Moderní metody využití integrovaných bezpečnostních systémů v ochraně průmyslových objektů

Modern methods of use of integrated security systems to protect industrial buildings

Bc. Michaela Lažová

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

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

Jméno a příjmení:	**Bc. Michaela Lažová**
Osobní číslo:	**A11375**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Moderní metody využití integrovaných bezpečnostních systémů v ochraně průmyslových objektů**

Zásady pro vypracování:

1. **Seznamte odbornou veřejnost s moderními metodami současné ochrany průmyslových objektů.**
2. **Uveďte současné možnosti integrované průmyslové ochrany technickými prostředky.**
3. **Jaké jsou výhody a nevýhody.**
4. **Uveďte technické řešení integrace poplachového zabezpečovacího a tísňového systému, uzavřeného televizního a dohledového systému a systému kontroly vstupů.**
5. **Popište jaký bude budoucí vývoj ve vztahu k dohledovému a poplachovému přijímacímu centru.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. 81 s. ISBN 978-80-7318-889-4.**
2. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9.**
3. **LAUCKÝ, Vladimír. Speciální bezpečnostní technologie. 1. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 223 s. ISBN 978-80-7318-762-0.**
4. **IVANKA, Ján. Mechanické zábranné systémy. 1. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. 151 s. ISBN 978-80-7318-910-5.**
5. **Lukáš, Luděk a kolektiv. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín : VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.**
6. **Lukáš, Luděk a kolektiv. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín : VeRBuM, 2012. 387 s.ISBN 978-80-87500-19-4.**

Vedoucí diplomové práce: **JUDr. Vladimír Laucký**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této diplomové práce je seznámit odbornou veřejnost s moderními metodami současné ochrany průmyslových objektů. Problematika průmyslové ochrany je velmi široká. K ochraně průmyslových objektů se využívají integrované bezpečnostní systémy. Posláním průmyslové ochrany je zabezpečit objekt, aby se zabránilo vniknutí cizích nežádaných osob. Pro dosažení minimálních rizik je potřeba využít dostupných odpovídajících prostředků. Zabezpečení těchto objektů vychází vždy z konkrétních potřeb zadavatele, pojistného ústavu, technické specifikace objektu a možnosti použitý vhodných prostředků pro tento objektu. Vždy také záleží na podmínkách i místu instalace a dostupným finančním možnostem zadavatele.

V praktické části se zaměřuji na návrh technického řešení integrace v průmyslovém objektu.

Klíčová slova: ochrana objektů, průmyslový objekt, elektronický zabezpečovací systém, čidla, kontrola vstupů, průmyslová televize, kamery, požár, poplach, integrace.

ABSTRACT

The main aim of this master´s thesis is to inform general public with modern methods of simultaneous protection of industrial buildings. The issue of industrial protection is very substantial. For the protection of industiral buildings are used integrated security systems. The main aim of industrial protection is ensuring object to prevent from the entry of strangers. Appropriate means are necessary to achieving minimal risks. Security of these objects is adapting for wishes of contract owner, insurance company, technical specification of object and options for using appropriate means for this object. Always also depends on the conditions and the installation location and the available financial means of contract owner.

In the practical part I am concentrating on the proposal of technical solution of integration in industrial object.

Keywords: buildings protection, industrial buildings, electronic security systems, sensors, access control, closed-circuit television, cameras, fire alarms, integrations.

Poděkování

Tímto bych chtěla poděkovat svému vedoucímu diplomové práce JUDr. Vladimíru Lauckému za odborné vedení, rady a cenné připomínky, které mi poskytoval.

Motto

Žádný člověk není šťastný, pokud nemá nějaký cíl. A žádný člověk nemůže být šťastný bez víry ve svou schopnost tohoto cíle dosáhnout.

Lafayette Ronald Hubbard

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

Tato diplomová práce se zabývá moderními metodami využití integrovaných bezpečnostních systémů k ochraně průmyslových objektů.

Účinné zabezpečení průmyslových objektů a ochrana majetku jsou v dnešní době kvůli narůstající kriminalitě jednou ze základních potřeb každého průmyslového objektu. Nutnost ochrany je ovlivněna pocitem bezpečí a předcházením možnosti vzniku škod. Bezpečnostní systém průmyslových objektů je tvořen účelným uspořádáním a aplikací mechanických a technických prostředků, organizačních i režimových opatření a v neposlední řadě využití lidských zdrojů. Komplexní řešení celého bezpečnostního systému v průmyslových objektech je řešení zapojení prvků klasické, technické, režimové a fyzické ochrany.

Diplomová práce bude rozdělena do dvou hlavních částí, a to části teoretické a praktické. Teoretická část se zabývá teorii využití bezpečnostních systémů v praxi. Úvod je zaměřen na právní předpisy, normy a směrnice vztahující se k dané problematice, a na jednotlivé moderní metody současné ochrany průmyslových objektů. Poté jsou představeny možnosti integrované průmyslové ochrany technickými prostředky. Nezbytnou součástí je i porovnání výhod a nevýhod jednotlivých bezpečnostních systémů. Následuje budoucnost vývoje dohledových a poplachových přijímacích center (DPPC). Závěr teoretické části je zaměřen na technické řešení integrace poplachového zabezpečovacího a tísňového systému (PZTS), uzavřeného televizního a dohledového systému (CCTV) a systému kontroly vstupů (EKV).

Praktická část se bude věnovat návrhem zabezpečením konkrétního průmyslového objektu. V něm následně bude aplikována integrace poplachového zabezpečovacího a tísňového systému (PZTS), uzavřeného televizního a dohledového systému (CCTV) a systému kontroly vstupů (EKV) a elektrická požární signalizace (EPS).

Výstupem diplomové práce bude komplexní návrh zabezpečení konkrétního průmyslového objektu.

Cenný zdroj informací pro zpracování mé diplomové práce mi poskytne odborná literatura vztahující se ke zvolenému tématu a internetové zdroje.

I. TEORETICKÁ ČÁST

1 MODERNÍ METODY SOUČASNÉ OCHRANY PRŮMYSLOVÝCH OBJEKTŮ

Ochrana v obecném pojetí představuje vytvoření bezpečného prostředí pro daný subjekt. Realizace ochrany představuje návrh a sladění všech dostupných prostředků, které zajistí požadovanou nebo definovanou bezpečnost. [1]

Právní základy ochrany majetku a osob

Každá činnost v oblasti ochrany majetku a osob musí být právně ošetřena. Vzhledem k absenci Zákona o civilních bezpečnostních službách v našem právním řádu, jsme nuceni platný právní řád aplikovat na naše podmínky.

Jde zejména o tyto právní normy:

- *Zákoník práce č. 65/1965 Sb. ve znění změna doplňků,*
- *Zákon o trestním řízení soudním (trestní řád) č. 141/1961 Sb. ve znění změn a doplňků,*
- *Trestní zákon č. 40/2009 Sb. ve znění změna doplňků,*
- *Živnostenský zákon č.455/1991 Sb. ve znění změn a doplňků (§6a). [2]*

Specifické normy oboru zabezpečovací techniky

Základní legislativní rámce je tvořen „Zákonem č. 22/97 Sb.“ o technických požadavcích na výrobky a jednotlivé součásti systémů.

Zákon vychází z dokumentů Evropské unie (EU):

- *Směrnice 93/59 o všeobecné bezpečnosti výrobků,*
- *Rezoluce Rady EU č.90/C 10/01 o globálním přístupu k posuzování shody,*
- *Rozhodnutí Rady EU 93/465/EHS o modulech posuzování shody a označování shody značkou CE,*
- *Rezoluce Rady EU 85/C 136/01 o novém přístupu k technické harmonizaci a normám,*
- *Technické požadavky z hlediska elektromagnetické kompatibility (EMC) NV 169/1997.Technické požadavky z hlediska EMC se vztahují na elektrická nebo na elektronická zařízení včetně vybavení a instalací obsahující elektrické nebo elektronické součásti. [3]*

Směrnice EU/Nařízení vlády České republiky (ČR) vztahující se k oboru zabezpečovací techniky.

Tab. 1. Směrnice EU/Nařízení vlády ČR [3]

Směrnice EU	Název	Nařízení vlády ČR
LVD 73/23	Technické požadavky na elektrická zařízení nízkého napětí	NV 168
EMC 89/336	Technické požadavky na výrobky z hlediska EMC	NV 169
ATEX 94/09	Technické požadavky na zařízení a ochranné systémy určené pro prostředí z možností výbuchu	NV 176
CPD 89/106	Bezpečnost při požáru	-
TTE 91/263	Telekomunikační koncová zařízení	NV 426
EEC 92/58	Ochrana zdraví při práci	-

Stupně zabezpečení objektů

Stupně zabezpečení stanoví ČSN EN 50131-1 a oborové předpisy pojišťoven.

Tab. 2. Orientační rozdělení stupňů zabezpečení [13]

Stupeň zabezpečení	Riziko	Využití zabezpečení
Stupeň 1	Nízké riziko	garáže, chaty, byty, rodinné domy, strojovny
Stupeň 2	Nízké až střední riziko	komerční objekty
Stupeň 3	Střední až vysoké riziko	zbraně, ceniny, informace, narkotika
Stupeň 4	Vysoké riziko	zejména objekty národního a vyššího významu

Pyramida bezpečnosti

Představuje pomůcku při orientaci ve výrobcích pro koncové zákazníky i pro montážní firmy. Stupně zabezpečení jsou označeny číselně 1 – 4 s barevným rozlišením. Tyto úrovně jsou dány normou ČSN P ENV 1627.

Obr. 1. Pyramida bezpečnosti

Zdroj: [5]

Obr. 2. Označení výrobků

Zdroj: [5]

1.1 Klasická ochrana

Představuje vývojově nejstarší typ ochrany a spočívá v tom, že k zajištění příslušného objektu použijeme taková mechanická zařízení, která je umožní spolehlivě chránit. Jde zejména o vytváření různých zábran, znemožňujících zpravidla odcizení či zničení cenných předmětů, výrobků, zařízení apod., anebo vytváření takové přepážky, které by pachateli ztížili dosažení jeho cíle. [6]

Klasická ochrana je základem každého zabezpečovacího systémů v průmyslovém objektu. Setkáváme se s ní ve formě mechanického systému zabezpečení objektů (MZS).

MZS považujeme za základní prvek ochrany objektů a osob v průmyslu komerční bezpečnosti. Pod MZS řadíme veškeré mechanické prvky, které ztěžují násilné vniknutí nepovolané osoby do chráněné zóny nebo objektu především přes oplocení nebo cestou dveřních nebo okenních otvorů, případně manipulací nepovolané osoby s chráněnými předměty v zabezpečeném objektu. [4]

Obr. 3. Rotační turniket pro kontrolu přístupu osob do vnitřního prostředí

Zdroj: [14]

Odolnost mechanických překážek proti narušení a vniknutí, závisí na materiálových a mechanických vlastnostech. Použitý materiál musí vykazovat např. dostatečnou pevnost, tvrdost, houževnatost.

Na hlavních vstupech a vjezdech do prostor pro veřejnost nepřístupných, ale přístupných pro větší počet pracovníků mohou být použity náročnější zábrany. Velkokapacitní odbavovací systémy bývají zabezpečeny kombinací turniketu a elektronicky kontrolovaným vstupem (EKV). Pro vjezd vozidel se využívá automatické vjezdové závory ve spojení se systémem EKV. U průmyslových areálů je základem mechanického zabezpečení objektu, především oplocení areálu firmy a kvalitní zabezpečení budovy v podobě např. bezpečnostních zámků, mříží apod.

Rozdělení technických ochran MZS:

- *obvodová ochrana – jedná se o prostředky zajišťující bezpečnost vyhrazenému území a prostor kolem chráněného objektu. Obvodem objektu rozumíme jeho katastrální hranice omezené obvykle přírodními nebo umělými bariérami (vodní toky, ploty, zdi apod.),*
- *plášťová ochrana – zabraňuje jakémukoliv narušení standardních i nestandardních vstupních jednotek objektu. Jedná se o zabezpečení vstupu do všech vstupních otvorů v objektu: dveří, oken, balkónových oken, sklepních oken, vikýřů, zásobovacích a energetických šachet apod. Někdy se používá i názvů objektová či obvodová ochrana,*
- *předmětová ochrana – zabezpečuje prostory či úschovná místa, kde jsou uloženy peníze, cennosti, utajované skutečnosti, technická zařízení utajovaného charakteru apod., před zcizením nebo neoprávněnou manipulací. [4]*

1.2 Technická ochrana

Technická ochrana zajišťuje bezpečnostní prvky, jejichž použitím se zabraňuje, ztěžuje nebo oznamuje narušení ochrany objektu. [3]

Součástí technické ochrany je tzv. klasická ochrana. Jde o využívání mechanických zařízení, prostředků a komponentů, které svou konstrukcí znemožňují jednoduché překonání a průnik nežádoucích osob do střeženého prostoru. Dalším způsobem technického zabezpečení objektu je využívání zařízení poplachových zabezpečovacích a tísňových systémů (PZTS), doplněné monitorovacími a záznamovými prostředky realizovanými technikou uzavřených televizních a dohledových systémů (CCTV). Součástí technické ochrany jsou prostředky elektrické požární signalizace (EPS) a systémy na řízení a kontrolu vstupu do objektu (EKV).

Technickou ochranu k zabezpečení průmyslových objektů považujeme za nejspolehlivější a nejhůře překonatelnou pro nežádoucí pachatele. Je to díky rychlé reakci zabezpečovacího systému a následnému předání signálu o změně vyvolané pachatelem nebo projevem, který je vyhodnocen jako nebezpečný. Technická ochrana podporuje klasickou ochranu tím, že předává informace o jejím napadení. Velkou výhodou je snížení počtu zaměstnanců klasické ochrany a tím i snížení nákladů k zabezpečení průmyslových objektů.

1.3 Režimová ochrana

Je souborem organizačně administrativních opatření a postupů směřujících k zajištění požadovaných podmínek pro funkci zabezpečení systému a jeho sladěním s provozem chráněného objektu. Ve své podstatě režimová ochrana jednak zajišťuje možnost řádné funkce ostatních druhů ochrany a rovněž snižuje zranitelnost chráněných zájmů množstvím dalších forem kriminální trestné činnosti, jako je vandalismus, výtržnosti, loupeže, přepadení, drobné krádeže a rozkrádání, pumové útoky, žhářství a sabotáže, průmyslová špionáž, případně i předstírání škod zaměstnanci i hosty. [6]

Opatření dělíme na vnější a vnitřní. Vnější opatření udává podmínky pro vstup a vjezd do chráněných objektů. Vnitřní opatření vyhrazuje pohyb osob a vozidel v objektech. K zajištění režimových opatření se v praxi využívá elektronické zabezpečení dveří či turnikety bran. K jejich odblokování je potřeba identifikace držitele karty s přiděleným oprávněným vstupu či vjezdu do chráněného průmyslového objektu.

Obr. 4. Přístupový systém

Zdroj: [14]

1.4 Fyzická ochrana

Umožňuje v případě nutnosti provést zásah (zákrok) k odvrácení nebezpečí (či snížení následků a škod). Aktivně se podílí na zmaření záměrů narušitele a umožňuje bezprostřední opatření k jeho dopadení. Fyzická ostraha objektu se zabezpečuje vyškolenými zaměstnanci. [3]

Fyzická ochrana chrání před neoprávněným vstupem do střeženého prostoru, únikem informací, vandalismem, krádeží, sabotáží, ohněm, havárií, ale i před následky přírodních katastrof. Rozlišujeme několik forem fyzické ostrahy (strážní službu, kontrolně propustkovou činnost, bezpečnostní dohled, ochranný doprovod, bezpečnostní výjezd či strážné se psy). Cílem ostrahy průmyslových objektů je minimalizace rizika vzniku škody na majetku a také ochrana životů a zdraví osob, které se ve střežených průmyslových objektech vyskytují. Vykonávaná je vyškolenými zaměstnanci provozovatele průmyslových objektů, zaměstnanci soukromých bezpečnostních služeb či příslušníky ozbrojených sil. Prostředkem k zajištění komplexní ochrany průmyslových objektů je kombinace fyzické ostrahy a technické ochrany zajišťované pomocí prvků MZS.

Obr. 5. Fyzická ostraha objektů

Zdroj: [15]

2 MOŽNOSTI INTEGROVANÉ PRŮMYSLOVÉ OCHRANY TECHNICKÝMI PROSTŘEDKY

Problematika zabezpečení a ostrahy komerčních a průmyslových objektů je oblastí poměrně širokou. Komerční objekty můžeme rozdělit podle jejich zaměření nebo z pohledu různých specifik (odlišnost objektů, velikosti či fungování). Jedná se o průmyslové objekty a areály, administrativní a kancelářské budovy, obchodní centra, sklady či logistická centra. Jsou to objekty s relativně volným pohybem nejrůznějších osob a může se zde vyskytovat široká škála nejrůznějších prostředí.

