních analytických funkcí IP kamer:

- PTZ Autotracking - aktivní sledování cíle pomocí automatického pohybu kamery, či pohybu více kamer sledujících pohyb narušitele po objektu,
- Evidence, počítání osob - pomůže například zjistit kolik osob se nachází v objektu,
- Rekognoskace osob – rozpoznání osoby (prováděno ve třech krocích - podle siluety osoby, tvaru tváře a nakonec podle obličejových znaků jako oči, uši, nos, ústa ...)
- Ochrana perimetru – detekce pohybu jen v části svého zorného pole kamery
- Monitorování délky zástupu lidí
- Rozpoznání RZ vozidla
- Detekce změny fyzické pozice IP kamery
- Detekce dynamiky pohybu – náhlé změny směru, pády apod.
- Detekce rychlosti pohybujícího se cíle
- Detekce zanechaného předmětu [13]

Pokud se jedná o záznamová zařízení, která k IP kamerám patří, jejich vývoj bude obsahovat zejména zvyšování kapacity pevných disků, zmenšování spotřeby, zvyšování počtu připojitelných kamer a zlepšování instalovaného ovládacího softwaru a operačních systémů. Dalo by se předvídat, že je nahradí počítače samotné, ovšem vzhledem k tomu, že je dodnes nenahradily, je možné, že to tak ještě nějakou dobu zůstane. Zde je několik důvodů proč využívat záznamové zařízení:

- PC je používáno k více činnostem, tudíž je možné, že by zasahovaly do funkcí záznamového SW a mohly snižovat jeho spolehlivost,
- nižší spotřeba,
- menší rozměry.

6.2 Vývoj integrace kamerových systémů

Pokud chceme odhadnout vývoj integrace kamerových systémů, musíme se opět ohlédnout do její krátké minulosti, či k jejím současným možnostem. Dříve byly kamerové systémy používány odděleně od ostatních systémů, tedy nedalo se hovořit o žádném druhu integrace, vyjma integrace s počítačem, který sloužil pro jejich nastavení. Dnes již máme mnoho možností jak kamerové systémy integrovat s ostatními poplachovými i nepoplachovými aplikacemi.

Nejmodernějším způsobem integrace prozatím zůstává softwarová integrace, kdy jsou využívány vizualizační nástroje a integrační softwary inteligentních budov. Nejnovějším fenoménem je možnost veškerého ovládání a sledování hlídaných prostor prostřednictvím internetových prohlížečů, či instalovaných aplikací odkudkoliv na světě, ať už z monitoru osobního počítače, notebooku, tabletu, nebo mobilního telefonu.

Dále jsou dnes kamerové systémy často integrovány s poplachovými zabezpečovacími a tísňovými systémy a přístupovými systémy. Je možné, že vzhledem k rychlému vývoji inteligentních analytických schopností kamer a jejich softwaru, se od tohoto trendu upustí a zabezpečovací systémy budou kompletně založeny pouze na kamerách a jejich analýze obrazu a budou integrovány pouze se zařízeními inteligentních domů.

Následují příklady nástrojů, které umožňují v dnešní době nejmodernější integraci kamerových systémů s různými aplikacemi.

- VAR-NET Integral – softwarový nástroj pro integraci převážně s aplikacemi typu PZTS, EPS a systémů kontroly vstupu
- XProtect od Milestone – softwarové nástroje zaměřené zejména na integraci s kasovním systémem a bankomaty v obchodech pro prevenci před krádežemi
- Genetec Security Center – software pro integraci více kamerových systémů v jeden celek s možností globální správy a přístupu přes internet
- NetRex – kompletní ovládání kamerového systému přes internet, kdy je správa vykonávaná poskytovatelem softwaru
- Kamery SICK – moderní kamery, s možnostmi 3D snímání (detekce tvaru objektu), využívané zejména při výrobních procesech potravin a nápojů