Obr. 6. Dotyková klávesnice s LCD

Zdroj: [16]

2.1 Poplachové zabezpečovací a tísňové systémy (PZTS)

Je soubor zařízení složený z několika částí, tvořících komplexní zabezpečovací řetězec (čidla, ústředny, přenosové prostředky, signalizační a ovládací panely). Propojení čidel s ústřednou může být realizováno tzv. drátově pomocí elektrických kabelů nebo bezdrátově pomocí rádiových vln. PZTS monitoruje vstup neoprávněných osob do prostorů, které jsou touto signalizací střeženy, a následně při vyhlášení poplachu dávají podnět k přivolání policie nebo bezpečnostní služby. Instalaci PZTS předchází zpracování bezpečnostního posouzení objektu, které stanoví kritická místa a vyhodnotí veškerá rizika, definuje úroveň a stupeň zabezpečení a navrhne technické řešení, včetně návrhu režimového opatření. Následně je zpracován projekt, následuje instalace zařízení, proškolení obsluh a uvedení

do trvalého provozu. Součástí nabízených služeb společnosti je také provádění servisu, pravidelných revizí a kontrol těchto zařízení. Úroveň zabezpečení rozlišujeme do čtyř kategorií a to na rizika velmi vysoká, vysoká, průměrná a nízká. Schvalování komponentů PZTS, navrhování, instalace a revize systémů EZS se řídí skupinou harmonizovaných norem ČSN EN 50131. [17]

Výrobci

Siemens, GE Interlogix -Aritech, Bosch, Novar, Jablotron, Telenot, Bentel, Sicurit, Galaxy, ATS, Sintony, Paradox Digiplex, Concept, Visonic, Esprit, CD Advisor, Omnia [17]

Legislativní požadavky

Tab. 3. Skupina norem PZTS [3]

Číslo normy	Zjednodušený název
EN 50131-1 (ed. 2)	Všeobecné požadavky
EN 50131-2-1	Společné požadavky na detektory
EN 50131-2-2	Detektory pasivní
	Detektory MW
EN 50131-2-4	Detektory kombinovaná PIR/MW
EN 50131-2-5	Detektory kombinovaná UZ/PIR
EN 50131-2-6	Detektory otevření
EN 50131-3	Ústředny
EN 50131-4	Výstražná zařízení
EN 50131-5-1	Společné požadavky pro propojovací zařízení
EN 50131-5-3	Propojovací zařízení využívající vyhrazené drátové spoje
EN 50131-5-4	Propojovací zařízení využívající vf techniku
EN 50131-5-5	Propojovací zařízení využívající IČ techniku
EN 50131-6	Napájecí zdroje
EN 50131-7	Pokyny pro aplikace

PZTS

Slouží k signalizaci nebezpečí ve střeženém objektu. Zejména informují o nežádoucím vniknutí (vloupání) do objektu. Mohou však být kombinovány s indikací jiných nebezpečí (např. tísňové hlášení při přepadení či zdravotních obtížích, požární nebezpečí, únik plynu, zaplavení apod.). [7]

Srdcem a řídící jednotkou každého systému PZTS je ústředna. Velikost ústředny a výkon volíme s ohledem na velikost střeženého objektu. Ústředny PZTS mohou obsluhovat různé množství smyček. Na smyčkách jsou připojena koncová zařízení. Podle očíslování a popisu smyček můžeme v případě vyhlášení alarmu stanovit, kde došlo k narušení a vyhlášení poplachu.

Základní rozdělení ústředen:

- ústředny smyčkové,
- ústředny s přímou adresací senzorů,
- ústředny smíšeného typu,
- ústředny s bezdrátovým přenosem poplachového signálu od senzorů.

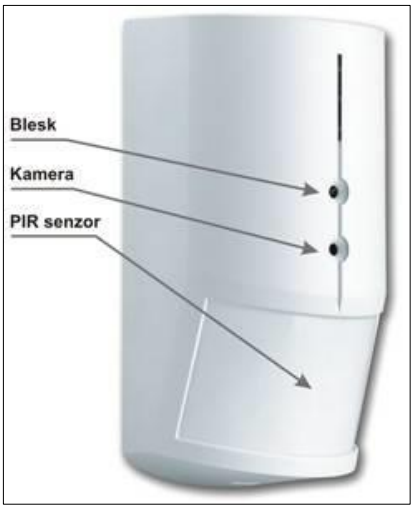
Složení PZTS:

- detektor – bezprostředně reaguje na fyzikální změny související s narušením střeženého objektu nebo prostoru či na nežádoucí manipulaci se střeženým předmětem. Při narušení detektor vysílá poplachové zprávy či signál,
- ústředna – přijímá a zpracovává informace. Umožňuje ovládání a indikaci zabezpečovacího systému, dále zajišťuje napájení a inicializaci přenosu informací,
- přenosové prostředky – jedná se o přenos vstupních informací z ústředny do místa signalizace či povelů opačným směrem,
- signalizační zařízení – převádí informace na vhodný signál (vyhlašuje poplach či výstrahu),
- doplňková zařízení – usnadňují ovládání signálu či umožňují realizaci některé speciální funkce.

Zabezpečení vnitřních prostor

V průmyslových objektech se využívá klasická PZTS s využitím standardních detektorů do vnitřního prostředí. Detektory pro vnitřní použití jsou určeny pro instalaci uvnitř zabezpečené budovy a do míst bez vlivu povětrnostních podmínek. Je to dáno jejich krycí

schopností a odolností proti falešným poplachům Před vypracováním návrhu zabezpečení je potřeba si s budoucím uživatelem upřesnit, které z následujících prvků budou vytvořeny (prvky prostorové detekce uvnitř objektu, vytvoření plášťové ochrany pomocí magnetů a detektorů tříštění skla, ochrana proti požáru).



Obr. 7. Duální detektor pro vnitřní detekci

Zdroj: [16]

Zabezpečení vnějších prostor

U velkých průmyslových objektů může nastat potřeba zabezpečit i vnější prostory. K tomuto zabezpečení se využívají odlišné detektory. Jedná se o detektory pro vnější prostředí nebo perimetrickou ochranu. Pro střežení menších vnějších prostor jsou využívány prostorové detektory pohybu. Pro větší plochy je nutné navrhnout řešení pro dané prostředí a omezit jeho hranice. Využívají se jednotlivé infračervené (IR) závory nebo IR bariéry tvořené soustavou IR závor. U oplocených ploch lze navrhnout detekci překonání plotu. U rozsáhlých systémů s významným podílem zemních prací se využívají zemní detekční kabelové systémy s aktivním vyzařováním. Pro zabezpečení prostor s nebezpečím výbuchu se využívá speciální technika.

Vyhodnocování

Jednotlivé prvky jsou připojeny na ústřednu PZTS přímo nebo přes koncentrátory sběrnicového systému. Ústředna PZTS zpracovává informace od detektorů a systémových prvků. S DPPC komunikuje díky přenosovým systémům. V komerčních a průmyslových objektech jsou využívány sběrnicové ústředny s velkým počtem možných podskupin

a pružnou výstavbou. Jednotlivé koncentrátory komunikují s vlastní ústřednou po datovém vedení. Redukují kabelové trasy v objektu. V ústředně PZTS je vestavěn zálohovaný zdroj pro koncentrátory a čidla. DPPC je posledním článkem PZTS. Zajišťují přenos poplachových událostí ze střeženého objektu do DPPC. Na základě přenesených informací je prováděn fyzický zásah v zabezpečeném objektu. Při poplachu vyhlášeném PZTS je okamžitě upozorněno nejbližší výjezdové vozidlo DPPC, které navede výjezdovou skupinu na místo. Operátoři mohou zavolat na předem dohodnutá telefonní čísla a informovat o situaci majitele objektu nebo pověřenou osobu.

Inovace PZTS

PZTS zaznamenávají rozvoj z mnoha hledisek:

- *komunikátory – zaručení kvalitního přenosu informace z PZTS je jednou z nejdůležitějších funkcí celého systému. Celá přenosová trasa od komunikátoru na straně PZTS až po komunikátor na straně DPPC. Dostupné možnosti spojení:*
  - *PSTN - zprávy z objektu jsou přenášeny pevnou telefonní sítí,*
  - *GSM/GPRC – přenos dat z objektivu na DPPC je uskutečněn pomocí GSM sítě,*
  - *rádiové spojení – rádiové spojení na DPPC využívá privátní rádiovou síť, v současnosti jde o nejbezpečnější způsob připojení,*
  - *TCP/IP – zprávy se z PZTS přenášejí prostřednictvím LAN modulu. Jedná se o moderní zařízení pro přenos dat z DPPC v reálném čase přes internet,*
- *ovládací periferie - strohé a nevzhledné klávesnice nahrazují designové klávesnice s LCD displejem, který umožní koncovému uživateli plnohodnotný přístup do systému, včetně nastavování základních i nadstandardních funkcí. V současné době jsou trendem biometrické čtečky otisků prstů. Uživatelský software má nainstalovaný ve svém počítači koncový uživatel, a tento software využívá hlavně k přehledové kontrole stavu střeženého objektu,*
- *inteligentní elektroinstalace – hlavní rozdíl mezi klasickou a inteligentní elektroinstalací je v rozdělení funkce domovního spínače. V klasické instalaci vypínač přímo spíná elektrický obvod a přes spínač se přivádí elektrická energie do spotřebiče. Inteligentní elektroinstalace rozděluje funkci domovního spínače do dvou funkčních bloků, senzoru, aktoru. Senzor při stisku vysílá zprávu, že se má „předurčené zařízení“ zapnout nebo vypnout. Aktor je výkonový spínač, který*

přijímá zprávu od libovolných senzorů a při požadavku připojí spotřebič ke zdroji energie.

- *aktivní ochrana – jedná se o účinnou ochranu při přepadení bank, čerpacích stanic, obslužného personálu v obchodech, apod. Pro spuštění je potřeba dvou nezávislých signálů na vstupech např. uvedení PZTS do střežení a následného vyhlášení poplachu. V případě aktivace je systém navržen tak, aby okamžitě vyplnil chráněnou oblast mlhou. Zařízení je odolné proti sabotáži a tudíž nemá ventilační otvory a veškeré odnímatelné části jsou střeženy tamper kontaktem, obsahuje záložní akumulátor a senzor pro detekci hustoty a kouře. [8]*

Obr. 8. Perimetrická ochrana objektu

Zdroj: [16]

2.2 Uzavřené televizní a dohledové systémy (CCTV)

Kamerové systémy CCTV jsou velmi významným prostředkem pro monitorování a to nejen pro bezpečnostní účely (pro ověření poplachového stavu, ale také pro sledování různých výrobních procesů v průmyslu). Černobílé nebo barevné CCTV systémy tvoří: kamery, monitory, videopřepínače, multiplexery, videomatice, záznamová zařízení analogová i digitální, detektory pohybu, přenosové cesty (metalické, optické), popřípadě audio komponenty. Nezbytným příslušenstvím jsou kamerové povětrnostní kryty, držáky, otočné hlavice ke kamerám, přisvětlení ve viditelném i infračerveném spektru světla. Současné systémy umožňují téměř neomezené možnosti ovládání (polohy, ostření, transfokace) a přenosu obrazu i zvuku na dálku, a to i na velké vzdálenosti s využitím buďto koaxiálních

nebo optických kabelů a nejnověji s využitím datových sítí s protokolem TCP/IP. Možné jsou i přenosy realizované pomocí mikrovlnných nebo laserových pojítek. CCTV jsou pojaty v EN jako doplňková zařízení poplachových systémů a nejsou na ně stanovena kritéria na stupně zabezpečení jako na EZS. Schvalování komponentů CCTV, navrhování a instalace systémů CCTV se řídí skupinou harmonizovaných norem ČSN EN 50132. [17]

Výrobci

GE Interlogix, Sicurit, Siemens, Bosch, Sanyo, Sony, Panasonic, Geutebruck, DedicatedMicros , Pelco, Dallmeier, Watec, Intelex [17]

Legislativní požadavky

Tab. 4. Skupina norem CCTV [3]

Číslo normy	Zjednodušený název
EN 50132-1	Systémové požadavky
EN 50132-2-1	Černobílé kamery
EN 50132-2-2	Barevné kamery
EN 50132-2-3	Objektivy
EN 50132-2-4	Příslušenství
EN 50132-3	Místní a hlavní řídící jednotka
EN 50132-4-1	Černobílé monitory
EN 50132-4-2	Barevné monitory
EN 50132-4-3	Záznamová zařízení
EN 50132-4-4	Zařízení pro okamžitý výtisk obrazu
EN 50132-4-5	Videodetektor pohybu
EN 50132-5	Přenos signálu
EN 50132-6	(volná)
EN 50132-7	Pokyny pro aplikace

CCTV

Kamerové bezpečnostní systémy, kamerové dohledové systémy, resp. systémy průmyslové televize v současnosti zaznamenávají největší rozvoj ze skupiny poplachových systémů. CCTV byl původně určený na identifikaci, rekonstrukci a detekci osob. Současné inteligentní kamerové systémy umožňují mnohem širší možnosti využití v průmyslu komerční bezpečnosti. Mohou být využité například na detekci podezřeného chování osob (nesprávný směr pohybu, rychlá chůze, výtržnictví, opuštění zavazadla.), biometrickou identifikaci osob, sledování osob, sledování osob na letišti, rozpoznání předmětů, identifikaci evidenčních čísel vozidel, sledování a vyhodnocování dopravních nehod na cestách, atd. [8]

Technické parametry kamer:

- rozlišovací schopnost,
- poměr stran obrazu,
- citlivost,
- dynamický rozsah,
- napájení kamer,
- řídící vstupy kamer.

Základní prvky kamery

Kameru tvoří tři základní stavební části: objektiv, fotocitlivý prvek a elektronická část. Objektiv spolu s ovládacími prvky pro zoom a clonu tvoří první část kamery a slouží k vytvoření obrazu scény. Za objektivem je umístěn snímací senzor (fotocitlivý prvek) pro záznam obrazu, senzor převádí obraz do elektronické podoby. Elektronická část spolu s mikroprocesorem zajišťuje digitalizaci získaných informací ze snímače, jejich kompresi a ukládání na využívané médium, případně přenos kanálem na vzdálené zobrazovací nebo záznamové zařízení.

- *objektiv – hlavním úkolem objektivu je promítnout zmenšený obraz snímané scény na plochu fotocitlivého prvku, vytvořený obraz musí být bez rušivých a negativních elementů. Objektiv je zpravidla složen z několika čoček a dalších stavebních částí, které jsou sestaveny v optické ose, jsou tedy opticky centrované. Jednotlivé části objektivu se během ostření či zoomování (změně ohniskové vzdálenosti) pohybují,*
- *technologie optických senzorů – fotocitlivý prvek spolu s optikou představují nejdůležitější součásti kamery a předurčují kvalitu snímaného obrazu. Objektiv*

zmenší obraz sledované scény a zobrazí ho na fotocitlivý prvek. Je několik druhů fotocitlivých prvků určených ke snímání obrazu, lišících se například technologií výroby, principem snímání nebo snímacími vlastnostmi - CCD senzor, super CCD senzor, senzory CMOS, DPS senzory. [9]

Obr. 9. Venkovní barevná
analogová kamera
Zdroj: [18]

Základní rozdělení CCTV

Kamery a jejich podpůrná infrastruktura se staly běžnou součástí našich životů. V minulosti převažovaly hlavně analogové CCTV systémy, dnes pomalu začínají dominovat vyspělejší IP sledovací systémy.

- konvenční – analogové bezpečnostní kamery zachytí analogový videosignál a přenesou jej prostřednictvím koaxiálního kabelu do digitálního videorekordéru (DVR). Každá z kamer vyžaduje vlastní napájecí kabel a z každé kamery musí jít separátní koaxiální kabeláž k DVR. U DVR proběhne konverze analogového signálu na digitální. Digitální signál je zkomprimován a uschován v úložišti nebo na záznamovém médiu. DVR nabízí základní funkce, jako je plánování, digitální zoom obrazu či detekce pohybu. Obrazovky ke sledování záznamů jsou připojeny k DVR,
- digitální – IP kamery vytváří digitalizovaný videosignál, který je přenášen po drátových nebo bezdrátových sítích. Umožňuje vzdálené monitorování a nahrávání v celé oblasti pokrytí bezdrátových sítí. IP kamerový systém se skládá s kamer, hardwaru, sledovacího softwaru a přenosové sítě. IP sledovací systém zahrnuje

inteligentnější IP, které zachytí obraz v mnohem vyšším rozlišení a zároveň je konvertují na digitální. Podle typu kamery mohou v rámci zlepšení kvality dále zpracovávat nebo je zkomprimují pro snížení náročnosti na přenosové pásmo. IP kamery disponují i dalšími funkcemi (např. detekcí pohybu), která přímo závislá na typu použitého softwaru. Digitální signál je dále posílán prostřednictvím ethernetového kabelu. Z toho vyplývají dvě další výhody. Kamery lze rovnou napájet pomocí PoE (Power-over-Ethernet) adaptérů a traffic je obousměrný (kamerám lze z monitorovacího stanoviště například vysílat nové instrukce). Data pak putují přímo do síťového videorekordéru NVR **(**Network video recorder**)**, což je díky nainstalovanému softwaru VMS (Video Management Software) jakýsi mozek celé operace,

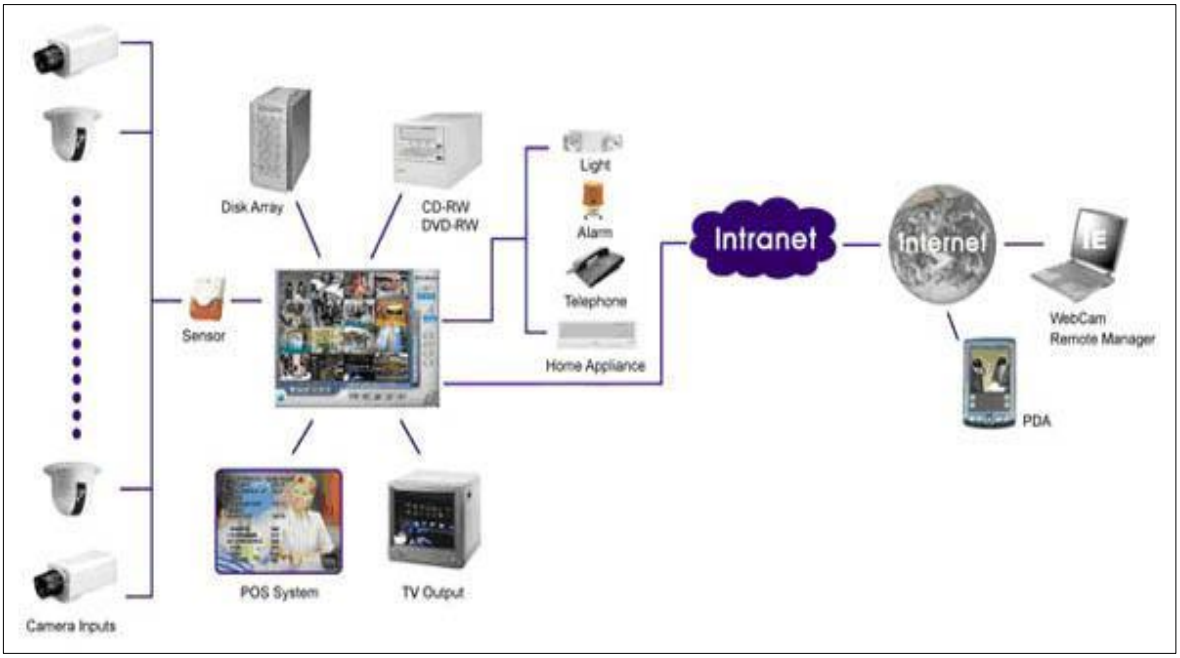
- hybridní – kombinace obou předchozích variant, kde je možné sledovat obraz i vzdáleně pomocí počítače.