- Blumenbecker – kamerové systémy určené pro průmysl s možnostmi jako je měření různých rozměrů (rozteče, průměry děr, plochy, objemy), identifikace typu výrobku dle jeho tvaru, kontrola úplnosti výrobku, navádění robota pomocí kamery
- Produkty Hasselblad – firma se zaměřuje na vývoj zařízení s vysokým rozlišením a exkluzivní kvalitou obrazu, nabízí možnost rozlišení fotografie až 200Mpx, také nabízí software Phocus pro správu a integraci kamerových systémů
- Mallincam – kamery využívané pro astronomické pozorování
- Bolidové kamery – sítě vytvářené těmito kamerami slouží k automatické fotografické registraci průletu meteorů a bolidů a k následnému vypočítávání jejich místa dopadu – jedná se o speciální kamery vyráběné na zakázku obvykle výzkumnými středisky

Dílčí závěr

Pokud jde tedy o pohled do budoucna, tak vzhledem k rychlosti vývoje, o které bylo výše pojednáno, nelze zcela přesně odhadnout schopnosti kamerových systémů na další desítky let do budoucna, avšak je velmi pravděpodobné, že se budou kamerové systémy dále zdokonalovat, rozrůstat a budou součástí v podstatě všech integrovaných systémů a možná některé aplikace i zcela nahradí. Největší vývoj je očekáván u inteligentních analytických funkcí kamer, které jim umožňují vykonávat činnosti, pro které v dřívější době neměly možnosti ani předpoklady.

ZÁVĚR

V teoretické části je definováno co je to integrovaný systém, z jakého důvodu je využíván a co nám přináší. Jsou zde také vyjmenovány a krátce popsány některé typy poplachových a nepoplachových aplikací, které jsou do integrovaných systémů nejčastěji začleňovány.

V další části teorie jsou popsány kamerové systémy samostatně, zejména jejich skladba vzhledem k normě ČSN EN 50132-1. Dále jsou zde také popsány komponenty tvořící běžný kamerový systém.

Poslední částí teorie jsou technické požadavky na integraci, které jsou rozděleny do dvou částí a to obecných požadavků na integrované systémy a požadavků na kamerové systémy v bezpečnostních aplikacích. Zde jsou popsány požadavky norem, jimiž je nutno se řídit při návrhu takovýchto systémů.

První kapitolou praktické části je popis jednotlivých možností integrace kamerových systémů různými způsoby dle základních typů hardwarové i softwarové integrace.

Dále je v praktické části vypracován návrh integrovaného kamerového systému pro objekt komerčního typu, kdy je kamerový systém integrovaný s poplachovým zabezpečovacím a tísňovým systémem, elektrickou požární signalizací a přístupovým systémem.

Poslední částí této práce je kapitola, v níž je popsán pohled autora na budoucí vývoj kamerových systémů a jejich možností integrace.

Přínosem této práce je přiblížení pojmů souvisejících s integrovanými systémy, možnosti kamerových systémů, požadavky na tyto systémy vycházející z aktuálních norem, dále nastínění možnosti hardwarové a softwarové integrace těchto systémů, vypracování návrhu integrovaného kamerového systému pro objekt komerčního typu a nastínění možnosti vývoje jak samotných kamerových systémů, tak jejich budoucích možností integrace s ostatními aplikacemi. Dále by tato práce mohla být využita ke studijním účelům jako příklad návrhu integrovaného systému spolu s teorií s ním spojenou.

ZÁVĚR V ANGLIČTINĚ

In the theoretical part of thesis is defined what is an integrated system, why it is used and what brings to us. There are also listed and briefly described some types of alarm and non-alarm applications that are integrated into most systems.

In other parts of the theory are described camera systems separately, in particular their composition with respect to the standard EN 50132-1 . Furthermore, there are also described components that make up a normal camera system.

The last part of the theory is technical integration requirements, which are divided into two parts: the general requirements for integrated systems and requirements for CCTV systems in security applications. There are described the requirements of the standards that need to be followed in the design of such systems.

The first chapter of the practical part is a description of each option integration of CCTV systems in different ways according to the basic types of hardware and software integration.

Further, in the practical part, there is designed a draft of the integrated surveillance system for commercial object, where the camera system is integrated with the emergency alarm and security systems, electrical fire alarm system and access control system.