Obr. 10. Vnitřní DOME analogová kamera

Zdroj: [18]

Návrh systému

Návrhu CCTV je potřeba věnovat dostatečnou pozornost, aby výsledek splňoval požadavky budoucího uživatele. Nejdříve je nutné definovat cíle, které chceme instalací systému dosáhnout. V závislosti na nich stanovíme potřebný návrh topologie jednotlivých kamer a jejich technické parametry. Využíváme dostupné druhy kamer, objektivy, kryty, držáky a zkušenosti z předchozích instalací CCTV.



Obr. 11. CCTV poskytují přehled o dění ve sledovaných prostorech

Zdroj: [19]

Dálkový dohled

Jedná se o velmi oblíbenou a stále častěji využívanou funkci CCTV. Díky ní se můžeme podívat z kteréhokoliv místa na světě na svůj CCTV. Nejčastěji se využívá k dálkovému dohledu zapotřebí klientského software. Některá sofistikovanější zařízení umožňují dálkový dohled přes webový prohlížeč. Je možnost v době nepřítomnosti a v reálném čase sledovat, co se děje na firmě, v kanceláři. V kterémkoli okamžiku je možné si zkontrolovat pohyb zaměstnanců a jejich činnost, zda dodržují technologické a výrobní postupy, výkon činnosti strážní služby nebo pohledem na váhu zkontrolovat správné namarkování ceny v obchodě. Na základě přístupových práv lze studovat záznam z jednotlivých kamer a celý systém CCTV vzdáleně ovládat, nastavovat. Majitelé více provozoven ocení možnost kontroly všech svých podniků z jednoho místa.

Budoucnost CCTV

Mezi nejnovější funkce kamerových systémů můžeme v současnosti zařadit například automatické sledování osob a předmětů, resp. inteligentní analýzu obrazu. V budoucnosti můžeme očekávat nové funkce související s identifikací osob na základě analýzy zaznamenání lidské tváře. [8]

2.3 Systém kontroly vstupů (EKV)

Systémy kontroly vstupu řídí přístup osob, resp. vozidel do chráněných prostorů nebo ke chráněným zařízením, případně informacím, na základě přidělených přístupových práv. Tato zařízení umožňují sledovat pohyb osob v definovaných prostorových zónách. Systémy EKV využívají koncové akční prvky, např. elektrické zámky, turnikety, brány, propusti a další. Jako nositel přístupového oprávnění jsou využívána různá média, např. magnetické a čipové karty, čipové přívěšky různých tvarů a nejnověji se využívá biometrických informací, např. otisky prstů, zobrazení oční duhovky nebo sítnice nebo obraz obličeje. Základní požadavky jsou nebo budou uvedeny ve skupině harmonizovaných norem ČSN EN 50133.[17]

Výrobci

Novar, Gold card, Interlogix, Northern, Honeywell, ABLOY [17]

Legislativní požadavky

Tab. 5. Skupina norem EKV [21]

Číslo normy	Zjednodušený název
EN 50 133-1	Systémové požadavky
EN 50 133-2-1	Všeobecné požadavky na komponenty
EN 50 133-3	Vyhodnocovací zařízení
EN 50 133-4	Výstupní ovládací prvek přístupového místa
EN 50 133-5	Komunikace
EN 50 133-6	(volná)
EN 50 133-7	Pokyny pro aplikace

EKV

Můžeme chápat jako soubor opatření k zajištění řízení a evidence přístupu do zabezpečeného objektu nebo prostor na základě jednoznačně přidělených práv tato opatření mohou být systémová, fyzická (ostraha), mechanická (zámky, mříže, závory) nebo elektronická, nejúčinnější je jejich kombinace. Přístupová práva jsou každému uživateli

přidělena na základě personální politiky, stupně oprávnění, časového harmonogramu, apod. Na základě jednoznačné identifikace uživatele je po ověření přístupových práv povolen nebo zamítnut přístup. Sofistikovanější systémy umožňují např. sledovat pohyb a přítomnost v jednotlivých úsecích, definovat návaznost průchodů nebo „za běhu" měnit přístupová práva. [8]

Obr. 12. Čtečka otisku prstů

Zdroj: [20]

Kontrola vstupů do místnosti

V jakékoliv firmě či instituci jsou prostory, kde má povolen vstup určitý okruh osob. Systém nabízí možnost získat přehled o vstupu, délky trvání, přesného data a času. Informuje o pokusu vstupu neoprávněných osob či neobvyklých událostech v objektu. Většina systémů se skládá z několika dílčích komponentů. Pro EKV jsou to snímače identifikačních karet, které jsou adresovatelné řídící jednotce. Systém může odemykat a zamykat křídlové dveře, posuvné lineární dveře, roletové dveře, turnikety, branky. V databázi je pro zpětnou kontrolu zaznamenán veškerý pohyb osob v budově a všechny ostatní stavy (poplachy, výpadky napájení, sabotáže). Jednotlivé systémy flexibilní, v praxi umožňuje napojení na další bezpečnostní systémy sloužící k ochraně objektu (PZTS, EPS, CCTV).

Tab. 6. Třídy identifikace [8]

Třída identifikace	Identifikace na základě	Příklad identifikačního média/kombinační bezpečnost
0	Není přímá identifikace	Tlačítko, kontakt, detektor pohybu (prostý požadavek na průchod)
		Pro vstup se předpokládá namátková kontrola nějakého dokladu nebo pověření fyzickou osobou (osoba, vrátný).
1	Dat uložených v paměti	Heslo, číslo zaměstnance
		Poměr počtu uživatelů k počtu všech kombinací kódů musí být alespoň 1:1000. Minimální počet kombinací 10000.
2	Identifikačních prvků nebo biometrie	Identifikační karta/přívěšek (token), čip, otisk prstu, oční duhovka, 3D model obličeje
		Min. 1 mil. kombinací, jednoznačná identita uživatele, chybovost max. 0,01 %. Identifikační číslo prvku nesmí být přímo zobrazeno.
3	Kombinace třídy 1 a 2	Jednoznačný token/otisk prstu + heslo
		Alespoň kombinace tříd 1 a 2

Tab. 7. Třídy přístupu [8]

Třída přístupu	Kritérium dělení
A	Pro přístupové místo není vyžadován časový filtr ani ukládání přístupových transakcí
B	Přístupové místo má funkci časových filtrů (minimální požadavek na třídu B1) a ukládání dat

Kontrola vjezdů

Kontrola vjezdů a výjezdů vozidel do soukromých parkovišť nebo přes podnikové vrátnice. Je to na místech, kde je nutné zabezpečit průjezd oprávněným vozidlům. Realizováno je to pomocí snímačů identifikačních karet, řídících jednotek, vyhodnocovacího software a vjezdového systému. Vjezdový systém může být ve formě elektrických závor, posuvné brány, křídlové brány, řetězové zábrany. Díky kombinaci s ostatními systémy je zajištěna maximální kontrola a ochrana objektu.

Evidence návštěv

Jedná se o návštěvy, které jdou do objektu za konkrétním účelem. Mohou to být zaměstnanci externích firem nebo servisní pracovníci. Při příchodu do objektu jsou vybaveni kartou, která jim umožní vstup do příslušných prostor, výtahu či parkoviště, ale zaznamená přesný čas samotného příchodu, odchodu. Při opakovaných návštěvách jsou návštěvníci evidováni v SW databázi, která urychlí opětovné vydávání karet. K zjednodušení systému při správě návštěvních karet jsou určeny speciální „pohlcovací" snímače, do kterých návštěvník při odchodu vhodí identifikační kartu.

Evidence docházky

Docházkové systémy slouží ke sběru informací o čase a důvodu průchodu místem kontroly a jejich dalšímu zpracování s vazbou na zpracování docházky a mzdovou agendu. K identifikaci pracovníka se používají tatáž média jako u systémů EKV. [17]

Výrobci

Eff-Eff, Goldcard, Honeywell, ANeT [17]

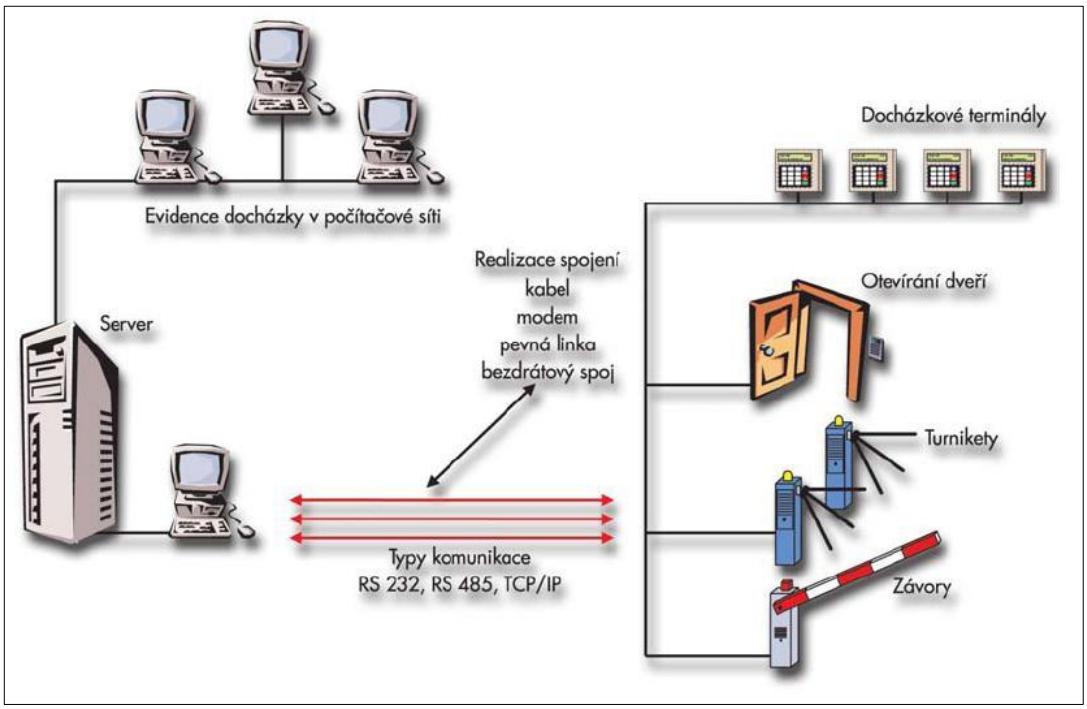
Evidence docházky pracovníků je zaznamenávána pomocí inteligentních terminálů a bezkontaktních identifikačních karet. Na terminálech lze provádět registraci začátku, konce nebo několika typů přerušení pracovní doby. Docházkový software zpracuje veškeré informace o pracovní době jednotlivých pracovníků a data převede do mzdové agendy.

Objednávání a výdej stravy

Využití identifikačních karet a snímačů karet lze využít k automatizaci objednávek a kontrole výdeje stravy. Komunikace strávníka se systémem je zprostředkován bezkontaktní kartou, která jej identifikuje při objednávkách přes příslušný snímač i při výdeji. Systém řeší restaurační, objednávkový i kombinovaný způsob stravování. V jedné jídelně se mohou stravovat zaměstnanci i externí osoby či firmy. Systém vyúčtování strávníků eviduje platby jednotlivých uživatelů, a to včetně příspěvků od zaměstnavatele.

Softwarová integrace

Softwarová integrace je vhodná tam, kde není možné bez počítačové nadstavby dosáhnout přehledného monitorování a řízení objektu. Z důvodu zjednodušení, zpřehlednění a zároveň snížení nákladů za jednotlivé systémové softwary, je možné použít tzv. „integrační softwary". Ty vzájemně integrují EKV, docházky, EPS, PZTS, CCTV a systémy měření a regulace. Nabízejí funkce vizualizace, centrálního managementu, analýzy událostí, automatizaci bezpečnostních procesů, správu identit, řešení krizových situací. [8]



Obr. 13. Elektronická kontrola vstupu

Zdroj: [22]

2.4 Elektrická požární signalizace (EPS)

Systémy EPS tvoří důležitou součást systémů protipožární ochrany objektů a budov. EPS zajišťuje včasnou a rychlou identifikaci a lokalizaci vzniku ohniska požáru. Nasazením systému EPS je tak možné zabránit vzniku velkých materiálových ztrát a v horších případech i ztrátě lidských životů. EPS lze začlenit do integrovaných bezpečnostních a havarijních systémů ochrany majetku, osob. Systém EPS tvoří vyhodnocovací ústředna, různé typy hlásičů a koncová a popřípadě ovládaní zařízení. EPS informuje uživatele

o vzniku požáru akustickou a optickou signalizací přímo v objektu nebo pomocí zařízení dálkového přenosu signalizace na stanoviště pultu centrální ochrany (DPPC), který je umístěn u hasičského záchranného sboru (HZS). Hlásiče EPS pracují na různých fyzikálních principech. Vyhodnocují optické, ionizační nebo teplotní parametry prostředí, ve kterém jsou umístěny. Všechny detektory jsou dnes již vybaveny složitou elektronikou řízenou procesorem, umožňující eliminovat plané poplachy. Systémy EPS mohou být instalovány jako samostatné aplikace nebo jako součásti vyšších integrovaných systémů řízení budov. Využití grafického nadstavbového vybavení potom umožňuje velmi rychlou orientaci v objektech a budovách a tím maximální zkrácení doby požárního zásahu od vzniku požáru. Programovatelnými výstupy ústředny je možné ovládat další zařízení související s protipožární ochranou (protipožární dveře, hasící zařízení, klíčové trezory, apod.). Legislativní rámec zřizování EPS tvoří zákon č.67/2001Sb.o požární ochraně a z řady vyhlášek především č. 246/2001Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru a stavební zákon. Normativním základem pro obor EPS jsou normy řady EN 54.[17]

Výrobci

GE Interlogix-Aritech, Siemens-Alarmcom, Esser, Lites, Eff-Eff, Bosch, Zettler, LaborStrauss [17]

Obr. 14. Elektronická požární signalizace

Zdroj: [23]

Legislativní požadavky

Tab. 8. Skupina norem EPS [3]

Číslo normy	Zjednodušený název
EN 54-1	Úvod
EN 54-2	Ústředna EPS
EN 54-3	Sirény
EN 54-4	Napájecí zdroj
EN 54-5	Hlásiče teplot
EN 54-7	Hlásiče kouře
EN 54-10	Hlásiče plamene
EN 54-11	Hlásiče tlačítkové
EN 54-12	Hlásiče lineární
EN 54-13	Systémové požadavky
EN 54-14	Aplikační návody
EN 54-15	Hlásiče multisenzorové
EN 54-18	Vstupní/výstupní zařízení
EN 54-19	Lineární tepelné hlásiče
EN 54-20	Nasávací hlásiče
EN 54-21	Přenosová zařízení

EPS

Rozvoj průmyslových zón v ČR přinesl s sebou celou řadu změn, které se odrážejí ve změnách užívání krajiny, ekonomických změnách i infrastruktuře. Společně s uvedenými změnami je nutné v těchto oblastech řešit zajištění požární bezpečnosti. Průmyslové zóny jsou tvořeny rozsáhlými stavebními objekty, kde nelze opomenout technologické zařízení, zásobování energiemi, dopravní obslužnost atd. Provozovateli je více právních subjektů, jež se liší rozsahem svých činností. Tyto činnosti mohou vykazovat různé úrovně požárního

nebezpečí, které se odvíjí od množství používaných požárně nebezpečných látek a jejich zpracování, velikost půdorysné plochy, popř. složitosti vnitřních dispozic objektu. Velké průmyslové podniky, u kterých se na základě zpracovaného posouzení požárního nebezpečí požaduje jednotka požární ochrany (PO), si musí tuto jednotku požární ochrany udržovat.[9]

EPS jsou systémy, které mají za úkol včasnou detekci případně prevenci vzniku požáru. Použití těchto systémů je značně rozsáhlé, ať už je to v oblasti průmyslových staveb, nákupních center, úřadů nebo, rodinný a bytových staveb. Jedná se o plně automatické systémy, které mohou dále varovat osoby, nacházející se v ohrožené lokalitě, spouštět hasební prvky určené k likvidaci požárů (sprinklery), zajistit únikové cesty z místa požáru a nakonec to nejdůležitější – zavolat hasičský záchranný sbor (HZS).[8]

Základní činnosti EPS

Na ústřednu EPS jsou napojeny požární hlásiče buďto automatické nebo neautomatické, manuální (tlačítkové). Ústředna má za úkol zpracovat informace z hlásičů a vybavit výstup, tj. signalizovat vznik požáru v hlídané oblasti, aktivaci výstupních obvodů pro signalizaci místa požáru v objektu a jeho předání HZS v případě potřeby. Současně musí provést sérii opatření, např. odblokování únikových cest, otevření kouřových klapek, odpojení výrobních či jiných technologií nebo aktivace požárního rozhlasu za účelem záchrany lidí a technologie přípravy budovy pro příjezd HZS. K akustické a optické signalizaci poplachu slouží sirény a majáky. Bloky KTPO (klíčový trezor požární ochrany) a OPPO (obslužné pole požární ochrany) slouží pro rychlejší přístup HZS do objektu a nastavení celého systému do stavu pro vstup požární jednotky. Zařízení ZDP (zařízení dálkového přenosu) slouží pro odeslání poplachové zprávy. [8]

Fungování EPS

EPS informuje svého uživatele o vzniku požáru akustickou a také optickou signalizací buď přímo v objektu nebo pomocí DPPC, který je umístěn u HZS. Detekci vznikajícího požáru zajišťují detektory, které jsou založené na různých principech. EPS signalizuje vznik požáru a následně dává signál zařízení zabraňujícímu rozšíření požáru (protipožární větrací zařízení, hasící zařízení, požární uzávěry otvorů).