The last part is the chapter in which the author describes his view to the future development of camera systems and their integration options.

The contribution of this work is to describe terms associated with integrated systems, camera systems options, requirements for these systems, that are based on current standards, as well as outlining the possibilities for hardware and software integration of these systems, the drafting of an integrated surveillance system for commercial building type and outline a development of both the camera systems and opportunities for the future integration with other applications. Furthermore, this work could be used for study purposes as an example of an integrated system together with the theory associated with it.

SEZNAM POUŽITÉ LITERATURY

- [1] ČSN CLC/TS 50398. Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009.
- [2] VALOUCH, Jan. Projektování bezpečnostních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2012. ISBN 978-80-7454-230-5.
- [3] Integrované zabezpečovací systémy. EBIS [online]. 2013 [cit. 2014-01-03]. Dostupné z: <http://www.ebis.cz/cs/produkty-a-sluzby/integrované-zabezpečovací-systemy>
- [4] Poplachové zabezpečovací a tísňové systémy. EBIS [online]. 2013 [cit. 2014-01-03]. Dostupné z: <http://www.ebis.cz/cs/produkty-a-sluzby/integrované-zabezpečovací-systemy/pzts-ezs>
- [5] Přístupový systém. EBIS [online]. 2013 [cit. 2014-01-03]. Dostupné z: <http://www.ebis.cz/cs/produkty-a-sluzby/integrované-zabezpečovací-systemy/ekv-acs>
- [6] KOŇAŘÍK, Jan. Porovnání bezpečnostních systémů a systémů inteligentní elektroinstalace. Zlín, 2012. Bakalářská práce. Univerzita Tomáše Bati.
- [7] Elektronická požární signalizace. E+Mplus [online]. 2013 [cit. 2014-01-03]. Dostupné z: <http://www.emplus.cz/pozarni-signalizace>
- [8] VALOUCH, Jan. Projektování integrovaných systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2013. ISBN 978-80-7454-296-1.
- [9] Eiko s.r.o. [online]. 2013 [cit. 2014-04-2]. Dostupné z: <http://www.eiko.cz/ozvučovací-systemy-a-system-rizeni-jednotneho-casu/>
- [10] LOVEČEK, T., NAGY, P. Bezpečnostné systémy: kamerové bezpečnostné systémy. Žilina: Žilinská univerzita v Žilíně, 2008. 272 s. ISBN 978-80-8070-893-1
- [11] Kamerové systémy (CCTV). EBIS [online]. 2013 [cit. 2014-01-3]. Dostupné z: <http://www.ebis.cz/cs/produkty-a-sluzby/integrované-zabezpečovací-systemy/cctv>
- [12] Součásti síťové kamery. NetRex [online]. 2014 [cit. 2014-01-3]. Dostupné z: <http://www.netrex.cz/cz/podpora/kamerovy-system/ip-kamery/soucasti-ip-kamera/>

- [13] Lukáš, Luděk a kol., Bezpečnostní technologie, systémy a management II. 1. Vyd. Zlín: VeRBuM, 2012. 387 s. ISBN 978-80-87500-19-4
- [14] Alarm focus. Stará Boleslav: ORSEC s.r.o., 2013, roč. 2013, č. 2. ISSN 1805-9007.
- [15] ČSN EN 50132-1. Poplachové systémy - CCTV dohledové systémy pro použití v bezpečnostních aplikacích: Část 1: Systémové požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.
- [16] Posterus [online]. 2008 [cit. 2014-04-5]. Dostupné z: <http://www.posterus.sk/?p=16195>
- [17] Lukáš, Luděk a kol., Bezpečnostní technologie, systémy a management I. 1. Vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7
- [18] ČSN EN 50132-7. Poplachové systémy - CCTV dohledové systémy pro použití v bezpečnostních aplikacích: Část 7: Pokyny pro aplikace. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.
- [19] LOVEČEK, Tomáš. REITŠPÍŠ, Josef. Projektovanie a hodnotenie systémov ochrany objektov. Žilina: EDIS – vydavateľstvo ŽU, 2011. 281 s. ISBN 978-80-554-0457-8.
- [20] VARIANT PLUS, spol. s.r.o. Katalog produktů 2014/2015. Praha, 2014.
- [21] Lomax s.r.o. [online]. 2014 [cit. 2014-05-22]. Dostupné z: <http://www.lomax.cz/cs/predokenni-rolety/pod-preklad/>
- [22] Palmat s.r.o. [online]. 2014 [cit. 2014-05-22]. Dostupné z: <http://www.zarovky-svitidla.cz/0,111,interierove-osvetleni.html>
- [23] GILD Smart house system [online]. 2009 [cit. 2014-05-22]. Dostupné z: <http://www.gildsystem.cz/cz/rozvadecove-jednotky/>
- [24] VARIANT plus s.r.o. [online]. 2012 [cit. 2014-05-22]. Dostupné z: <http://www.integracebudov.cz/modularita-systemu-vni/>
- [25] VARIANT plus s.r.o. [online]. 2012 [cit. 2014-05-22]. Dostupné z: <http://www.integracebudov.cz/zkusenosti-s-navrhem-implementaci-a-provozem-systemu/>
- [26] VARIANT plus s.r.o. [online]. 2012 [cit. 2014-05-22]. Dostupné z: <http://www.integracebudov.cz/screenshoty-var-net-integral/>

- [27] Software firmy Milestone [online]. 2013 [cit. 2014-05-22]. Dostupné z:
<http://www.netcam.cz/produkty/software-sprava-videa/milestone.php>
- [28] Software firmy Milestone [online]. 2013 [cit. 2014-05-22]. Dostupné z:
<http://www.netcam.cz/produkty/software-sprava-videa/xprotect-lpr.php>
- [29] Software firmy Milestone [online]. 2013 [cit. 2014-05-22]. Dostupné z:
<http://www.netcam.cz/produkty/software-sprava-videa/xprotect-smart-wall.php>
- [30] Integoo integrated solutions [online]. 2012 [cit. 2014-05-22]. Dostupné z:
<http://www.integoo.cz/genetec-security-center>
- [31] Integoo integrated solutions [online]. 2012 [cit. 2014-05-22]. Dostupné z:
http://www.integoo.cz/sites/default/files/genetec_10216477.jpg
- [32] Integoo integrated solutions [online]. 2012 [cit. 2014-05-22]. Dostupné z:
<http://www.integoo.cz/sites/default/files/integra-integoo-technicky-popis-f.pdf>
- [33] Integoo integrated solutions [online]. 2012 [cit. 2014-05-22]. Dostupné z:
<http://www.integoo.cz/integra>
- [34] NetRex s.r.o. [online]. 2014 [cit. 2014-05-22]. Dostupné z:
<http://www.netrex.cz/cz/sluzby-a-produkty/platforma-netrex>
- [35] NetRex s.r.o. [online]. 2014 [cit. 2014-05-22]. Dostupné z:
<http://www.netrex.cz/cz/sluzby-a-produkty/people-counting/vyhody-pocitani-lidi/>
- [36] NetRex s.r.o. [online]. 2014 [cit. 2014-05-22]. Dostupné z:
<http://www.netrex.cz/cz/aktuality/pocitani-zakazniku/>
- [37] Scott and Weber [online]. 2010 [cit. 2014-05-22]. Dostupné z:
<http://www.scottweber.cz/sidlo-spolecnosti-praha10-virtualni-kancelar>
- [38] Lukáš, Luděk a kol., Bezpečnostní technologie, systémy a management III. 1. Vyd. Zlín: VeRBuM, 2013. 456 s. ISBN 978-80-87500-35-4
- [39] Google maps [online]. 2014 [cit. 2014-05-22]. Dostupné z:
<https://maps.google.cz/maps?hl=cs&tab=wl>
- [40] Axis Communications [online]. 2014 [cit. 2014-05-22]. Dostupné z:
http://www.axis.com/techsup/cam_servers/cam_200/index.htm?tab=datasheets