Základní rozdělení EPS:

- konvenční - na smyčku můžeme připojit několik hlásičů. Při uvedení hlásiče do poplachu víme, že na smyčce je některý hlásič v poplachu,
- adresovatelné – hlásič rozhodne o uvedení do poplachu, ústředna ví, který hlásič byl uvedený do stavu poplachu. Adresace rezistorem nebo komunikace datová,
- analogové – hlásiče, které mají adresu a provádějí měření fyzikálními veličinami. Naměřené hodnoty posílají do ústředny a ta rozhodne o předpoplachu či poplachu.

Složení EPS:

- ústředna – zařízení přijímající a vyhodnocující výstupní elektrické signály hlásičů EPS. Signalizuje a vysílá informace o vlastním provozním stavu, ovládá doplňující zařízení,
- hlásiče požáru - přístroje, které reagují na daný signál a vytváří výstupní elektrický signál (samočinně nebo jsou uvedeny do činnosti osobou).

Základní rozdělení:

- tlačítkové hlásiče,
- samočinné hlásiče,
- optický hlásič kouře,
- hlásiče teplot.

Návrh systému

Jedná se o zpracování projektové dokumentace a koordinaci se zpracovatelem požárně bezpečnostního řešení stavby. Projektová dokumentace musí být schválená HZS místně příslušejícímu místu realizace. Firmy poskytující tuto činnost zajišťují dodávku zařízení, montáž, instalaci, programování, uvedení do provozu, pravidelné revize a kontroly.

Komplexně řešený systém EPS umožňuje:

- *rychlé a spolehlivé určení místa vzniku požáru,*
- *vyhlášení požárního poplachu,*
- *aktivace a řízení evakuačního systému v dané oblasti,*
- *ovládání a signalizace stavu dalších požárně bezpečnostních zařízení,*
- *automatickou komunikaci s HZS. [8]*

Inovace EPS

Při vzniku nových průmyslových zón může být návrh rozmístění požárních stanic a doby dojezdu jednotek PO řešen pomocí technologie GIS s ohledem na stávající potřeby a sjednocen v rámci územního celku tak, aby nové požární stanice a/nebo komunikace byly potřebné pro plnění nejen současných, ale i budoucích potřeb stále rostoucí společnosti. Výhledově by bylo účelné hledat způsob návrhu, který by byl řešil rozmístění, vybavení a finanční zabezpečení jednotky požární ochrany v místech nebo v blízkostech průmyslových či komerčních zón. [9]

Obr. 15. Elektronická požární signalizace

Zdroj: [23]

3 JAKÉ JSOU VÝHODY A NEVÝHODY

3.1 PZTS

Výhody systému:

- hlavním úkolem je informovat obsluhu o pokusu vniknutí cizí osoby do chráněného prostoru a na tento stav upozornit,
- okamžité odeslání informace o narušení prostoru na DPPC, kde operátoři mohou zavolat na dohodnutá telefonní čísla a informovat o nastalé situaci s cílem minimalizovat rizika a ztráty,
- přijímá a vyhodnocuje výstupní elektrické signály od čidel PZTS,
- napájí čidla a další prvky PZTS elektrickou energií,
- možnost instalace bezdrátových zařízení, která mají stejné funkční vlastnosti jako „konvenční“. Každé koncové zařízení je vybavené vysílačem a baterií. Vysílače pracují v režimu úsporném a zároveň signalizují ústředně PZTS stav baterií,
- detektory pro vnitřní použití slouží pro instalaci uvnitř zabezpečené budovy nebo do míst bez vlivu povětrnostních podmínek,
- detektory pro vnější použití jsou využívány hlavně u velkých průmyslových objektů.

Nevýhody systému:

- PZTS (alarm) u špatně nastavených, navržených nebo neudržovaných systémů, dochází k zbytečné signalizaci o narušení prostoru,
- nastavení není složité, ale servisní technik, který nastavení provádí, musí mít dostatečnou kvalifikaci k vyladění tohoto zařízení,
- podobně je tomu s navržením sytému a to z hlediska rozmístění detektorů PZTS. Údržbou se myslí i občasné ometení pavučin či ochrana čidel při malování,
- zabezpečovací zařízení, které je nefunkční a tudíž nemůže plnit svoji funkci je pro investora ztrátovým a zbytečným projektem,
- alarm sice nechytí zloděje, ale úkolem PZTS je upozornit na vzniklou situaci,
- výše investice, vynaložená na PZTS se může zdát relativně vysoká. Srovnejte ji ale s hodnotou majetku, který taková PZTS chrání.

3.2 CCTV

Výhody systému:

- detekce vniknutí, detekce konfliktů, funkce pro odhad počtu obyvatel nebo počítání zaměstnanců u vstupních bran,
- v oblasti dopravy detekce hledaných vozidel, kontrola rychlosti, analýza průjezdnosti, dopravní hustoty,
- v komerčních a průmyslových objektech jsou doplněny o funkci přehledovou a informační,
- napomáhá k odhalení případné neloajálnosti vlastního personálu,
- kontrola dodržování technologických a výrobních postupů,
- záznam průběhu měřených nebo sledovaných veličin (váhy, kasy, pokladny),
- přesná lokalizace míst narušení s identifikací narušitele,
- dokonale archivuje historie událostí (archivuje záběry z chráněného prostoru před, v průběhu i po vzniku mimořádné události),
- kompatibilita a možnost integrace s ostatními bezpečnostními systémy,
- zaznamenávají největší rozvoj ze skupiny poplachových systémů.

Nevýhody systému:

- hlavním problémem velkého počtu kamer je hlavně velké množství informací, které generují,
- ztráta soukromí neboť zvláště při pohybu ve velkých městech či v nákupních střediscích člověk dohledu CCTV neuteče, proto je žádáno o změnu legislativy pro zpřísnění jeho ochrany,
- mnohé kamery jsou rozmístěny protiprávně a k těžko zjistitelným účelům, když zabírají prostory soukromých bytů,
- zpochybňována je i funkce efektivity v potlačování zločinnosti.

3.3 EKV

Výhody systému:

- je souborem opatření k zajištění řízení i evidence přístupu do zabezpečeného objektu a prostor. Přístupová práva jsou přidělena každému uživateli dle předem daných kritérií,

- u evidence docházky lze na terminálech provádět registraci začátku, konce nebo několika typů přerušení pracovní doby,
- možnost sledování pohybu a přítomnosti v jednotlivých úsecích,
- kontrola vstupů do místností (možnost získat přehled o vstupu, délce trvání včetně příslušného data a času),
- evidence návštěv jsou využívaný identifikační karty nejen pro pracovníky dané společnosti, ale i pro návštěvy, které vstupují do objektu za konkrétním účelem,
- kontrola vjezdů do soukromých parkovišť nebo přes podnikové vrátnice,
- systém může odemykat a zamykat křídlové dveře, posuvné lineární dveře, turnikety, branky,
- objednávání a výdej stravy lze využít k automatizaci objednávek a kontrole výdeje stravy. Zejména pro hromadné stravování v závodních jídelnách,
- jednotlivé systémy jsou flexibilní a umožňují napojení na další bezpečností systémy sloužící k ochraně objektu,
- maximální kontrola a ochrana objektu.

Nevýhody systému:

- je instalováno do horní části dveří, což pro dveře méně tuhé konstrukce není optimální,
- méně vhodné pro dveře, které se otvírají směrem ven, protože instalace zámku sníží výšku průchodu dveřmi,
- nejsou certifikovány jako zámky (nelze u nich deklarovat bezpečnostní třídu) což může v případě vloupání přinést potíže při jednání s pojišťovnou o náhradě škody,
- mezi speciality na požární bezpečnost stavby není jednotný názor o přípustnosti jejich použití na únikové východy.

3.4 EPS

Výhody systému:

- EPS informuje svého uživatele o vzniku požáru akustickou nebo optickou signalizací v objektu nebo pomocí DPPC,
- přesná identifikace jednotlivých požárních prvků v systému a tím i možnost přesné a rychlé lokalizace místa vzniku požáru,

- každý prvek je opatřen přesným popisem, který je zobrazován na displeji požární ústředny nebo ovládacího panelu,
- jednoduchá kabeláž požárních linek a jejich velká kapacita k osazení jednotlivými detekčními prvky,
- na lince mohou být připojeny jak prvky detekční tak i ovládací. Na 1 adresné lince mohou být řádově stovky prvků v závislosti na jejich odběru a použitém systému požární signalizace EPS,
- jehož úkolem je včasná detekce případně prevence vzniku požáru,
- signalizuje vznik požáru a dává signál zařízení zabraňující rozšíření požáru,
- rychlé a spolehlivé určení místa, kde požár vznikl,
- následně je vyhlášen požární poplach,
- aktivace a řízení evakuace v objektu,
- ovládání a signalizace stavu požárně bezpečnostních zařízení,
- automatická komunikace s HZS.

Nevýhody systémů:

- velmi omezená nebo žádná možnost přesného umístění požárního hlásiče detekujícího poplach,
- není možnost zjišťovat stavy jednotlivých detekčních prvků v rámci linky,
- obsluha konvenční požární signalizace je omezena pouze na ovládání celých linek (nikoli jednotlivých požárních hlásičů),
- problematické provádění různých změn v EPS z hlediska ovládání či přiřazování jednotlivých požárních hlásičů do skupin (zpravidla 1 linka = 1skupina hlásičů).

4 BUDOUCÍ VÝVOJ VE VZTAHU K DOHLEDOVÉMU A POPLACHOVÉMU PŘIJÍMACÍMU CENTRU (DPPC)

S rozvojem komerčních služeb soukromých hlídacích agentur přebírají úlohu vyhlášení poplachu od sirén přenosová zařízení, která zprostředkují po zvoleném médiu (telefonní linka, ISDN linka, rádiová síť, GSM síť) přenos informací o stavu systému či narušení objektu v digitální podobě majiteli nebo na monitorovací pracoviště DPPC hlídací agentury nebo policie. V odůvodněných případech je žádoucí používat dvě nezávislé přenosové cesty, např. telefonní linka a rádiová síť. Používané formáty přenosů jsou normalizovány. Oproti lokální signalizaci poplachových stavů nabízí připojení elektronických bezpečnostních systémů (EPS, PZTS, CCTV) na pracoviště DPPC daleko efektivnější ochranu objektů. V případě narušení vyjíždí na místo speciální zásahová jednotka hlídací agentury, policie nebo hasičů. Přenos poplachových signálů je samostatná úloha vymezená funkcí poplachového přenosového systému. Tato oblast je normalizačně popsána souborem norem řady ČSN EN 50136. [17]

Výrobci

Radom, NAM [17]

Obr. 16. Elektronická ostraha objektů

Zdroj: [24]

4.1 DPPC

Jedním z nejdůležitějších pracovišť průmyslu komerční bezpečnosti jsou DPPC. Tento název původně znamenal název jednoho z pracovišť Policie ČR, zpravidla dispečerské

pracoviště, které provádělo vyhodnocování signálů PZTS. V dnešní době má však DPPC daleko širší význam a zahrnuje také širší okruh činností než v minulosti. [11]

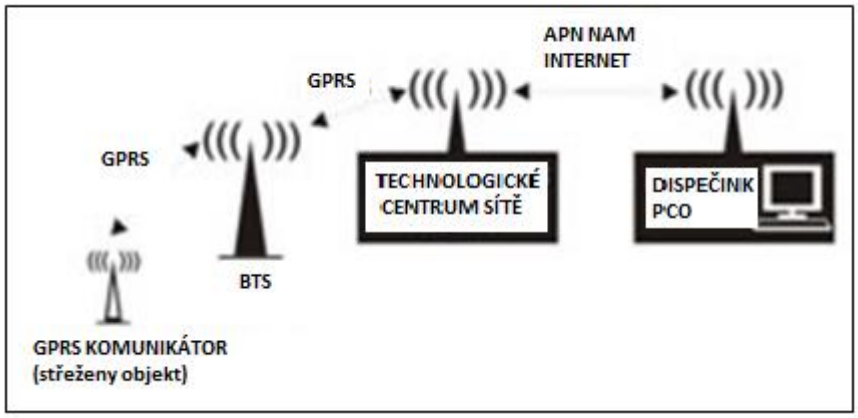
DPPC jsou koncipovány:

- samostatný systém s vlastním síťovým napájením a zálohováním,
- integrální součást osobního počítače.

Současné typy DPPC, jako přístrojové zařízení

Tab. 9. Současné typy DPPC, jako přístrojové zařízení [2]

Linkové	jednostranné, oboustranné, jednolinkové, vícelinkové, s využitím JTS
Kombinované	kombinace linkového a radiopultu
GSM	s využitím mobilních sítí a GSM brány
ISDN	s využitím virtuálních linek a rychlosti přenosu dat na PCO
CCTV	kamerové - linkové i radiové
kombinované	kombinované z hlediska využití technických prostředků



Obr. 17. Napojení pomocí GSM/GPRS

Zdroj: [25]

Služby DPPC

Tab. 10. Služby DPPC [10]

Základní nabídka	Dálkový monitoring PZTS
	Dálkový monitoring EPS
	Dálkový monitoring CCTV
	Kontrola stavu objektu výjezdovou jednotkou
	Monitoring uzamykání objektu
	Zajištění objektu proti vzniku dalších škod
	Služba TÍSEŇ – přivolání rychlé pomoci
Využití v dopravě	Střežení automobilů pomocí systému GPS
	Odstavení odcizeného vozidla v provozu
	Navigování zásahové jednotky k vozidlu
Jiná využití	Dálkové ovládání topení
	Hlídání teploty chladících zařízení
	Chod záložních agregátů
	Monitoring klimatizace, vzduchotechniky, elektrické, komunikační a počítačové sítě
	Provozní kontinuita a nouzové stavy
	Evakuační postupy
	Zpracování signálů

4.2 Budoucnost DPPC

Celé technologické odvětví zaznamenává v posledních letech strhující vývoj. První zařízení DPPC neumožňovala ani archivaci zpráv, pouze vizuálně signalizovala poplachové stavy v objektech. Postupem času se indikační zařízení modernizovala do podoby tabla s LCD

displejem, kde se již zobrazovaly typy zpráv z objektů. S příchodem PC se pak začaly vyvíjet aplikace, které se staraly o kódový překlad, zobrazení i automatickou archivaci dat. Drtivá většina dnes v praxi využívaných zařízení již funguje na platformě softwarové aplikace, pro které se obecně ustálil název monitorovací software. V poslední době se snaží využít výrobci těchto monitorovacích softwarů pro přenosy zpráv ze vzdálených objektů na DPPC také internet. Typickým zástupcem tohoto moderního přístupu je KRONOS NET 2. REVOLUTION. [8]

4.3 KRONOS NET 2. REVOLUTION

Základní vlastnosti jsou komplexnost, kapacita, automatizace, bezpečnost, skupinová práce, nové technologie a kontinuální vývoj, nezávislost na dodavatelích a přenosových zařízení. [13]

Výhody

Tab. 11. Výhody KRONOS NET 2.0 REVOLUTION [13]

Výhody pro management a obchod	Kontrolní funkce (vyřizování požadavků klientů)
	Statistiky a reporty (zásahy, servisní práce, reklamace)
	Zvyšování výnosů (fakturace jednorázových úkonů, poskytování nových služeb)
	Implementace obchodních akcí (např. 3 měsíce zdarma, 1. výjezd zdarma)
	Nižší ceny přenosových zařízení
	Řízení smluv (automatické připomínání termínů)
Výhody pro správce	Vzdálený přístup k aplikaci
	Automatické SMS/email informace o problému
	Automatické reportování o funkčnosti systému
	Rychlé zadávání objektů pomocí šablon
	Automatické připomínání prací u objektů
	Opakovaná kontrola uzavření objektu, a to na minuty

	Kontrola reportů poplachů s možností dodatečné editace
	Detailní historie změn na objektech
	Znalostní báze
	Automatické zálohování databáze
Výhody pro dispečinky	Intuitivní ovládání (komiks)
	Nastavení barevnosti a zvuku pro jednotlivé události
	Obsluha akce na objektu, nikoli jednotlivých poplachů
	Zpoždění vybraných poplachů (výpadek sítě, baterie)
	Kontrolní seznam předepsaných úkonů
	Jednoduchá tvorba reportů (zásah)
	Jednoduché zakládání servisních požadavků
	Možnost přímého vytočení telefonního čísla, odeslání SMS či emailu zákazníkovi
	Identifikace volajícího zákazníka s propojením na kartu objektu
	Záznam hovoru se zápisem databáze
	Chatování mezi konzolami
Výhody pro techniky	Sledování servisních prací (automatické informace o zpoždění, priority)
	Vzdálený přístup ke kartě a historii událostí objektu
	Kontrola přenesení zpráv při testu komunikace
Výhody pro účetní	Komplexní podklady pro fakturaci (poplatky dle smlouvy, slevy, jednorázové úkony, zásahy)
Výhody pro zákazníka	Nové služby (automatické vyřizování SMS dotazů, automatické výpisy v nastavených intervalech, internetový přístup, odložení doby kontroly uzavření objektu, řízení jednorázových či dočasných přístupů do objektu)

4.4 IP kamerové systémy

IP kamery, respektive IP kamerové systémy tvoří bezpochyby novou generaci DPPC. Na základě kombinace inovativních technologií, jako pořizování videa, jeho zpracování, přenos s koordinací celého systému prostřednictvím VMS softwaru, nabízí IP kamerové systémy širokou škálu možných využití. Problematika projektování sofistikovaných dohledových systémů se bude jistě v následujících letech ještě intenzivně vyvíjet a vytváří, tak prostor dalšího možného výzkumu či jiného uplatnění.

Odvětví bezpečnostního průmyslu prochází již několik let intenzivním rozvojem, což je zapříčiněno, jak stále větší potřebou chránit ohrožené zájmy uživatelů, tak strmým vývojem ICT (informačních a komunikačních technologií). Právě implementace ICT do sektoru komerční bezpečnosti je stále častěji využívána především za účelem přizpůsobení současným trendům. Těmi jsou především interoperabilita systémových prvků, tvorby specializovaných bezpečnostních aplikací a také integrace jednotlivých bezpečnostních systémů, jako například EKV, PZTS, CCTV do jednoho sofistikovaně fungujícího celku. Tento trend je možné sledovat i v problematice dohledových systémů a právě IP kamery, respektive síťové video, jsou prvky, jež na tyto požadavky reagují. [9]

4.5 Biometrická identifikace

Nová technologie nezadržitelně proniká do našeho každodenního života. Čím dál častěji se při otevírání dveří či při vstupování do počítačů identifikujeme pomocí našeho těla. Tato identifikace se provádí pomocí otisku prstu, dlaně, oční duhovky, obličeje, kartografie žil, tvaru lebky atp. Používání klíčů, magnetických karet, čipů, jmenovek a jiných prostředků ke vstupu do dané místnosti či lokality, přístupu k aplikacím atd. se blíží ke svému konci. Zrozená technologie, která umožňuje absolutně nezpochybnitelnou identifikaci osob, se nazývá biometrie. Biometrie je souhrn výpočetních technik, které dovolují automaticky rozpoznat jakoukoliv osobu na základě jejich fyzických parametrů. Biometrie se stala během několika let tím nejmodernějším a nejspolehlivějším způsobem v oblasti kontroly vstupů.

„Rozdíl mezi čipovou kartou a otiskem prstu je propastný!“ [26]

Biometrické systémy:

- *jedinečná identifikace - proces identifikace je založený na rozpoznávání fyzických charakteristik osoby. Proto má obrovský význam používat metody biometrie všude*

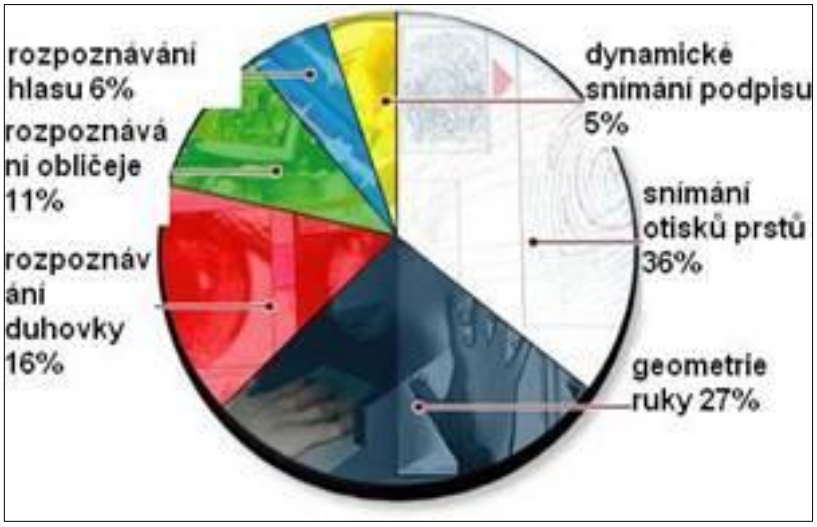
tam, kde záleží na unikátní identifikaci. Jde především o aplikace spojené s bezpečnou autorizací do chráněného systému nebo k určení správné totožnosti,

- *ověřování identity - ověřování neboli verifikace označuje proces potvrzení správnosti (pravosti). Totožnost jedince je potvrzena až po srovnání sejmutého vzorku s již dříve uloženou šablonou vzoru.*
- *postup autentizace - nejprve dojde k sejmutí (skenování) potřebných fyziologických charakteristik a vytvoření referenčního profilu (vzoru). Při identifikaci se nasnímaný vzorek porovná se šablonou. Výsledek celého procesu je vlastně shoda (povolen přístup) nebo neshoda (odmítnutí). O nic jiného se v podstatě biometrie nestará.*

Nejvíce rozšířené biometrické vlastnosti s popisem toho, co se měří:

- *otisk prstu (struktura papilárních linií a jejich detailů),*
- *dynamika podpisu (rozdíly v tlaku a rychlosti psaní),*
- *geometrie tváře (vzdálenosti specifických částí – oči, nos, ústa…),*
- *duhovka (obrazový vzorec duhovky),*
- *sítnice (struktura žil na očním pozadí),*
- *geometrie ruky (rozměry dlaně a prstů),*
- *struktura žil na zápěstí (struktura žil),*
- *tvar ucha (rozměry viditelné části ucha),*
- *hlas (tón a zabarvení hlasu),*
- *DNA (řetězec deoxyribonukleové kyseliny).*

- *BioStation/BioEntry Plus - nabízí komplexní řešení pro dobu docházky a řízení přístupu. S barevným LCD a vysoce kvalitním zvukem, nabízí různé úrovně interakce pro uživatele, včetně možnosti bezdrátové sítě LAN a USB paměti umožňující snadnou integraci do sítě. BioEntry Plus nabízí navíc bezkontaktní RF karety. Toto zařízení lze použít od nejběžnějších aplikací, které fungují autonomně až po kompletní přístupové systémy připojené k síti.[27]*



Obr. 18. Podíl jednotlivých technologií biometrických systémů na trhu

Zdroj: [27]

Biometrie je klíčovou schopností, která dokáže identifikovat nepřítele, odhalit jeho anonymitu, kterou potřebuje skrýt a včas jej odhalit. Schopnost identifikovat a ověřit jedince je také nutné zajistit pro bezpečnou a rychlou pracovní funkci. Biometrické funkce jsou uplatňovány prostřednictvím různých taktik, technik a postupů. Biometrická identifikační manažerská agentura (BIMA), podle DoD směrnice 8521 01E , slouží k:

- *Zákon DoD, jako zastánce pro biometrii,*
- *důležité ve vývoji a zavádění biometrických technologií,*
- *doporučení schopností s cílem přispět k posílení biometrického společenství. [28]*

Obr. 19. Biometrie

Zdroj: [28]

4.6 Inteligentní budovy (IB)

Za IB je považována budova, v níž jsou jednotlivé inteligentní prvky či systémy integrovány a řízeny prostřednictvím jediného systému. Všechny automatizační prvky či subsystémy v budově mají jediný základní cíl. Cílovým chováním tohoto systému je ve všech systémech vytváření, udržování a správa podmínek pro pobyt v prostorách budovy (anebo procesy v budově probíhající) takových, že reagují na měnící se vnější podmínky anebo vnitřní či vnější požadavky. To vše s cílem optimální spotřeby energií a minimalizace nákladů. Protože budování automatizačních systémů v budovách zvyšuje investiční náročnost budovy za zvýšení komfortu poskytovaných služeb v IB a snížení provozních nákladů. [29]

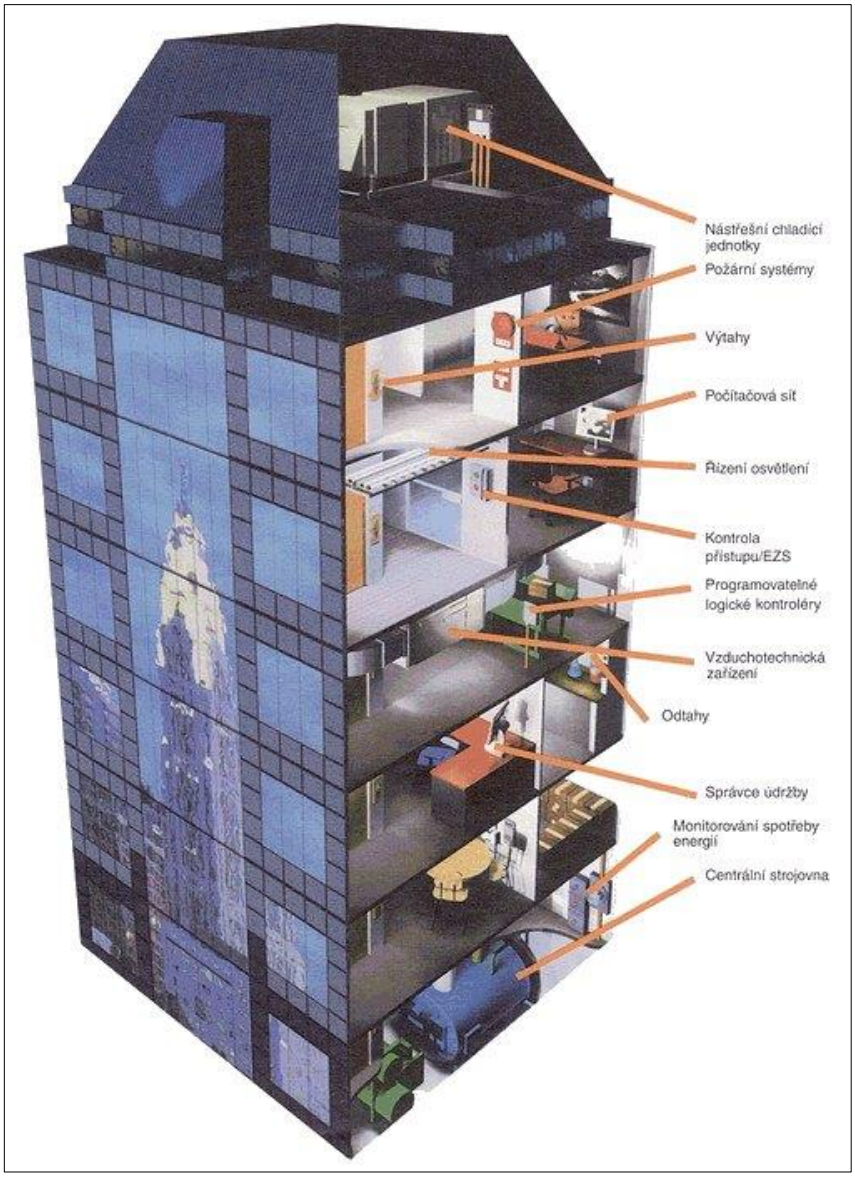
Důvody proč vůbec IB vznikají:

- *zvýšení komfortu poskytovaných služeb a s ní spojené zvýšení ceny pronájmu,*
- *snížení spotřeby energií,*
- *snížení provozních nákladů,*
- *zvýšení produktivity,*
- *zrychlení návratnosti investice,*
- *prodloužení životnosti budovy. [29]*

Budoucnost IB:

- *v poslední době dochází zpravidla k propojování systémů. Dodavatel systému IB je obvykle majoritně zaměřen na část osvětlení, zabezpečení, multimédií nebo částečně na řízení teplot v objektu,*
- *trendem světového výzkumu je jednak efektivní využití zdrojů energie, například včetně napojení na chytré sítě, jednak silná snaha implementovat prvky kybernetické inteligence tak, aby budova předvídala potřeby svých obyvatel a nedělala pouze to, co technik naprogramoval,*
- *jedná se o obor s širokou budoucností. Trend ukazuje vzrůstající poptávku po IB, která však u investorů často naráží na vyšší cenovou zátěž a obavu z komplikovanosti, která bude mimo kontrolu uživatelů,*
- *cílem je soběstačnost, maximální provozní bezpečnost, minimální energetická náročnost,*

- *největší výzvou je poskytnout všem takové systémy IB, které pomohou dostat budovu pod kontrolu (např. na chytrém telefonu). Zároveň je ale třeba jejich cenu dostat na úroveň dosažitelnou pro všechny, kdo staví nebo rekonstruují, aby tyto systémy ztratily punc luxusu a výstředního módního výstřelku podobně jako již zmíněné chytré telefony.[30]*



Obr. 20. Inteligentní budova

Zdroj: [31]

5 UVEĎTE TECHNICKÉ ŘEŠENÍ INTEGRACE POPLACHOVÉHO ZABEZPEČOVACÍHO A TÍSŇOVÉHO SYSTÉMU, UZAVŘENÉHO TELEVIZNÍHO A DOHLEDOVÉHO SYSTÉMU A SYSTÉMU KONTROLY VSTUPŮ

Integrace představuje moderní způsob využití současných technologických možností prvků PZTS, CCTV a EKV. Uvedené aplikace je možno integrovat navzájem nebo doplnit o systémy nepoplachové a tím zabezpečit zjednodušení automatizačních procesů v objektech.

Integrace:

- sjednocení, ucelení, splynutí, proces spojování ve vyšší celek, začlenění, zapojení,
- integrovaný systém - jedná se o systém mající jedno nebo více společných zařízení, alespoň jedním, z nichž je poplachová aplikace (ČSN CLC/TS 50398).

Aplikace:

- poplachová aplikace - PZTS, CCTV, EKV a EPS,
- nepoplachová aplikace - systémy určené k ovládání a jejichž primární funkcí není ochrana života, majetku anebo prostředí (např. topení, větrání, ventilace, správa energetiky, správa budovy, osvětlení).

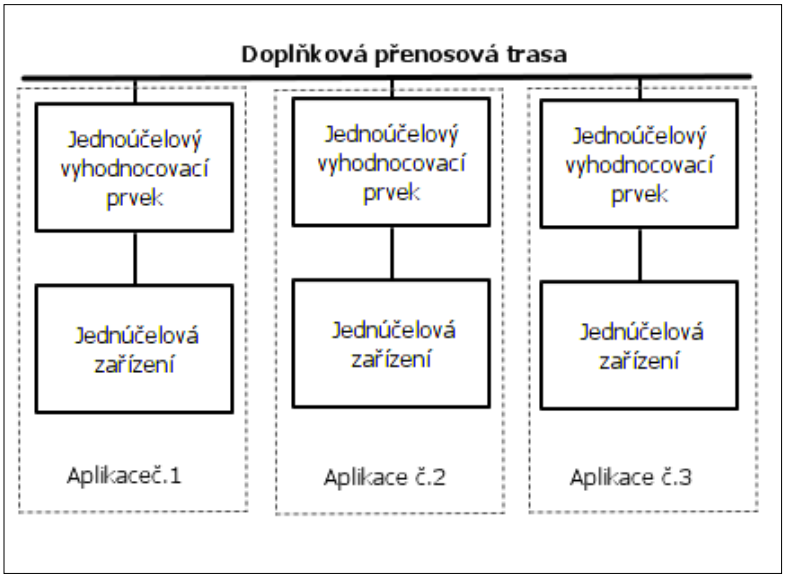
5.1 Konfigurace integrovaných poplachových systémů

Typ 1 – kombinace nebo integrace jednoúčelových poplachových systémů a jednoúčelových nepoplachových systémů,

Typ 2 A – kombinace a integrace poplachových a nepoplachových systémů, používající společné přenosové trasy a společná zařízení. Porucha v kterékoliv aplikaci nemá žádný negativní účinek na jakoukoliv další poplachovou aplikaci. K dosažení tohoto stavu je potřebné znásobení (nadbytečnost),

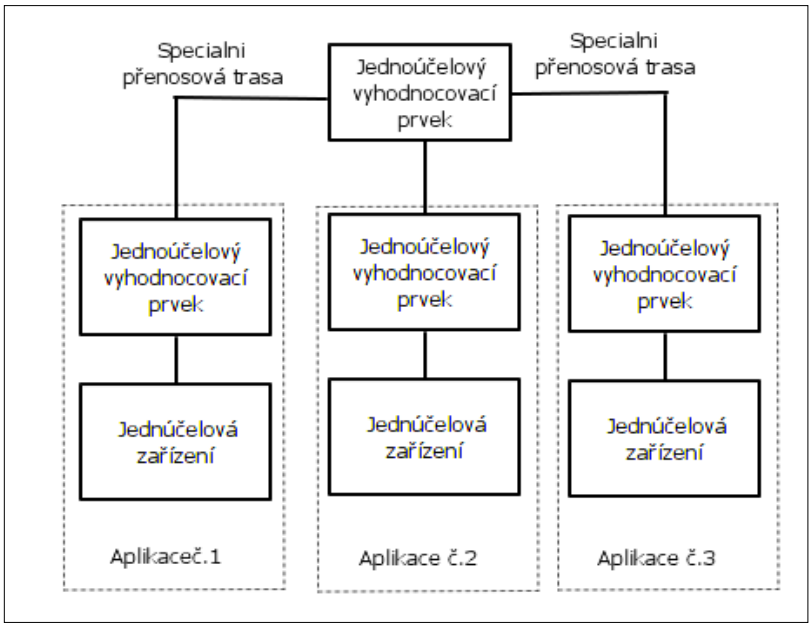
Typ 2 B – kombinace a integrace poplachových a nepoplachových systémů, používající společné přenosové trasy a společná zařízení. Porucha v jedné aplikaci může mít negativní účinek na jinou poplachovou aplikaci.[12]

Typ 1 - *kombinace nebo integrace jednoúčelových poplachových systémů a jednoúčelových nepoplachových systémů. Jednoúčelová zařízení jsou připojena ke společnému doplňkovému zařízení. Zařízení vyžadovaná normou v poplachové aplikaci nesmí být v žádném provozním stavu ovlivněna jakýmkoliv dalším jednoúčelovým systémem nebo doplňkovým zařízením. [12]*



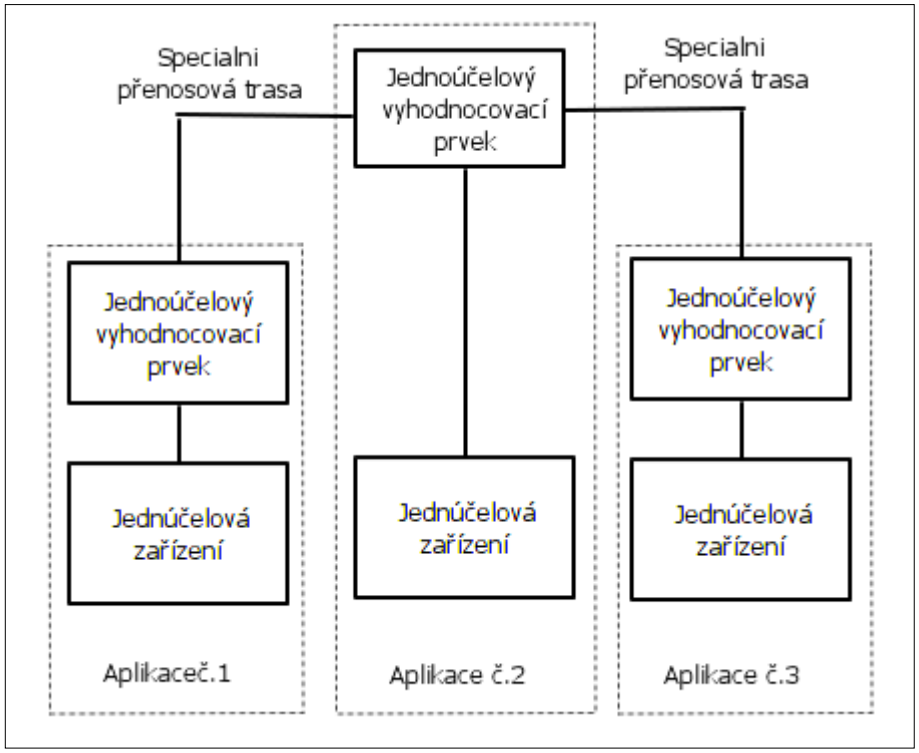
Obr. 21. Příklad konfigurace typu 1

Zdroj: [12]



Obr. 22. Příklad konfigurace typu 1, ústřední ovládací zařízení (CCF) třídy 1

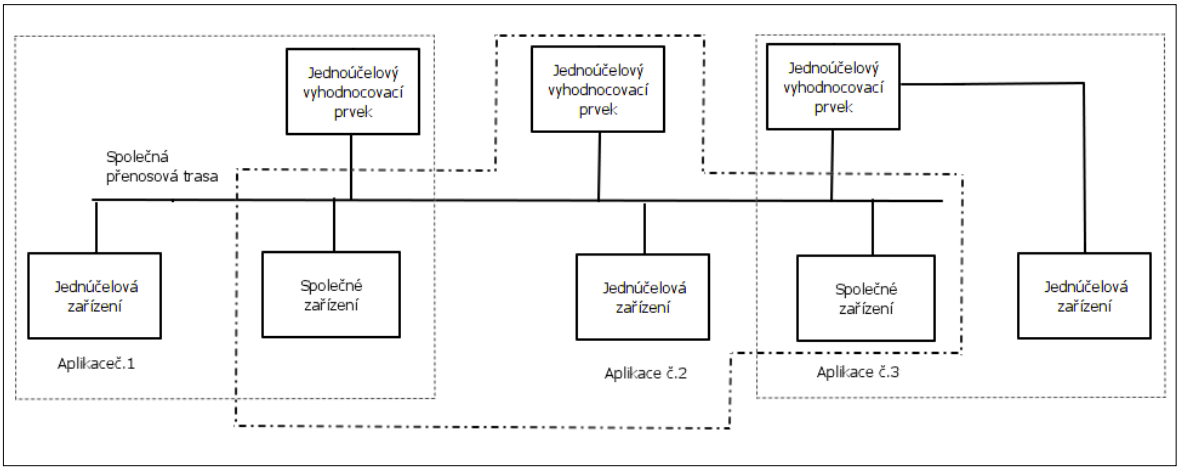
Zdroj: [12]



Obr. 23. Příklad konfigurace typu 1, ústřední ovládací zařízení (CCF) třídy 2

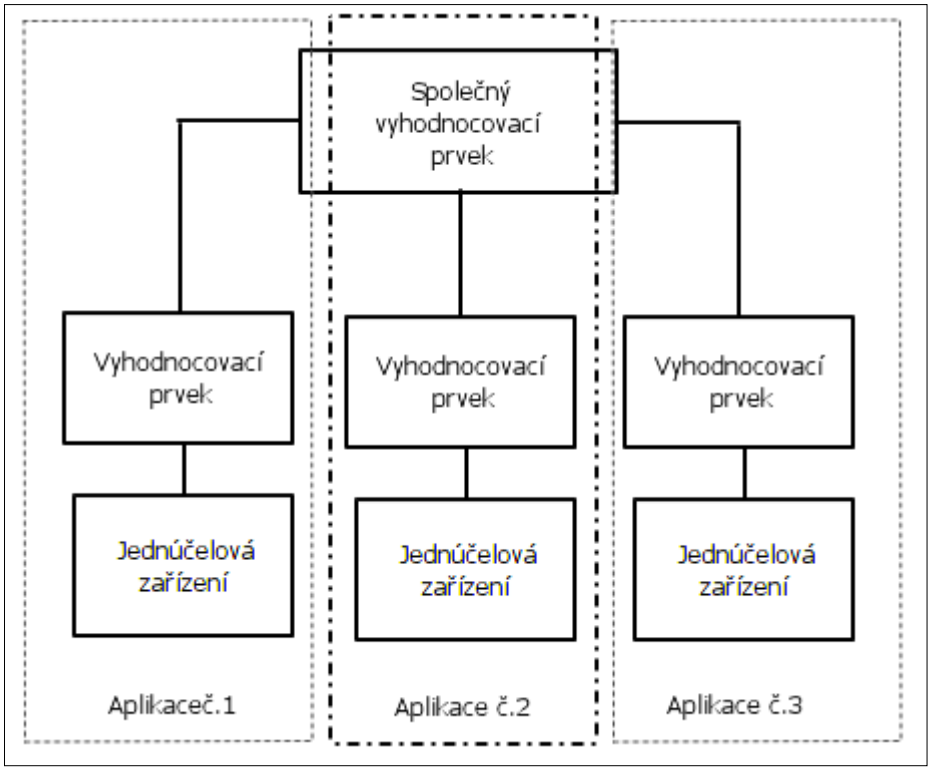
Zdroj: [12]

Typ 2 - *kombinace typu 2 je kombinací dvou nebo více jednoúčelových systémů, všechny využívají normou vyžadované zařízení společné nejméně pro jednu aplikaci. Kombinace typu 2 jsou dále rozděleny na Typ 2A a 2B. [12]*



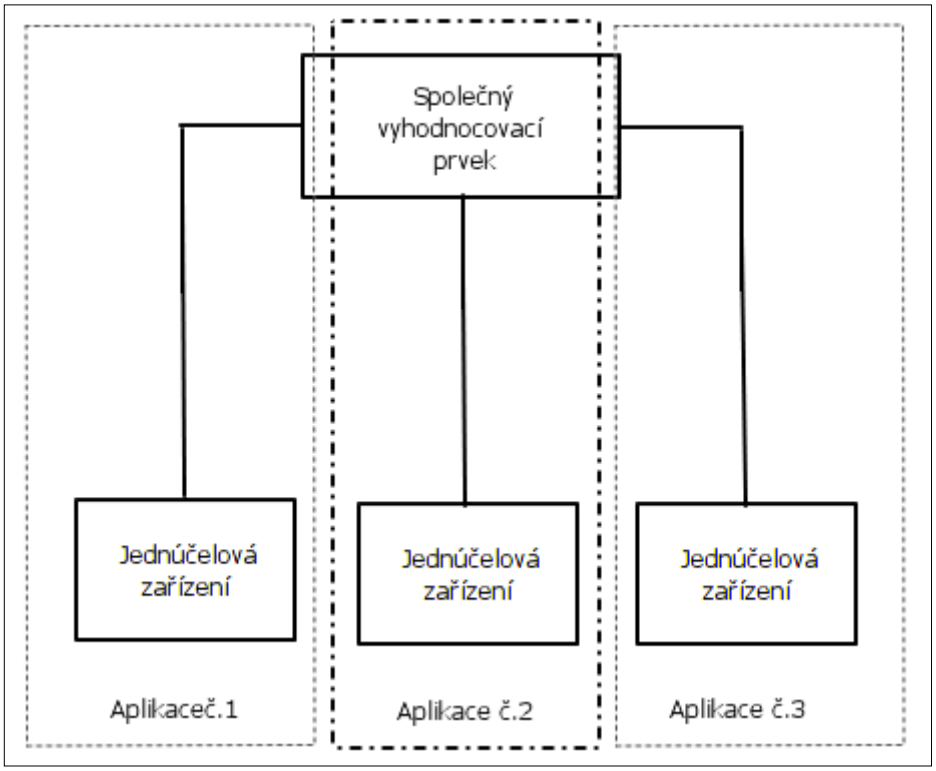
Obr. 24. První příklad konfigurace typu 2

Zdroj: [12]



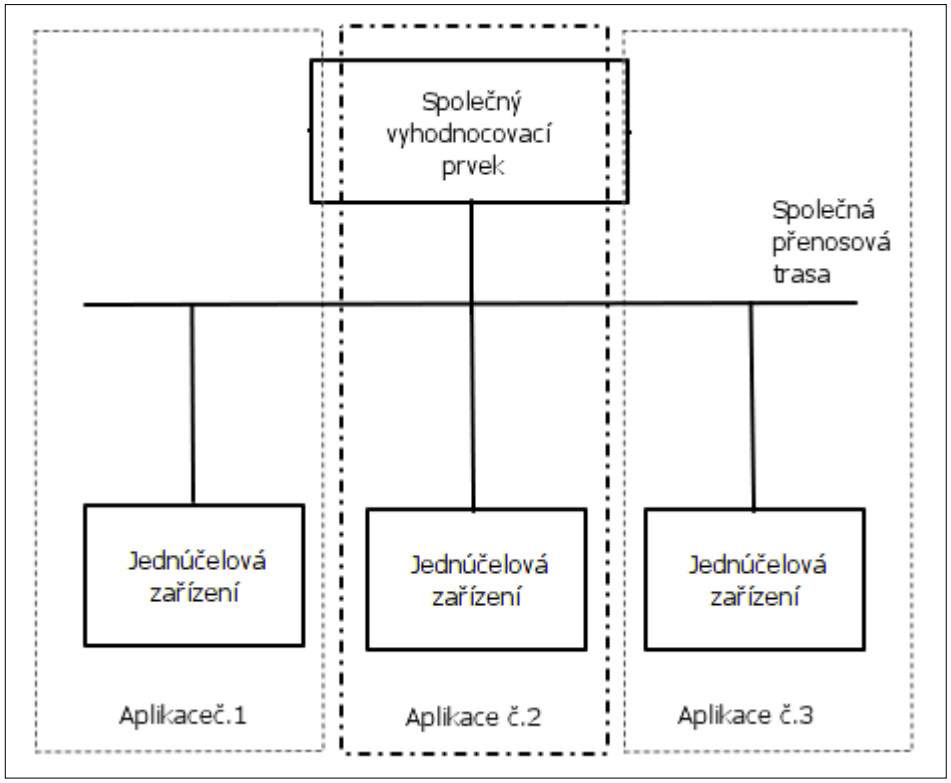
Obr. 25. Druhý příklad konfigurace typu 2

Zdroj: [12]



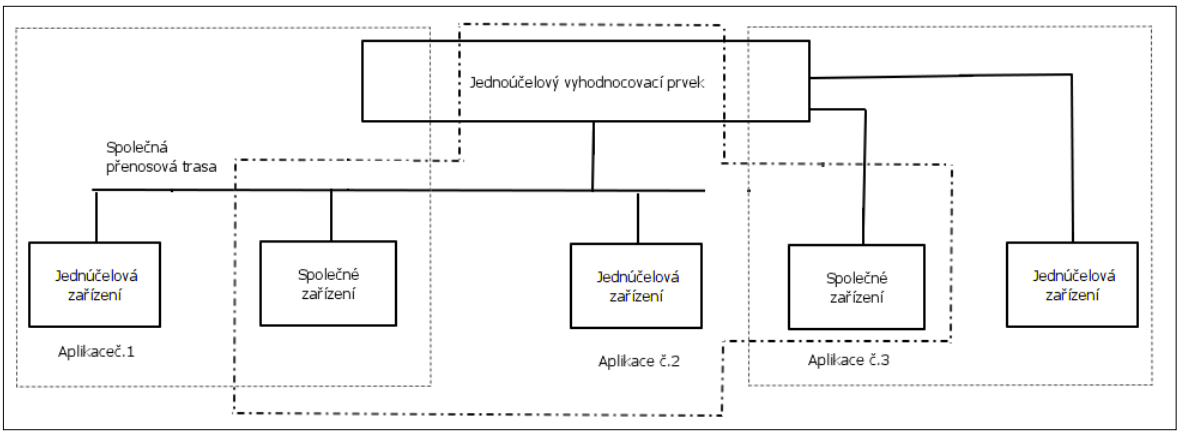
Obr. 26. Třetí příklad konfigurace typu 2

Zdroj: [12]



Obr. 27. Čtvrtý příklad konfigurace typu 2

Zdroj: [12]



Obr. 28. Pátý příklad konfigurace typu 2

Zdroj: [12]

5.2 Systémové požadavky na integrované poplachové systémy

Jedná se o systémové požadavky:

- návrh IPS – vyloučit možnost vzájemného negativního ovlivnění jednotlivých aplikací,

- možnost přenosu povelových signálů mezi aplikacemi, nebo z CCF,
- použití povelových signálů,
- přístupové úrovně (např. přístup/docházka),
- porucha společného zařízení - indikace ve všech dotčených aplikacích (sdílející toto zařízení),
- společné ovládací zařízení - doplněno o indikaci ovládaných aplikací,
- signalizace informací,
    - priority signalizace*:*
        1. poplachové signály (ochrana života, požár, napadení),
        2. poplachové signály (ochrana majetku, vniknutí do objektu),
        3. poplachové signály ostatní,
        4. poruchové signály (systémy ochrany života a majetku),
        5. poruchové signály ostatní,
        6. informace z nepoplachových systémů.
    - všeobecné požadavky na signalizaci priorit:
        1. možnost zobrazení doplňkových informací na vyžádání,
        2. jakákoliv činnost aplikace nesmí zamezit indikaci poplachu,
        3. signalizovat stav, kdy existují poplachy z více než jedné aplikace,
        4. nezobrazovat opakovaný poplachový signál,
        5. signalizace stavu, kdy již není možno zobrazit všechny poplachy.
- integrita prvků – společný monitoring – možnost detekovat a signalizovat selhání monitorovací sekvence jednotlivých aplikací

Centrální ovládací zařízení CCF:

- třída 1 - pouze k zobrazování informací v prostorách s provozní obsluhou + normou vyžadované signalizační zařízení (ústředny, signalizační panely) musí být ve stejných prostorech, - tj. V případě poruchy CCF bude signalizace poplachu zaznamenána obsluhou,

- třída 2 – pouze k zobrazování informace v prostorách s provozní obsluhou a to jako jediný signalizační prvek (informační displej) + pokud CCF II umožňuje i nastavení stavu STR/KLID,ZAP/VYP zón, ukládání parametrů musí být v souladu s aplikačními normami:
    - požadavky na CCF – identifikovat třídu CCF, umístit do příslušného prostředí, nevyužívat mimo IPS,
    - požadavky na CCF II - provoz CCF monitorovat v místě jeho nasazení, porucha CCF, monitoring napájení, signalizace výpadku jednotlivé monitorovací sekvence, plán postupu při poruše CCF, monitorovat komunikace s aplikacemi dle požadavků norem, UPS na dobu min. dle plánu při poruše.

II. PRAKTICKÁ ČÁST

6 UKÁZKOVÝ PŘÍPAD

Průmyslový objekt bude zabezpečen ve 2. bezpečnostní třídě. Na zabezpečení jsem použila výrobky firmy Jablotron, která nabízí široký sortiment kvalitních výrobků.

6.1 Charakteristika objektu

Průmyslový objekt (obrázek č. 30) je součástí průmyslového areálu (obrázek č. 29) v katastru obce Valašské Příkazy, které se nachází v údolí na rozhraní Bílých Karpat a Vizovické Vrchoviny. Jedná se o objekt bývalého zemědělského družstva, který bude v nejbližší době nově zrekonstruován. Budova je zděná z roku 1970. Své sídlo v něm najde nová společnost, která se bude zabývat návrhem a realizací interiérů na klíč, rekonstrukcemi bytových jader a zakázkovou truhlářskou výrobou. Firma bude zaměstnávat cca 40 zaměstnanců. V kanceláři bude pracovat 5 technických zaměstnanců, kteří budou zastřešovat výrobní proces. Samotnou výrobní činnost bude obstarávat 20 dělníků. Zbytek zaměstnanců budou montážní dělníci v terénu.

Průmyslový areál:

Obr. 29. Letecký snímek průmyslového areálu

Zdroj: [32]

Průmyslový objekt:

Obr. 30. Letecký snímek průmyslového objektu

Zdroj: [32]

6.2 Popis objektu

V průmyslové budově se budou nacházet následující prostory (příloha P III). V levé části budovy bude sklad s kanceláří pro skladníka. Do skladu povedou sekční vrata se vstupními dveřmi. Ve skladu budou uskladněny materiály pro truhlářskou výrobu, spotřebiče, stavební materiál a bytové doplňky.

Střední část budovy bude koncipována jako dílna s potřebným výrobním zařízením.

V pravé části budovy se budou nacházet kanceláře, technická místnost, kotelna, šatna, sprchy a sociální zařízení a chodba.

7 NÁVRH BEZPEČNOSTNÍHO SYSTÉMU

7.1 PZTS

Úkolem PZTS je informovat obsluhu o pokusu vniknutí do chráněného prostoru. Slouží k zabezpečení vnitřních prostor a vnějších prostor.

Rozmístění prvků

K zabezpečení vnitřních prostor (příloha P II) jsem použila u vstupních dveří ústřednu s GSM/GPRS/LAN komunikátorem s rádiovým modulem, sběrnicový přístupový modul s displejem, klávesnicí a RFID a 4 ovládací segmenty přístupových modulů. Do skladu budou instalována sekční vrata. Vnější prostory průmyslového objektu (obrázek č. 36) budou chráněny plotem. Ke vjezdu do areálu bude sloužit elektricky ovládaná brána. Zaměstnanci budou vstupovat brankou s elektrickým zámkem. V případě narušení chráněného prostoru bude díky napojení na DPPC okamžitě upozorněno jeho nejbližší výjezdové vozidlo se sídlem v nedalekých Valašských Kloboukách.

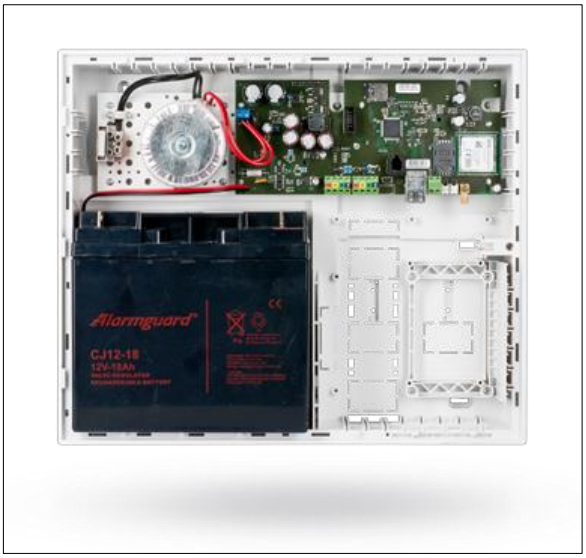
Soupis prvků

Tab. 12. Soupis prvků PZTS [33]

Druh	Cena za jednotu v Kč bez DPH	Množství	Celková cena v Kč bez DPH
Ústředna	9871	1	9871
Přístupový modul	1730	1	1730
Ovládací segment přístupových modulů	92	4	368
Sekvenční vrata	38000	1	38000
Elektricky ovládaná brána	40000	1	40000
Branka s elektrickým zámkem	7000	1	7000
Oplocení areálu	251	280 m	70280
Cena celkem			167249

Rozpis prvků

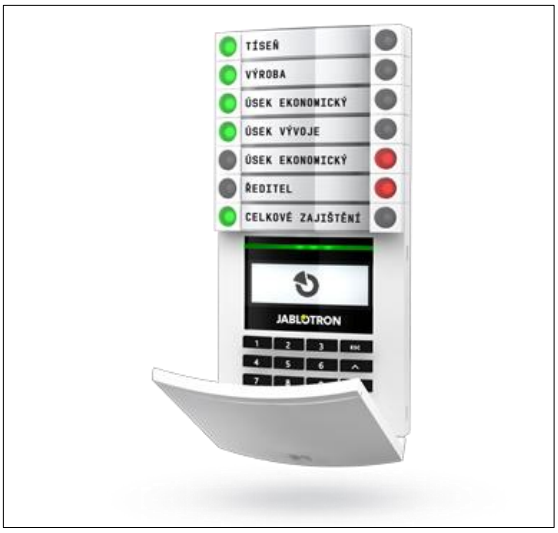
- JA-106KR Ústředna s GSM/GPRS/LAN komunikátorem s rádiovým modulem
  Cena 9871 Kč bez DPH
  Počet: 1



Obr. 31. Ústředna

Zdroj: [33]

- JA-114E Sběrnicový přístupový modul s displejem, klávesnicí a RFID
  Cena 1730 Kč bez DPH
  Počet: 1



Obr. 32. Sběrnicový přístupový modul

Zdroj: [33]

- JA-192E Ovládací segment přístupových modulů
  Cena 92 Kč bez DPH
  Počet: 4

Obr. 33. Ovládací segment přístupových modulů

Zdroj: [33]

- Průmyslová sekční vrata Alutech3 x 3 metry (vhodná do všech průmyslových a skladovacích objektů).
  Cena 38000 Kč bez DPH
  Počet: 1

Obr. 34. Sekvenční vrata

Zdroj: [34]

- Elektricky ovládaná brána - průjezd 4,5 metrů, automatizace brány, GSM ovládání
  Cena 40000 Kč bez DPH
  Počet: 1
- Branka s elektrickým zámkem
  Cena 7000 Kč bez DPH
  Počet: 1

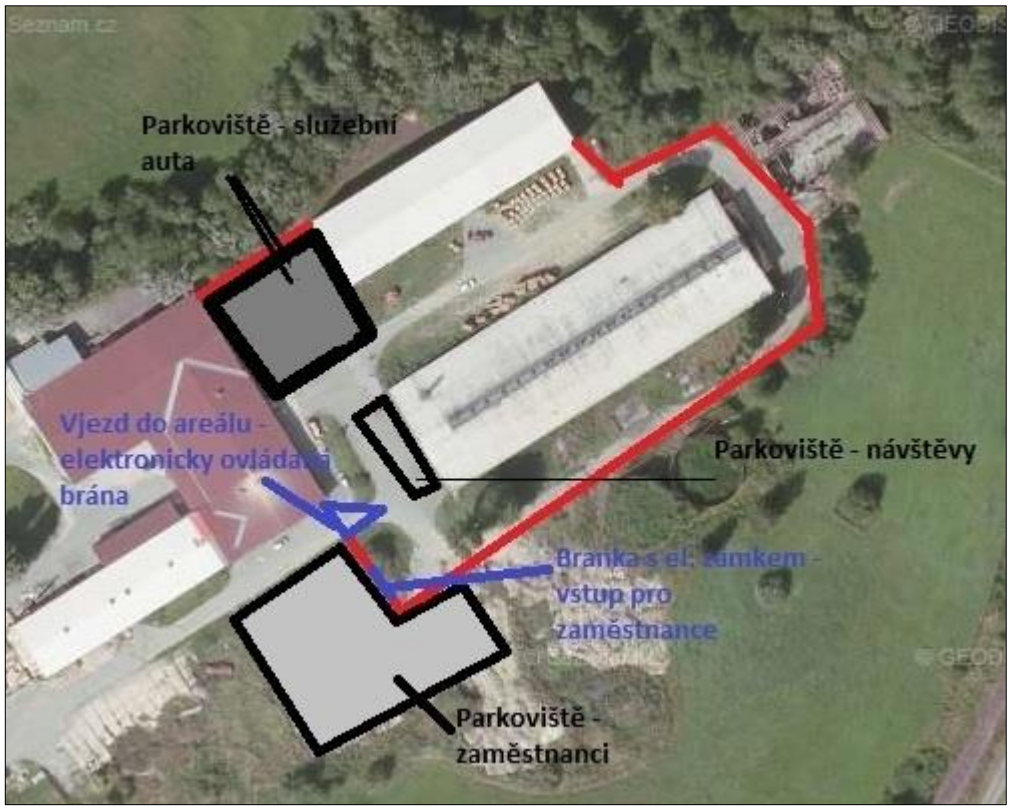
Obr. 34. Elektricky ovládaná brána a branka

Zdroj: [34]

- Oplocení areálu - plot se sloupky a betonováním – výška 2 metry, délka 280 metrů
  Cena 70280 Kč bez DPH

Obr. 35. Oplocení areálu

Zdroj: [34]



Obr. 36. Návrh PZTS v průmyslovém objektu

Zdroj: [33]

7.2 CCTV

Kamerové systémy slouží k předcházení krádežím. Dále plní funkci přehledovou, informační, monitoringu (např. výroby, kdy je sledován určitý výrobní postup nebo záznam expedovaných výrobků).

Rozmístění prvků

V daném návrhu (příloha P II) jsem použila 6 kamer (K1 – K6):

- K1 – venkovní kamera, monitoruje prostor vjezdu do areálu (bránu),
- K2 – vnitřní kamera, monitoruje vstup do budovy (vchodové dveře),
- K3 – venkovní kamera, monitoruje parkoviště pro zákazníky,
- K4 - venkovní kamera, monitoruje parkoviště pro firemní vozidla,
- K5 – venkovní kamera, monitoruje vjezd do skladu,
- K6 – venkovní kamera, monitoruje prostor za budovou (okna dílny).

Soupis prvků

Tab. 13. Soupis prvků CCTV [33]

Druh	Cena za jednotu v Kč bez DPH	Množství	Celková cena v Kč bez DPH
IR DOME bezpečnostní kamera barevná	3047	1	3047
Venkovní bezpečnostní IR kamera barevná	3463	5	17315
Napájecí zdroj	1351	1	1351
DVR rekordér	7616	1	7616
Harddisk	2067	1	2067
Venkovní systémový kabel	1247	1	1247
Adaptér	15	7	105
Konektor	30	12	360
Napájecí distributor	210	1	210
Cena celkem			33318

Rozpis prvků:

- FS-9761HB29 - IR DOME bezpečnostní kamera barevná (obrázek č. 10), varifokal objektiv 2.8mm/105°~12mm/23°, 700TVř, 0Lux – IR 10 – 15m, DWDR, 2 DNR, Den/Noc, BLC, OSD, čip 1/3 SONY Super HAD II, DC12V/320mA
  Prodejní cena: 3047 Kč bez DPH
  Počet: 1 (K2)
- KPF150 – Venkovní bezpečnostní IR kamera barevná (obrázek č. 9), varifokal objektiv 2.8mm/105°~12mm/23°, 700TVř, dosvit IR 40~50m, 2 DNR, HLC, čip 1/3 SONY Super HAD II, OSD, 12V/200mA (600mA s IR)
  Prodejní cena: 3463 Kč bez DPH
  Počet: 5 (K1,K3, K4, K5, K6)

- Napájecí zdroj 12V/9A pro bezpečnostní kameru, pulsní, stabilizovaný DRST-10812-T3, 168 x 70 x 39 mm, 590 gramů, 3 vodičová přívodní šňůra
  Prodejní cena: 1351 Kč bez DPH
  Počet: 1

Obr. 37. Napájecí zdroj

Zdroj: [33]

- DVR 5008 ELN – REAL TIME – DVR rekordér pro 8 kamer + 4 Audio, 200 obr/sec/D1, rozměry: 430 x 65 x 390 mm, DC12V/4A (adaptér je součástí), 2x SATA HDD (není součástí), HDMI, VGA, LAN, H.264, VDM
  Prodejní cena: 7616 Kč bez DPH
  Počet: 1

Obr. 38. DVR rekordér

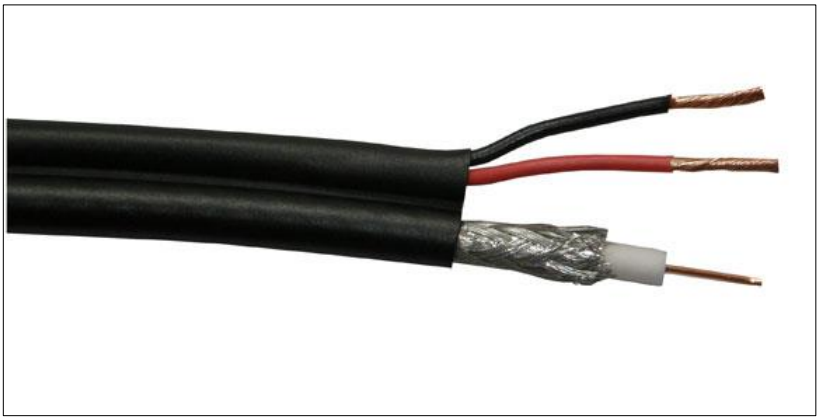
Zdroj: [33]

- Harddisk SATA 1 TB speciální pro digitální záznamové zařízení – DVR rekordér
  Prodejní cena: 2067 Kč bez DPH
  Počet: 1

Obr. 39. Harddisk

Zdroj: [33]

- Venkovní systémový kabel – koaxiální kabel RG59 (FeCu) + napájecí kabel 2 x 1.0 mm (Cu) – červený a černý, balení po 305 m
  Prodejní cena: 1247 Kč bez DPH
  Počet: 1 balení



Obr. 40. Venkovní systémový kabel

Zdroj: [33]

- Adaptér – standard DC 2.1/5.5 konektor napájení (pro CCTV kamery)
  Prodejní cena: 15 Kč bez DPH
  Počet: 7
- BNC konektor Platinum (kolík) – kompresní pro CAMSET/RG-59
  Prodejní cena: 30 Kč bez DPH
  Počet: 12
- Napájecí distributor LZ-8 (8 výstupů)
  Prodejní cena: 210 Kč bez DPH
  Počet: 1

7.3 EKV

Jedná se o systém umožňující organizovat přístup určitých skupin osob do určených prostor a v určených časech.

Rozmístění prvků

V daném návrhu (příloha P III) jsem použila:
- zóna 1 - chodba - detektor 1.1,
- zóna 2 - kanceláře - detektory 2.1, 2.2, 2.3, 2.4, 2.5,
- zóna 3 - dílna detektory - 3.1,3.2,
- zóna 4 - sklad detektory - 4.1, 4.2,4.3.

Soupis prvků

Tab. 14. Soupis prvků EKV [33]

Druh	Cena za jednotu v Kč bez DPH	Množství	Celková cena v Kč bez DPH
Bezdrátový magnetický detektor mini	1062	6	6372
Bezdrátový detektor pohybu osob a rozbití skla	1892	5	9460
Cena celkem			15832

Rozpis prvků:

- JA-151M Bezdrátový magnetický detektor mini – okamžitý poplach
  Prodejní cena: 1062 Kč bez DPH
  Počet: 6 (1.1,2.5,3.1, 3.2, 4.1, 4.2)

Obr. 41. Magnetický detektor

Zdroj: [33]

- JA-180PB Bezdrátový detektor pohybu osob a rozbití skla – okamžitý poplach
  Prodejní cena: 1892 Kč bez DPH
  Počet: 5 (2.1, 2.2, 2.3, 2.4,4.3)

Obr. 42. Bezdrátový detektor

Zdroj: [33]

7.4 EPS

EPS je instalována v prostorách průmyslových podniků s větší pravděpodobností vzniku požáru. Nutnost instalace EPS je v objektech řešena stavebně bezpečnostními předpisy. Není výjimkou požadavek uživatele na zřízení EPS i v případě, že podle výpočtů není instalace EPS nutná. Jedná se o předcházení škodám na výrobním zařízení.

Rozmístění prvků

U EPS jsem použila bezdrátový kombinovaný detektor kouře a teploty ve 2 ks (v kotelně a technické místnosti) a bezdrátový detektor úniku plynu (v kotelně).

V daném návrhu (příloha P II) bezdrátový kombinovaný detektor kouře a teploty P1 a P2 v kotelně a technické místnosti. V kotelně je použit také detektor úniku plynu P3.

Soupis prvků

Tab. 15. Soupis prvků EPS [33]

Druh	Cena za jednotu v Kč bez DPH	Množství	Celková cena v Kč bez DPH
Bezdrátový kombinovaný detektor kouře a teploty	1011	2	2022
Bezdrátový detektor úniku plynu	1316	1	1316
Cena celkem			3338

Rozpis prvků

- JA-150ST Bezdrátový kombinovaný detektor kouře a teploty
  Cena: 1011 Kč bez DPH
  Počet: 2 (P1, P2)

Obr. 43. Kombinovaný detektor

Zdroj: [33]

- JA-180G Bezdrátový detektor úniku plynu
  Cena: 1316 Kč bez DPH
  Počet: (P3)

Obr. 44. Detektor úniku plynu

Zdroj: [33]

ZÁVĚR

Tato diplomová práce je zpracována na téma Moderní metody využití integrovaných bezpečnostních systémů v ochraně průmyslových objektů. Problematika ochrany průmyslových objektů je aktuálním problémem. Potřeba chránit svůj majetek před poškozením nebo odcizením je v dnešní době nezbytná. Efektivní zabezpečení průmyslového objektu vychází z charakteru průmyslového objektu, jeho velikosti, lokalitě, očekáváním a přáním zákazníka a obecným rizikům, jimž objekt čelí.

V teoretické části jsou popsány všechny typy zabezpečení, které by se měly v praxi aplikovat společně a měly by se vzájemně doplňovat. Jedná se o metody současné ochrany průmyslových objektů. Dále možnosti integrované průmyslové ochrany PZTS, CCTV, EKV a EPS. Jejich výhody a nevýhody. Následuje budoucí vývoj DPPC. DPPC se neustále vyvíjí v rámci inteligentních budov, IP kamerových systémů a biometrické identifikace. Následuje technické řešení integrace jednotlivých prvků.

Cílem této diplomové práce je návrh zabezpečení průmyslového objektu. K zabezpečení jsem použila prvky PZTS, CCTV, EKV a EPS, které jsou již popsány v teoretické části této diplomové práce. Daný návrh jsem vypracovala ve spolupráci s firmou Link24 systems s.r.o., která se zabývá danou problematikou.

Návrh PZTS je technickým řešením ochrany vnitřních i vnějších prostor. Ve vnitřních prostorách jsou použity tyto prvky: ústředna, sběrnicový přístupový modul s displejem a ovládací segmenty přístupových modulů pro každou střeženou zónu. Do skladu budou nainstalována sekční vrata. Vnější prostory jsou chráněny bezpečnostním plotem. Příjezd k budově bude chráněn pomocí elektricky ovládané brány. Zaměstnancům bude sloužit branka s elektrickým zámkem. V případě narušení střeženého prostoru bude díky DPPC ihned kontaktováno nejbližší výjezdové vozidlo.

K monitorování průmyslového objektu jsem použila celkem 6 kamer. Venkovních kamer bude 5 k monitorování prostor vjezdu do areálu, parkoviště pro zákazníky, parkoviště pro firemní vozidla, vjezd do skladu a prostor za budovou. Vnitřní prostor bude monitorovat 1 kamera, která bude instalována naproti hlavním dveřím.

Při návrhu EKV v daném průmyslovém objektu rozlišila 4 ochranné zóny (1, 2, 3 a 4), kde jsem použila celkem 11 detektorů. Zóna 1 - chodba (1 detektor), zóna 2 - kanceláře (5 detektorů), zóna 3 - dílna (2 detektory) a zóna 4 - sklad (3 detektory).

U EPS jsem použila bezdrátový kombinovaný detektor kouře a teploty ve 2 ks (v kotelně a technické místnosti) a bezdrátový detektor úniku plynu (v kotelně).

Průmyslový objekt bude zabezpečen ve 2 bezpečnostní třídě. Na zabezpečení jsem použila výrobky firmy Jablotron, která nabízí široký sortiment kvalitních výrobků. Vzhledem k tomu, že se jedná o nově zrekonstruovaný průmyslový objekt a své sídlo v něm najde nově vzniklá firma navrhla jsem cenově přijatelné, ale účinné prvky, které mohou být v budoucnu doplněny dalšími prvky průmyslové ochrany.

ZÁVĚR V ANGLIČTINĚ

This master´s thesis is elaborated on the following topic - Modern methods of use of integrated security systems to protect industrial buildings. Issue of protection of the industrial buildings is current problem. Nowadays is very necessary to protect own property from damage or theft. Efficient security of the industrial building is based on a character of the industrial building, its size, location, expectations and customer wishes and a general risks to which the object is facing.

In the theoretical part there are described all types of security, that should be together applied in practice and they should be complementary together. These are methods of simultaneous protection of the industrial buildings. And the next are possibilities of integrated industrial PZTS, CCTV, EKV and EPS. Their advantages and disadvantages. Followed by the future development of DPPC. In intelligent buildings, IP closed circuit television and biometric identification, there is the DPPC constantly evolving. And the next is technical solutions for integration of elements.

The aim of this master´s thesis is proposal of security of the industrial buildings. I used for the security the PZTS, the CCTV, the EKV a the EPS elements, which are described in the theoretical part of this master´s thesis. I developed the proposal in cooperation with Link24 systems, s.r.o., which deals with this issue.

The PZTS proposal is a technical solution of internal and external space. In indoor spaces there are used these elements: central, access modul with display and control segments of access module for each guarded zone. Sectional door will be installed to warehouse. Exterior surfaces are protected by a security fence. Access to the building will be protected by electrically operated gates. Gate with an electric lock will serve an employees. Thanks to the DPPC, in case of disruption of the protected area, there will be immediately contacted the nearest exit vehicle.

For monitoring of the industrial objects I used 6 cameras. It will be used 5 exterior cameras for the monitoring of entrance area to the site, parking for customers, parking for company vehicles, entrance to the warehouse and the area behind the building. Interior space will be monitored by one camera, that will be installed in front of the main door.

During a designing the EKV in the industrial building I distinguished 4 protection zones (1, 2, 3 and 4), where I have used a total of 11 detectors. The zone 1 - a corridor (1

detector), the zone 2 - an offices (5 detectors), the zone 3 - a workroom (2 detectors), the zone 4 - a warehouse (3 detectors).

At the EPS I have used a 2 pieces of combined wireless smoke and temperature detector (in a boiler room and in a technical room) and wireless gas leak detector (in the boiler room).

The industrial building will be protected in the 2 safety class. At the security I have used products of Jablotron, which offers a wide range of quality products. In view of the fact, that this is a newly renovated industrial building and newly established company there finds its company address, I suggested affordable, but effective elements, that may be in the future, supplemented by the other elements of an industrial protection.

SEZNAM POUŽITÉ LITERATURY

[1] KINDL, Jiří. *Projektování bezpečnostních systémů I.* 2. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. 130 s. ISBN 978-80-7318-554-1.

[2] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I.* 3. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. 81 s. ISBN 978-80-7318-889-4.

[3] IVANKA, Ján. *Systemizace bezpečnostního průmyslu.* 4. rozšířené vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2011. 123 s. ISBN 978-80-7454-122-3.

[4] IVANKA, Ján. *Mechanické zábranné systémy.* 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. 151 s. ISBN 978-80-7318-910-5.

[5] ČESKÁ PŘEDBĚŽNÁ NORMA. *ČSN P EN 1627 Okna, dveře, uzávěry – Odolnost proti násilnému vniknutí : Požadavky a klasifikace.* Praha: Český normalizační institut, 2000.

[6] UHLÁŘ, Jan, 2005. *Technická ochrana objektů II. Díl – Elektrické zabezpečovací systémy II.* 1. vyd. Praha: Policejní akademie České republiky. ISBN 80-7251-189-0.

[7] PODNIKOVÁ NORMA. *Poplachové systémy – Pravidlo zřizování poplachových zabezpečovacích a tísňových systémů objektu (PZTS).* Jablotron: Září 2007, 20s.

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

[9] LUKÁŠ, Luděk a kolektiv. *Bezpečnostní technologie, systémy a management II*. 1. vyd. Zlín: VeRBuM, 2012. 387 s. ISBN 978-80-87500-19-4.

[10] LAUCKÝ, Vladimír a Rudolf DRGA. *Speciální technologie komerční bezpečnosti.* 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. 291 s. ISBN 978-80-7454-146--9.

[11] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II.* vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9.

[12] Česká Republika. ČSN CLC/TS 50398 : *Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky*. In Česká technická norma. 2009, 33 4597

[13] R.H.M. System [online]. 2013 [cit. 2013-03-17]. Dostupný z WWW: <http://www.rhmsystem.com/index.php?option=com_content&view=article&id=2&Itemid=4>.

[14] ASParking [online]. 2013 [cit. 2013-03-10]. Dostupný z WWW: <http://www.asparking.cz/download/katalog/turnikety.pdf>.

[15] FENIX INTERNATIONAL, spol. s.r.o. [online]. 2013 [cit. 2013-03-10]. Dostupný z WWW:<http://www.fenix-international.cz/cs/bezpecnostni-sluzby/fyzicka-ostraha-objektu>.

[16] TECHNICOM, s.r.o. [online]. 2013 [cit. 2013-04-07]. Dostupný z WWW: <http://www.technicom.cz/pzts.html>.

[17] SECURITY TECHNOLOGIES [online]. 2013 [cit. 2013-05-01]. Dostupný z WWW: <http://www.security.cz/cz/produkty/bezpecnostni-systemy.html>.

[18] VIAKOM CZ s.r.o. [online]. 2013 [cit. 2013-03-11]. Dostupný z WWW: <http://www.viakom.cz/kategorie/ekonomicke-kamery/>.

[19] PD CERKOM s.r.o. [online]. 2013 [cit. 2013-03-16]. Dostupný z WWW: <http://www.pdcerkom.cz/1.11-cctv-uzavrene-kamerove-systemy>.

[20] INTO CZ spol. s r.o.**[**online]. 2013 [cit. 2013-04-07]. Dostupný z WWW: <http://www.timelink.cz/snimace-otisku-prstu/>.

[21] Profi Elektrika.cz [online]. 2013 [cit. 2013-04-07]. Dostupný z WWW: <http://elektrika.cz/data/clanky/zszven021203>.

[22] PD CERKOM s.r.o. [online]. 2013 [cit. 2013-03-16]. Dostupný z WWW: <http://www.pdcerkom.cz/1.13-ekv-elektronicka-kontrola-vstupu>.

[23] PD CERKOM s.r.o. [online]. 2013 [cit. 2013-03-16]. Dostupný z WWW: <http://www.pdcerkom.cz/1.10-eps-elektricka-protipozarni-signalizace>.

[24] Loter [online]. 2013 [cit. 2013-03-25]. Dostupný z WWW: <http://www.loter.eu/pult-centralni-ochrany-pco/>.

[25] D.I.Seven, a.s. 2013 [cit. 2013-03-25]. Dostupný z WWW: <http://www.diseven.cz/sluzby/pco/>.

[26] Biometrie s.r.o. [online]. 2013 [cit. 2013-05-01]. Dostupný z WWW: <http://www.biometrie.cz/>.

[27] Odborný vědecký časopis Trilobit [online]. 2013 [cit. 2013-05-01]. Dostupný z WWW: <http://trilobit.fai.utb.cz/systemy-identifikace-vstupu-a-biometricke systemy_aed2ef89-1626-49ef-b9d3-1925b7fec789>.

[28] BIMA biometrics identity management agency [online]. 2013 [cit. 2013-05-01]. Dostupný z WWW: <http://www.biometrics.dod.mil/>.

[29] Inteligentní budovy [online]. 2013 [cit. 2013-05-04]. Dostupný z WWW:

<http://www.inteligentni-budovy.cz/>.

[30] Inteligentní budovy ve světě, Copyright TMI HoldingsSp. z o.o.[online]. 2013 [cit. 2013-05-04]. Dostupný z WWW:

<http://inbudovy.cz/artykul/article/co-je-inteligentni-budova-a-kam-kraci/>.

[31] Top info s.r.o. [online]. 2013 [cit. 2013-05-04]. Dostupný z WWW:

<http://tzb-info.cz>.

[32] Mapy Google [online]. 2013 [cit. 2013-05-12]. Dostupný z WWW: <http://maps.google.cz/>.

[33] JABLOTRON [online]. 2013 [cit. 2013-05-12]. Dostupný z WWW:

<http://www.jablotron.com/cz/katalog-produktu/>.

[34] Garážová vrata – vjezdové brány – zámečnictví – Czech Republic [online]. 2013 [cit. 2013-05-17]. Dostupný z WWW: < http://www.vrata-brany.eu/ >.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

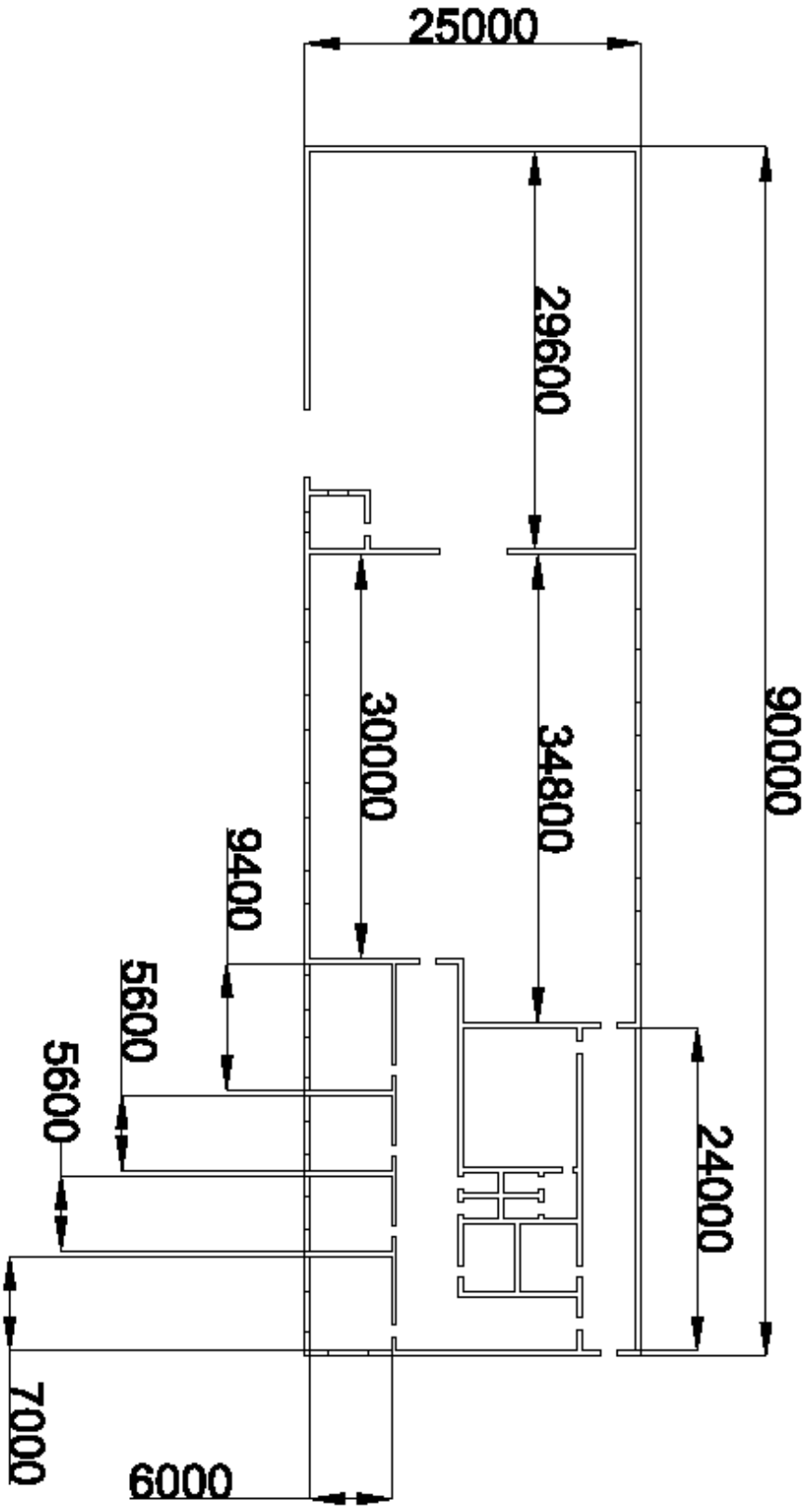
BIMA	Biometrická identifikační manažerská agentura
CCF	Centrální ovládací zařízení
CCTV	Uzavřený televizní a dohledový systém
ČR	Česká republika
ČSN	Česká státní norma
DPPC	Dohledové a poplachové přijímací centrum
DVR	Digitálního videorekordéru
EKV	Systém kontroly vstupů
EMC	Elektromagnetická kompatibilita
EN	Evropská norma
EPS	Elektrická požární signalizace
EU	Evropská unie
HZS	Hasičský záchranný sbor
IB	Inteligentní budovy
ICT	Informačních a komunikačních technologií
IPS	Integrovaný poplachový systém
IR	Infračervené
KTPO	Klíčový trezor požární ochrany
MZS	Mechanické zábranné systémy
NVR	Network video recorder
OPPO	Obslužné pole požární ochrany
PO	Požární ochrana
PZTS	Poplachový zabezpečovací a tísňový systém
VMS	Video Management Software
ZDP	Zařízení dálkového přenosu

SEZNAM OBRÁZKŮ

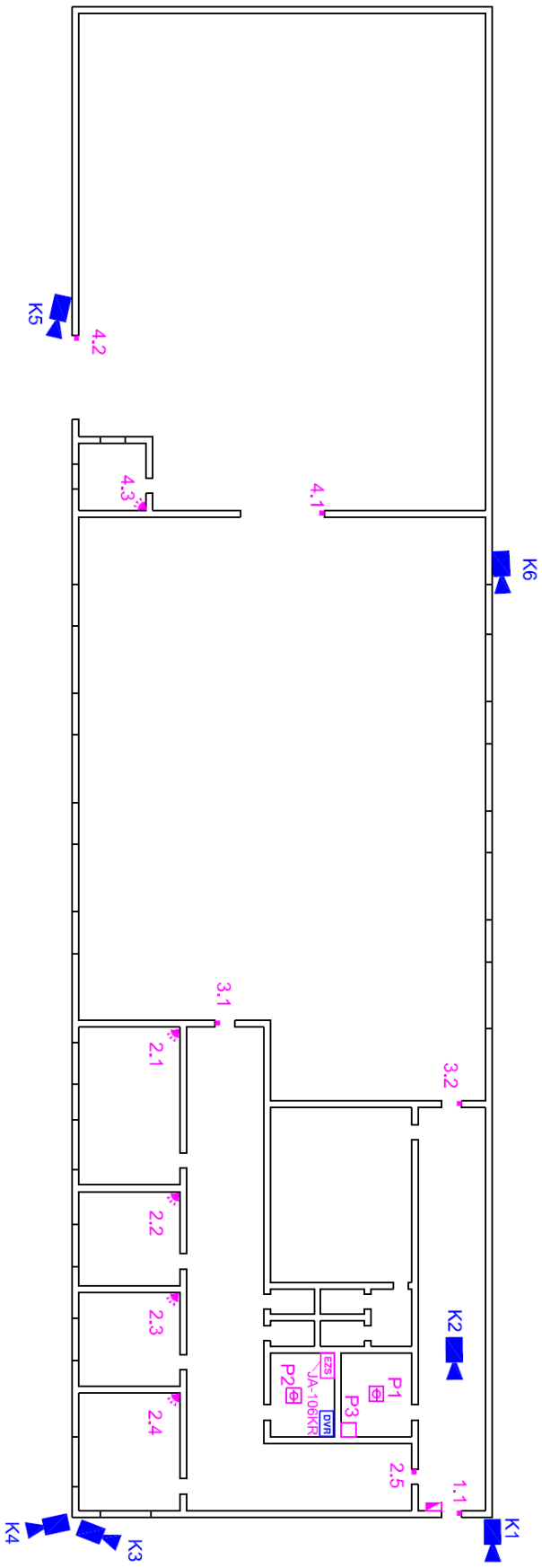
SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ROZMĚRY BUDOVY



PŘÍLOHA P II: NÁVRH V AUTOCADU – ROZMÍSTĚNÍ PRVKŮ



PŘÍLOHA P III: NÁVRH V AUTOCADU - ZÓNY