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PIR	Passive infra red (pasivní infračervený)
DPPC	Dohledové a poplachové přijímací centrum
CCTV	Uzavřený televizní okruh (closed circuit television)
PZTS	Poplachové zabezpečovací a tísňové systémy
EPS	Elektrická požární signalizace
ACS	Elektronická kontrola vstupu (Access control system)
GSM	Globální systém pro mobilní komunikaci (Global System for Mobile Communications)
GPRS	Služba pro přenos dat a připojení k internetu (General Packet Radio Service)
MZS	Mechanické zábranné systémy
PDA	Osobní digitální pomocník (Personal digital assistant)
I/O	Vstupní/výstupní rozhraní (In/Out)
IP	Adresovatelný, jednoznačně identifikovatelný v počítačových sítích
ATZ	Ochrana proti sabotáži
RAID	Vícenásobné diskové pole nezávislých disků (Redundant Array of Independent Disks)
HZS	Hasičský záchranný sbor
PČR	Policie České republiky
LAN	Místní síť (Local Area Network)
PTZ	Pan, Tilt, Zoom – směry pohybu a přiblížení
PGM	Programovatelný výstup
SMS	Krátká textová zpráva (Short message service)
CCF	Centrální ovládací zařízení
RZ	Registrační značka
CPU	Procesor (Central Processing Unit)
DRAM	Počítačová paměť

SEZNAM OBRÁZKŮ

Obrázek 1 Součásti Integrovaného poplachového systému.....	11
Obrázek 2 Skladba IP kamery [13].....	17
Obrázek 3 Schéma video prostředí [14]	18
Obrázek 4 Integrace IN/OUT pomocí PGM výstupů [20]	30
Obrázek 5 Integrace s ústřednou PZTS jako integračním prvkem [20]	31
Obrázek 6 Využití IP kamery jako integračního prvku [20]	33
Obrázek 7 Automatizační systém jako integrační prvek [20][21][22][23].....	34
Obrázek 8 Propojení aplikací pomocí systému VAR-NET Integral [25].....	38
Obrázek 9 Prostředí programu VAR-NET Integral – vyhlášení poplachu [26]	38
Obrázek 10 XProtect LPR – rozpoznávání RZ [28].....	40
Obrázek 11 XProtect Smart Wall [29].....	41
Obrázek 12 Prostředí programu Genetec Secirity Center [31]	43
Obrázek 13 Prostředí nástroje Integra 3 [33].....	44
Obrázek 14 Prostředí systému NetRex [36]	46
Obrázek 15 Fotografie objektu [37].....	47
Obrázek 16 Plán kancelářských prostor [37].....	47
Obrázek 17 Umístění zabezpečeného objektu [39]	50
Obrázek 18 Schematické znázornění integrovaného kamerového systému	54
Obrázek 19 Zakreslení použitých prvků v půdorysu	55
Obrázek 20 Zakreslení použitých prvků v půdorysu	56
Obrázek 21 Legenda pro nákres zabezpečení.....	57
Obrázek 22 Trasa od PČR (A) ke chráněnému objektu (B) [39].....	70
Obrázek 23 Trasa od HZS ČR (A) ke chráněnému objektu (B) [39]	71

SEZNAM TABULEK

Tabulka 1 Mechanické zábranné systémy a jejich.....	14
Tabulka 2 Stupně zabezpečení pro kamerové systémy [15] a pro PZTS [17].....	24
Tabulka 3 Hodnocení majetku.....	49
Tabulka 5 Nastavení zón.....	65
Tabulka 6 Události a reakce – PZTS, stav odstřeženo	66
Tabulka 7 Události a reakce – PZTS, stav zastřeženo	66
Tabulka 8 Uživatelská práva.....	67
Tabulka 9 Události a reakce – přístupový systém, stav odstřeženo.....	67
Tabulka 10 Události a reakce – EPS.....	68
Tabulka 11 Porovnání IP kamer [40].....	74

SEZNAM PŘÍLOH

PŘÍLOHA P I: