

Návrh integrovaného systému kontroly vstupů

Design of Integrated Access Control System

Bc. Radek Pavlínek

Diplomová práce
2014



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Radek Pavlínek**
Osobní číslo: **A12324**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **prezenční**

Téma práce: **Návrh integrovaného systému kontroly vstupů**
Téma anglicky: **A Proposal for an Integrated Access Control System**

Zásady pro vypracování:

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

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. VALOUCH, Jan. Projektování bezpečnostních systémů. [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5. 152 s.
2. VALOUCH, Jan. Projektování integrovaných systémů. [skriptum]. Zlín: UTB, 2013. ISBN 978-80-7454-296-1 152 s.
3. LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management. 1. vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.
4. LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012. 387 s. ISBN 978-80-87500-19-4.
5. LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management III. 1. vyd. Zlín: VeRBuM, 2013. 456 s. ISBN 978-80-87500-35-4.
6. LOVEČEK, Tomáš. REITŠPÍS, Josef. Projektovanie a hodnotenie systémov ochrany objektov. Žilina: EDIS – vydavateľstvo ŽU, 2011. 281 s. ISBN 978-80-554-0457-8.
7. ČSN EN 50133-7 Poplachové systémy– Systémy kontroly vstupů pro použití v bezpečnostních aplikacích– Část 7: Pokyny pro aplikace. Praha: Český normalizační institut, 2000. 16 s. Třídící znak 334593.

Vedoucí diplomové práce:

Ing. Jan Valouch, Ph.D.

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

7. února 2014

Termín odevzdání diplomové práce:

27. května 2014

Ve Zlíně dne 7. února 2014


prof. Ing. Vladimír Vašek, CSc.
děkan




doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Téma diplomové práce zahrnuje problematiku integrace systémů kontroly vstupů. Úvodní část představuje vymezení pojmů z oblasti integrovaných poplachových systémů. Následuje analýza technických požadavků na integrované systémy a integraci systémů kontroly vstupu v bezpečnostních aplikacích. Součástí práce je rovněž analýza technických způsobů řešení integrace systémů kontroly vstupů s poplachovými a nepoplachovými aplikacemi. Stěžejní část práce představuje návrh integrace systému kontroly vstupů pro modelový objekt komerčního typu. Uvedené informace jsou doplněny přehledem vývojových trendů v dané oblasti.

Klíčová slova: integrovaný poplachový systém, systém kontroly vstupů, integrace, poplachové systémy, nepoplachové aplikace.

ABSTRACT

The topic of the thesis is about the issues in the integration of access control systems. The introductory presents the demarcation of definitions of integrated alarm systems. Next, the thesis discusses the analysis of technical conditions for integrated systems and integrated access control systems in applications of safety. The thesis also contains an analysis of technical options that solve the integration of access control systems with alarm and non-alarm applications. The main part of the thesis introduces us to a draft of integrated access control systems in a model commercial building. The following information is supplemented by an overview of developing trends in the given area discussed.

Keywords: integrated alarm system, access control system, integration, alarm systems, non-alarm applications.

Poděkování

Děkuji tímto svému vedoucímu Ing. Janu Valouchovi, Ph.D. za odborné vedení, podnětné rady, informace a připomínky, které mi poskytoval během zpracovávání diplomové práce. Dále chci poděkovat svým rodičům a blízkým za podporu, které se mi dostávalo během mého studia.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD.....	10
I TEORETICKÁ ČÁST.....	11
1 INTEGROVANÉ POPLACHOVÉ SYSTÉMY	12
1.1 POPLACHOVÉ APLIKACE	13
1.2 NEPOPLACHOVÉ APLIKACE.....	15
1.3 VÝHODY INTEGROVANÉHO POPLACHOVÉHO SYSTÉMU.....	16
1.3.1 Výhody z pohledu bezpečnosti	16
1.3.2 Výhody z hlediska úspory nákladů na zařízení.....	17
1.3.3 Výhody z hlediska zvýšení komfortu.....	17
1.4 NEVÝHODY INTEGROVANÉHO POPLACHOVÉHO SYSTÉMU	18
1.5 ZPŮSOBY INTEGRACE	19
1.5.1 Softwarová integrace.....	20
1.5.2 Hardwarová integrace	23
2 TECHNICKÉ POŽADAVKY NA INTEGROVANÉ POPLACHOVÉ SYSTÉMY.....	27
2.1 KONFIGURACE INTEGROVANÝCH POPLACHOVÝCH SYSTÉMŮ	27
2.1.1 TYP 1	27
2.1.2 TYP 2	28
2.2 PŘEHLED TECHNICKÝCH POŽADAVKŮ NA INTEGROVANÉ POPLACHOVÉ SYSTÉMY	29
2.2.1 Požadavky na společné ovládací zařízení	29
2.2.2 Požadavky na signalizační zařízení.....	29
2.2.3 Požadavky na centrální ovládací zařízení	30
2.2.3.1 Požadavky na záložní napájení centrálního zařízení	31
2.2.4 Požadavky na montáž a propojení jednotlivých aplikací.....	31
2.2.5 Požadavky na napájecí zdroje	32
2.2.6 Provozní kniha	32
3 TECHNICKÉ POŽADAVKY NA PŘÍSTUPOVÉ SYSTÉMY.....	33
3.1 ANALÝZA TECHNICKÝCH POŽADAVKŮ NA PŘÍSTUPOVÉ SYSTÉMY	34
3.1.1 Společné technické požadavky pro třídy přístupu A a B	35
3.1.1.1 Požadavky na hlášení.....	35
3.1.1.2 Požadavky na ovládání přístupových míst.....	35
3.1.1.3 Požadavky na napájení.....	36
3.1.2 Doplnkové technické požadavky pro třídu přístupu B.....	36
3.1.2.1 Požadavky na hlášení.....	36
3.1.3 Technické požadavky na komponenty přístupových systémů	37
3.1.3.1 Požadavky na vlivy prostředí.....	37
3.1.3.2 Požadavky na elektromagnetickou kompatibilitu.....	37
3.1.3.3 Požadavky na kabeláž	37
3.1.3.4 Požadavky na kryty zařízení	38
3.1.3.5 Požadavky na napájecí zdroje.....	39
3.1.3.6 Požadavky na identifikaci a značení	39
II PRAKTICKÁ ČÁST	41
4 INTEGRACE PŘÍSTUPOVÉHO SYSTÉMU S DALŠÍMI APLIKACEMI	42

4.1	INTEGRACE PŘÍSTUPOVÉHO SYSTÉMU S POPLACHOVÝMI APLIKACEMI.....	43
4.1.1	Integrace přístupového systému s poplachovými zabezpečovacími a tísňovými systémy.....	44
4.1.1.1	Integrace přístupového systému se zamlžovacími systémy.....	47
4.1.2	Integrace přístupového systému s elektrickou požární signalizací	48
4.1.3	Integrace přístupového systému s uzavřeným kamerovým systémem.....	51
	Aktivace přístupového systému na základě rozpoznání tváře.....	53
4.1.4	Integrace přístupového systému se systémem přivolání pomoci	55
4.2	INTEGRACE PŘÍSTUPOVÉHO SYSTÉMU S NEPOPLACHOVÝMI APLIKACEMI	56
4.2.1	Integrace přístupového systému s docházkovým systémem	56
4.2.2	Integrace přístupového systému s výtahy	59
4.2.3	Integrace přístupového systému s prvky domácí automatizace	59
5	NÁVRH INTEGRACE PŘÍSTUPOVÉHO SYSTÉMU	64
5.1	BEZPEČNOSTNÍ POSOUZENÍ OBJEKTU	64
5.1.1	Popis objektu	64
5.1.2	Analýza rizik	66
5.1.2.1	Zabezpečované hodnoty	66
5.1.2.2	Budova	68
5.1.3	Ostatní vlivy	70
5.1.3.1	Vlivy působící na zabezpečovací systém a mající původ uvnitř střeženého objektu	70
5.1.3.2	Vlivy působící na zabezpečovací systém a mající původ vně střežených objektů	71
5.2	NÁVRH SKLADBY INTEGROVANÉHO SYSTÉMU KONTROLY VSTUPŮ	72
5.2.1	Údaje o klientovi a střežených objektech.....	72
5.2.2	Stanovení stupně zabezpečení	73
5.2.3	Stanovení třídy prostředí	73
5.2.4	Půdorysy objektu a popis místností.....	74
5.2.5	Přehled zařízení	76
5.2.6	Konfigurace systému.....	89
5.2.7	Cenová kalkulace	94
5.2.8	Rozmístění komponentů.....	95
5.2.9	Hlášení poplachu	96
5.2.10	Legislativa, normy a další předpisy	96
5.2.11	Zásah, údržba a opravy	97
6	NOVÉ TRENDY V OBLASTI PŘÍSTUPOVÝCH SYSTÉMŮ.....	99
6.1	SPRÁVA PŘÍSTUPOVÝCH SYSTÉMŮ POMOCÍ NÁSTAVBOVÝCH SOFTWARE	99
6.2	VZDÁLENÉ OVLÁDÁNÍ PŘÍSTUPOVÝCH SYSTÉMŮ POMOCÍ MOBILNÍCH APLIKACÍ	100
6.3	PŘÍSTUPOVÝ SYSTÉM S TECHNOLOGIÍ NFC	101
6.4	ZVÝŠENÍ BEZPEČNOSTI PŘÍSTUPOVÝCH TERMINÁLŮ.....	102
6.5	INTEGROVANÝ PŘÍSTUPOVÝ SYSTÉM S KAMEROVÝM SYSTÉMEM	103
6.6	BEZDRÁTOVÁ KOMUNIKACE PRVKŮ PŘÍSTUPOVÉHO SYSTÉMU.....	103
6.7	NĚKOLIKANÁSOBNÁ VERIFIKACE OSOB	104
	ZÁVĚR	106
	ZÁVĚR V ANGLIČTINĚ.....	108

SEZNAM POUŽITÉ LITERATURY.....	110
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	113
SEZNAM OBRÁZKŮ	115
SEZNAM TABULEK.....	118
SEZNAM PŘÍLOH.....	119
PŘÍLOHA P I: CERTIFIKÁT VAR-NET INTEGRAL SPOLEČNOSTI VARIANT PLUS, S.R.O.....	119

ÚVOD

V současnosti se stále zvětšují komerční a průmyslové objekty a jejich rozloha a počty zaměstnanců se zvyšují. Současně stále narůstají bezpečnostní požadavky a pro zajištění bezpečnosti, zdraví a života osob a zajištění ochrany aktiv je nutné instalovat poplachové aplikace (poplachové zabezpečovací a tísňové systémy, kamerové systémy či přístupové systémy). Bohužel v mnoha rozsáhlých objektech není možné zajistit jedním systémem celý areál a je nutné použití několika poplachových či nepoplachových aplikací a současně definovat jejich vzájemné vazby a tím vytvořit integrovaný systém. Požadavky klientů zejména na zvýšení bezpečnosti a komfortu či snížení nákladů rostou a je nutné zajištění jednotného ovládání pro celý systém, což přineslo značné zvýšení celkové bezpečnosti, snadnější monitorování i správu objektu, komfortu při užívání a značnou úsporu financí.

Přístupové systémy či systémy kontroly vstupů jsou synonymy a představují soubory technických řešení sloužící k řízení a evidenci přístupu do chráněného objektu na základě přístupových práv, které jsou jednoznačně přiděleny povolané osobě. K integraci přístupových systémů s ostatními poplachovými i nepoplachovými aplikacemi dochází častěji v novějších sofistikovaných objektech, kde je nutné zajistit kontrolu přístupu do objektů a správu databáze a současně ovládat na základě definovaných akčních a reakčních událostí jiné poplachové nebo nepoplachové aplikace.

Nejčastějšími možnostmi integrace přístupového systému je propojení s docházkovým a stravovacím systémem, ale možností integrace je velmi mnoho. Například integrace s kamerovými systémy (CCTV), kdy dochází k poskytnutí doplňkové informace z kamerového systému od každého přístupového bodu. Dalšími možnostmi je integrace s poplachovým zabezpečovacím systémem nebo elektrickou požární signalizací. Z nepoplachových aplikací je to integrace s měřicími a regulačními či IT systémy.

Integrace systémů může přinášet i problémy projevující se nejčastěji nekompatibilitou zařízení či snižováním spolehlivosti způsobené zejména použitím prvků od různých výrobců.

Předpokládaným přínosem diplomové práce je zhodnocení technických požadavků na integrované poplachové systémy a systémy kontroly vstupu a následným návrhem pro konkrétní objekt komerčního typu a definování vývojových trendů v oblasti integrace systémů kontroly vstupu.

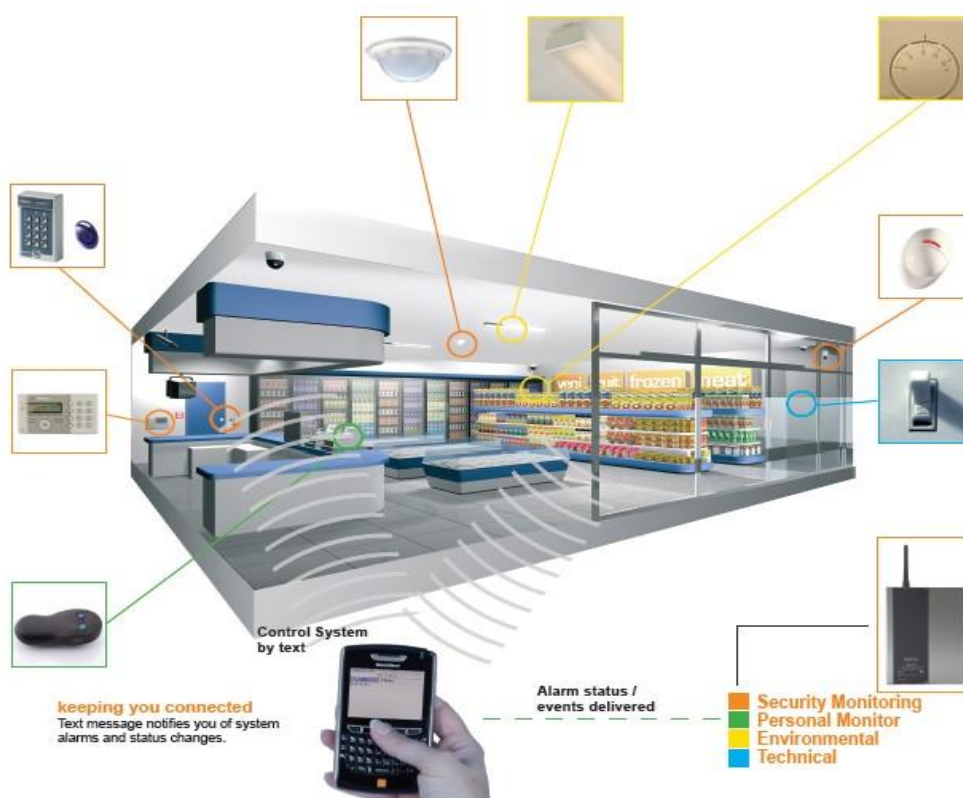
I. TEORETICKÁ ČÁST

1 INTEGROVANÉ POPLACHOVÉ SYSTÉMY

Integrovaný poplachový systém (IPS) je definován jako systém složený z jednoho nebo více společných zařízení a alespoň jedno z nich tvoří poplachová aplikace. Poplachové aplikace představují zejména: poplachové zabezpečovací a tísňové systémy (I&HAS), elektrická požární signalizace (EPS), systémy přivolání pomoci (SAS), systémy kontroly vstupu (ACS), a kamerové systémy (CCTV). Kombinace jednotlivých poplachových aplikací vede ke zvýšení bezpečnosti systému. S rostoucími požadavky zákazníků je v současnosti velmi rozšířené slučovat poplachové aplikace s nepoplachovými aplikacemi. Integrace s nepoplachovými aplikacemi zvyšuje zejména komfort ovládání systému.[1]

Složení integrovaného poplachového systému je vždy závislé na konkrétním typu objektu, zda se jedná o komerční, rezidenční či průmyslový objekt. V praxi není možné vytvořit šablonu použitelnou pro daný typ objektu z důvodu odlišnosti konkrétních požadavků klientů. Z hlediska legislativních požadavků nepatří mezi integrované poplachové systémy:

- *přenosové systémy,*
- *jednoúčelové systémy připojení přes jednosměrné výstupy ostatních zařízení bez přenosu dat.*



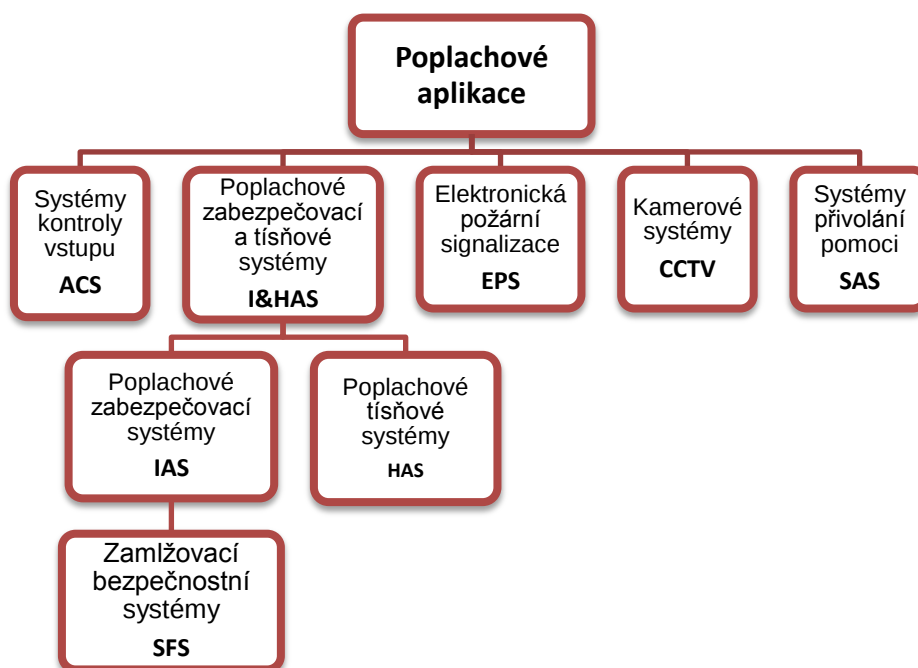
Obr. 1. Integrovaný poplachový systém [2]

Dále se mnohdy zaměřují pojmy kombinované poplachové systémy a integrované poplachové systémy. Z pohledu technické normy ČSN CLC/TS 50398 *Poplachové systémy- Kombinované a integrované systémy* nerozlišuje mezi těmito výrazy rozdíl. Avšak z technického hlediska jsou:

- **kombinované systémy** – souhrn poplachových a nepoplachových systémů, které mezi sebou nemají vzájemné vazby a vzájemně se neovlivňují,
- **integrované systémy** – souhrn poplachových a nepoplachových systémů, mezi nimiž jsou definovány vzájemné vazby a vzájemně se ovlivňují.

1.1 Poplachové aplikace

Poplachová aplikace je zařízení sloužící primárně pro ochranu života, majetku a prostředí. Typickým příkladem je detekce pohybu v objektu nebo detekce vniknutí do střeženého objektu. Na následujícím obrázku jsou znázorněny typické příklady poplachových aplikací.



Obr. 2. Poplachové aplikace

a) Poplachové zabezpečovací a tísňové systémy (I&HAS)

Poplachové zabezpečovací a tísňové systémy jsou definovány jako soubory kombinovaných systémů skládající se z:

- **poplachových zabezpečovacích systémů (IAS)**,
jejíž hlavní funkce je detekce a indikace vniknutí do objektu detektorem narušení (narušení střeženého prostoru),

- **poplachových tísňových systémů (HAS),**

funkce poplachových tísňových systémů je založena na možnosti člověka úmyslně vyvolat poplachový stav.

K poplachovým zabezpečovacím a tísňovým systémům patří i poplachový přenosový systém sloužící pro přenos informací mezi jednotlivými poplachovými systémy nebo mezi jednotlivými poplachovými přijímacími centry.

b) Elektrická požární signalizace (EPS)

Pro včasnou signalizaci požáru se využívají požárně bezpečnostní zařízení nazývané elektronická požární signalizace. První příznaky požáru jsou detekovány hlásiči požáru předávající signál ústředně EPS. Zajištění obsluhy ústředny EPS může být realizováno pomocí stálé obsluhy, která v případě požáru přivolá jednotku požární ochrany nebo v případě nepřítomnosti stálé obsluhy je přivolána jednotka požární ochrany přes zařízení dálkového přenosu.

c) Systém kontroly vstupu (ACS)

Systém kontroly vstupu nebo přístupový systém představují stejná zařízení a jsou v podstatě synonyma. Systém kontroly vstupu je definován jako: „*Soubor opatření k zajištění řízení a evidence přístupu do zabezpečeného objektu nebo prostoru na základě jednoznačně přidělených přístupových práv*“.[3] Realizace těchto prostředků může být představována:

- elektronickými prostředky (snímač místa přístupu, jednotky řízení vstupu aj.),
- mechanickými prostředky (turnikety, zámky, mříže, závory aj.),
- systémovými opatřeními (oprávnění ke vstupu, časový harmonogram aj.),
- fyzickou ochranou (fyzická přítomnost osoby kontrolující vstup do objektu).

d) Kamerové systémy (CCTV)

Základním prvkem kamerových systémů jsou kamerové zařízení sloužící ke snímání střeženého prostoru. Přenos videosekvence je zajištěn pomocí přenosových zařízení a následně prostřednictvím zobrazovacích zařízení je videosekvence zobrazena operátorovi na poplachovém přijímacím centru. Ukládání a následné zpracování videosekvence je zajištěno pomocí záznamových zařízení.

e) Systémy přivolání pomoci (SAS)

Systém přivolání pomoci slouží pro automatické nebo manuální přivolání pomoci prostřednictvím speciálních prostředků. Určen pro osoby s vysokou pravděpodobností zdravotních potíží, zejména seniory nebo zdravotně postižené osoby.

f) Zamlžovací systémy (SFS)

Zamlžovací systém tvoří generátor husté mlhy, který je aktivován zabezpečovacím systémem při vyhlášení poplachu, například detektorem rozbití skla nebo PIR detektorem. Využívá se pro prostory s uloženými cennými aktivy a slouží pro snížení viditelnosti a dezorientaci pachatele.[4] Zamlžovací systémy patří do kategorie poplachových zabezpečovacích systémů.

1.2 Nepoplachové aplikace

Nepoplachové aplikace jsou zařízení, jejichž primární funkce není ochrana života, majetku a prostředí a při integraci s poplachovými aplikacemi mohou sloužit ke zvýšení efektivity využití energie a zvýšení komfortu ovládání. Představují je většinou procesy ovládání a řízení:

- osvětlení,
- vytápění,
- klimatizace,
- zavlažování,
- výtahů,
- odvětrávání,
- energetických systémů,
- spouštění jiných zařízení.



Obr. 3. Nepoplachové aplikace

1.3 Výhody integrovaného poplachového systému

V současnosti se stále rostoucími požadavky zákazníků jsou kladeny vysoké nároky systémů zejména na **zabezpečení, zvýšení komfortu ovládání a úsporu nákladů na zařízení** v celém systému. Požadavky se samozřejmě rapidně mění v závislosti na typu objektu, zda se jedná o rezidenční, komerční (průmyslové) nebo městské (obecní) objekty.

Požadavky klientů na IPS



Obr. 4. Nejčastější požadavky klientů

Požadavky klientů se liší a kladou důraz na jinou složku, ale na prvním místě by měla vždy být preferována bezpečnost osob, majetku a životního prostředí a následně řešit ekonomické hledisko a komfort ovládání. Proto se nabízí řada možností integrací poplachových systémů s jinými poplachovými nebo nepoplachovými aplikacemi.

1.3.1 Výhody z pohledu bezpečnosti

Hlavní výhodou při integraci poplachových systémů s jinými poplachovými systémy je zvýšení kvality vyhodnocení signálů či stavů jednotlivých poplachových aplikací. Při použití přístupového systému s kamerovým systémem, může sloužit kamerový systém jako verifikační prvek rozhodující, zda se jedná o správně identifikovanou osobu. Toto řešení může sloužit jako prostředek pro získání předpoplachové informace o nestandardním chování v monitorovaném objektu.[1]

V rozsáhlých objektech při instalaci více vzájemně propojených přístupových systémů je možnost získávat centrálně informace o jednotlivých osobách a o bezpečnostní situaci v objektu a zvýšit kontrolu pohybu osob, vozidel nebo materiálu. Moderní zabezpečovací systémy umožňují integrovat širokou škálu automatizačních systémů.

1.3.2 Výhody z hlediska úspory nákladů na zařízení

Se stále zvyšujícími se cenami energií rostou i požadavky uživatelů na jejich úsporu. Úsporné řešení se snaží optimalizovat stav systému, při kterém dochází ke snížení spotřeby energií při maximální efektivitě požadovaného stavu. Takového stavu je možno dosáhnout například naprogramováním ústředny poplachového zabezpečovacího systému tak, aby při podmínkách zastřežení a nepřítomnosti osob v objektu vyslala požadavek na snížení výkonu plynového topného systému a vypnutí vybraných světel v objektu. V systému se to projeví snížením spotřeby plynové kotle a současně snížením spotřeby elektrické energie. Za předpokladu aplikace takového systému na rozsáhlé firemní areály, může takový typ integrace projevit rapidním snížením nákladů firmy na dodávku energií.

Při instalaci integrovaných systémů jako celku v rámci jednoho projektu dochází k rychlejšímu, přehlednějšímu a méně finančně náročnému postupu než s postupnou aplikací jednotlivých systémů. Postupně vytvářený integrovaný systém, realizovaný různými firmami specializujícími se pouze na jedno odvětví a neznalostí ostatních částí systému často vede k nedokonalostem řešení projevující se chybami v provozu. Následný servis spotřebuje mnoho finančních prostředků. Z tohoto důvodu je vhodné pověřit návrhem projektu prověřeného systémového integrátora.

Další aspekt v rámci úspory finančních prostředků na pořizování integrovaných systémů je možnost integrace jednotlivých subsystémů od různých výrobců lišících se v cenách a tím ušetřit další finanční zdroje.

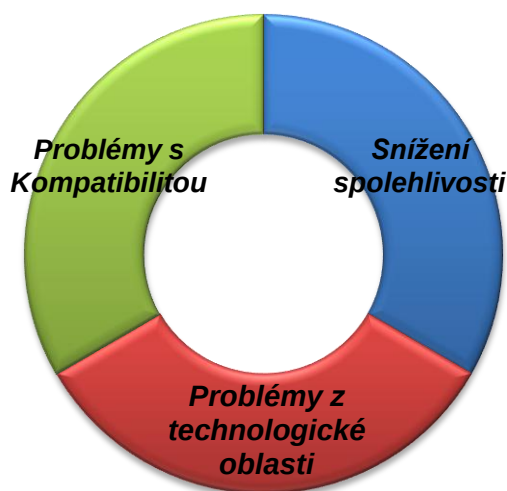
1.3.3 Výhody z hlediska zvýšení komfortu

Komfort lze definovat jako vnímání pohody a pohodlí vyjadřující velký dostatek až nadbytek určité lidské potřeby [5]. V rámci IPS lze za komfortní považovat bezobslužné integrované systémy pracující dle předem definovaných pravidel (naprogramovaných činností). Další aspekt zvyšující komfort je využití centralizované obsluhy s jednotným uživatelským prostředím pro všechny prvky integrovaného systému. Při integraci systému krizového řízení se zvyšuje možnost efektivního řízení krizových situací. Použitím široké škály aplikací dochází k širokému rozsahu využitelných funkcí, zvyšuje se flexibilita a univerzálnost integrovaného systému. Při účinném řízení nepoplachových aplikací umožňuje i získávat informace o nežádoucích změnách fyzikálních veličin bez nutnosti přítomnosti kontrolující osoby, což je další aspekt navyšující komfort. Integrací

poplachového zabezpečovacího systému s přístupovým systémem je zvyšována účinnost řízení přístupu osob do jednotlivých částí objektu a není nutná přítomnost fyzické ochrany.

1.4 Nevýhody integrovaného poplachového systému

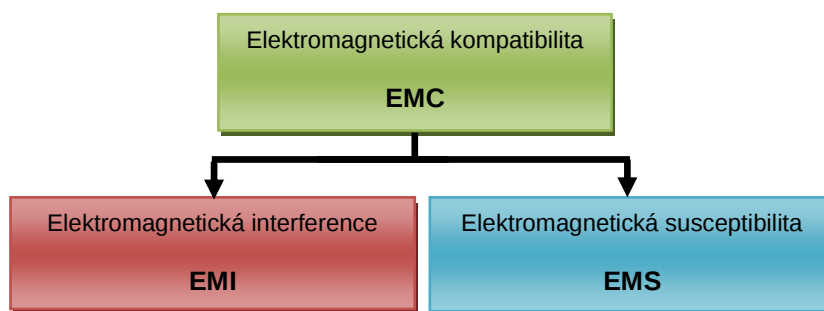
Kombinované poplachové systémy nejsou na rozdíl od integrovaných poplachových systému vázány vzájemnými vztahy, a tedy nedisponují jejich nevýhodami, u kterých se mohou projevit negativní projevy zejména s kompatibilitou, spolehlivostí systému a v oblasti technologií.



Obr. 5. Nevýhody IPS

V rámci integrace jednotlivých poplachových a nepoplachových aplikací od různých výrobců často dochází ke vzájemné nekompatibilitě rozhraní, komunikačních protokolů a dalších částí potřebných pro vzájemnou komunikaci. Je tedy nutné v rámci návrhu projektu, aby projektant znal technické specifikace výrobků.

S kompatibilitou zařízení souvisí i elektromagnetická kompatibilita (EMC), která se zabývá vzájemným ovlivňováním zařízení elektromagnetickým zářením. Ideálním stavem a nutností pro výrobce je zajištění, aby elektrické zařízení nerušilo svou funkcí jiné zařízení (elektromagnetická interferencí - EMI) a současně dokázalo pracovat v zarušeném prostředí bez snížení provozuschopnosti (elektromagnetická susceptibilita - EMS). Nekompatibilita zařízení se projevuje vzájemným negativním ovlivňováním jednotlivých aplikací a může docházet ke snižování provozuschopnosti celého systému. Tyto negativní důsledky se často projevují náhodně (například při současné funkci mnoho aktivních prvků nebo při zhoršených povětrnostních podmínkách aj.) a mohou vést ke snížení spolehlivosti systému.



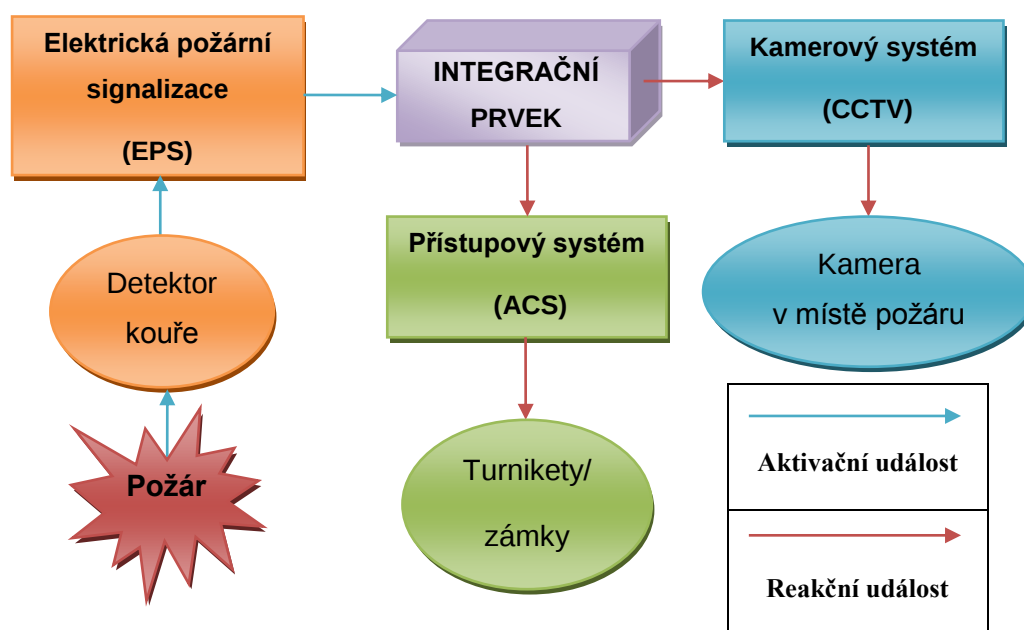
Obr. 6. Schematické znázornění elektromagnetické kompatibility

Aplikací rozsáhlých komplikovaných integrovaných systémů dochází k náročnějšímu technickému zabezpečení elektromagnetické kompatibility a roste složitost systému. Současně rostou pořizovací náklady, nároky na montáž a projektovou činnost. Při softwarovém řešení integrovaného poplachového systému řízeného jedním centrálním prvkem může dojít k jeho selhání a tím dojde k výpadku celého systému. Je tedy vhodné zajistit redundanci nejdůležitějších zařízení a spojů a tím zajistit zálohu systému. Řízení a kontrolu odběru energií je často složité zajistit z důvodu nejednotného připojení každé aplikace. Problémem je i případná úspora energií. [1]

1.5 Způsoby integrace

V rámci návrhu integrovaných poplachových systémů je možnost realizace softwarového nebo hardwarového typu integrace. U softwarového řešení jde v podstatě o vzájemné propojování systémů pomocí nastavbových programů na základě definovaných pravidel. Hardwarové řešení propojuje jednotlivé systémy pomocí výstupů a vstupů a přídatných rozšiřujících modulů. V praxi je častější použití kombinace softwarového a hardwarového typu integrace. První aspekt při návrhu integrovaných systémů je analýza systémů, které budou integrovány a definice jejich vzájemných vztahů. Tedy je nutno definovat co se má provést (reakční událost), když se něco stane (aktivační událost). [1]

Tyto vztahy je možno demonstrovat na systému kontroly vstupu integrovaným s elektrickou požární signalizací. Při vzniku požáru dojde k aktivaci detektoru kouře (aktivační událost), který může předat signál systému kontroly vstupu, který vydá povel k automatickému otevření všech zámků a turniketů v objektu (reakční událost č.1) a aktivaci kamerového systému v místě vzniku požáru (reakční událost č.2) (viz. Obr. 7).



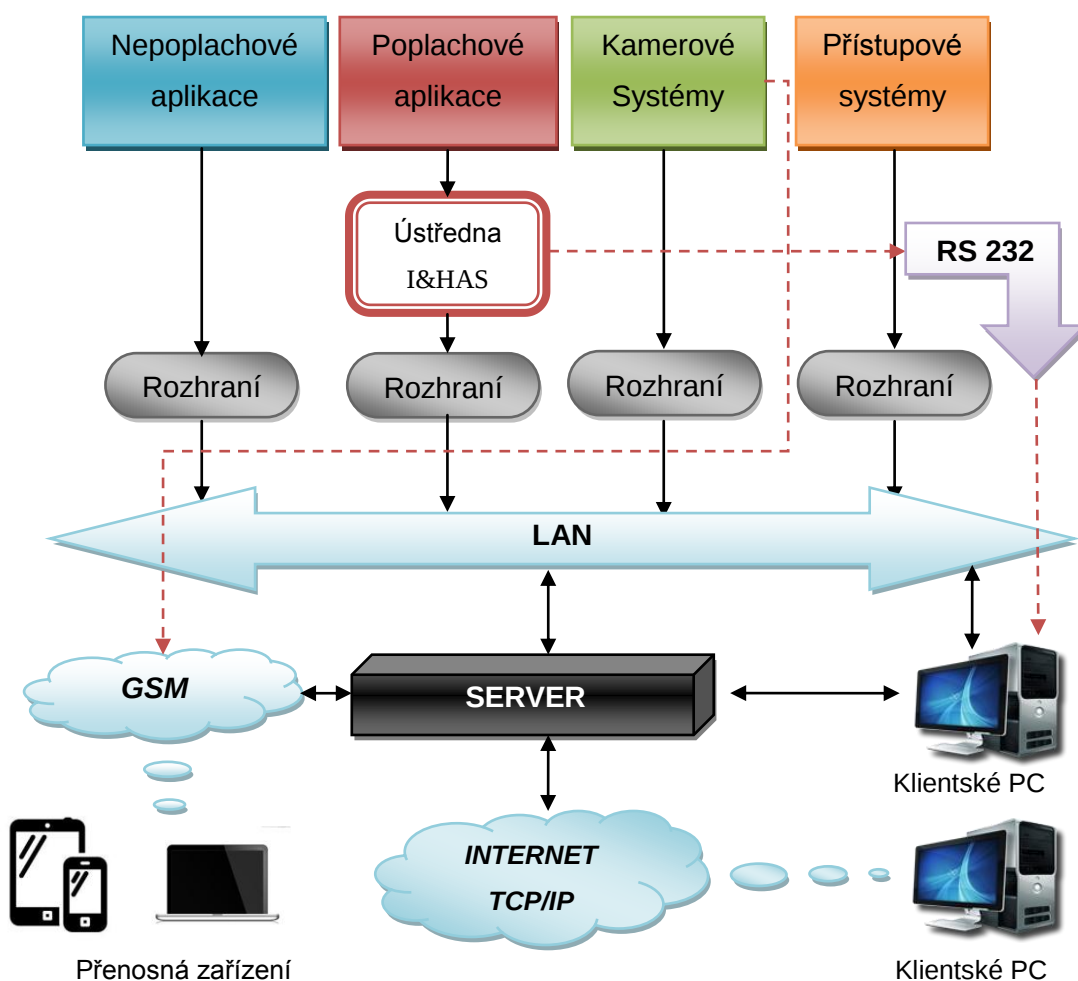
Obr. 7. Schéma aktivačních a reakčních událostí

1.5.1 Softwarová integrace

Princip softwarové integrace je založen na propojování jednotlivých poplachových a nepoplachových aplikací pomocí rozhraní do centrální řídicí jednotky. Centrální jednotky nejčastěji představují počítače nebo autonomní bezobslužné řídicí centrály vybavené speciálním nastavbovým softwarem, umožňující definovat vzájemné vazby a součinnosti jednotlivých aplikací.

V současnosti se jednotlivé aplikace připojují k lokální síti a přes ni následně k řídicí jednotce (serveru) a poté buď přímo nebo pomocí internetu či mobilní sítě ke klientským počítačům. U integrovaných systémů menšího rozsahu se realizuje připojení jednotlivých aplikací pomocí rozhraní RS232 nebo USB přímo ke klientskému počítači.

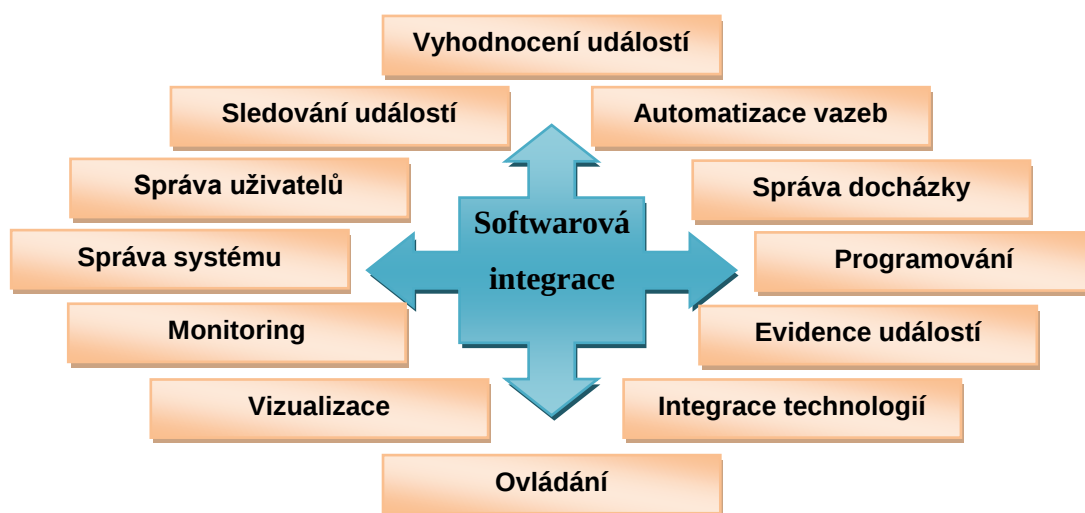
U kamerových systémů může být přenos realizovaný přes rozhraní prostřednictvím LAN sítě na řídicí server nebo v případě GSM kamery vybavené SIM kartou mohou být přenášeny signály a data přímo na server prostřednictvím GSM sítě. Další možností je připojení ústředny poplachového zabezpečovacího a tísňového systému přes rozhraní RS232 přímo ke klientskému PC.[1]



Obr. 8. Modelové schéma softwarové integrace

Trendem současných integrovaných systémů je zajištění přístupu a ovládání systému pomocí přenosných zařízení (notebooků, mobilních zařízení či tabletů) u kterých je nutná instalace podpůrného softwaru či aplikací. U těchto zařízení je vzájemná komunikace s integrovaným systémem zajištěna prostřednictvím internetu a to buď technologií bezdrátové sítě (WIFI) nebo mobilního datového přenosu (GPRS, EDGE, 3G, LTE). Ovšem pro rozsáhlé nebo kamerové systémy, kde dochází k obousměrné komunikaci a velké výměně dat (vysoký datový tok) je nutné zvolit rychlé datové přenosy 3G nebo LTE. Ve městech a příměstských oblastech je 3G připojení standardem, ale problém s dostupností může nastat v odlehlých místech. Ovládání integrovaného systému lze realizovat i pomocí klasického textového přenosu SMS.

Se softwarovou integrací souvisí i softwarové produkty tříděné podle použití v praxi a slouží pro snadnou orientaci v instalačních softwarech. Přehled funkcí, které softwarové produkty nabízejí a možnosti využití vzájemné integrace jsou uvedeny na obr. 9.



Obr. 9. Funkce softwarových produktů

Každý hardwarový prvek řídící určitou činnost musí obsahovat podpůrný software. Podle použití je dělíme na:

1. Software ústředěn poplachových systémů

Software ústředěn představují programy dodávané jako součást k danému typu ústředny a jejich hlavními funkcemi je sledování a vyhodnocování událostí a jejich archivaci a programování pro potřeby servisního technika. Zajišťují místní nebo vzdálené spojení ústředny I&HAS s PC, [1]

2. Software pro uživatelskou správu

Tento typ softwaru umožňuje uživatelům systému nastavení realizovat uživatelskou správu řídicích jednotek. Nejrozšířenějším typem softwarů pro uživatelskou správu je použití přístupových systémů, kde je možnost úpravy jednotlivých prvků databázových systémů. A to zejména přidělování uživatelských práv, vytváření a nastavování uživatelských profilů s časovými rozvrhy přístupů, vyfiltrování určitých událostí aj.,

3. Software pro vizualizaci

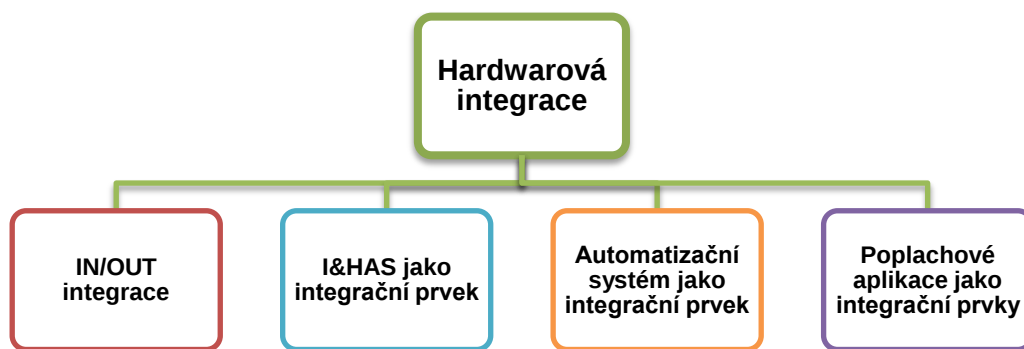
Vizualizační softwary jsou nástavbové programy sloužící pro zobrazení aktuálního stavu systému v reálném čase. Tyto softwary se často používají pro rozsáhlé objekty rozdělené na podsystémy, u kterých grafické zobrazení výrazně zvyšuje uživatelský přehled. Vizualizační programy tedy zvyšují komfort, přehlednost a zjednodušují ovládání jednotlivých prvků systému.

4. Integrační software systémů budov

Integrační software systémů budov je realizovaný jako program implementovaný do hlavního řídicího prvku (serveru) a slouží ke vzájemnému propojování jednotlivých bezpečnostních systémů a dalších technologií budov. Ovládání těchto systémů zajišťují klientské PC prostřednictvím webového prohlížeče. Integrační software musí být navrhnout tak, aby při jeho kolizi nebyly negativně ovlivněny funkce připojených poplachových a nepoplachových aplikací. Ochrana proti výpadku se řeší zabezpečením jednotlivých vazeb na hardwarové úrovni. Výhodou integračního softwaru je možnost realizace většiny funkcí softwarových produktů v rámci integrace poplachových systémů, [1]

1.5.2 Hardwarová integrace

Způsob realizace integrace jednotlivých aplikací hardwarovým řešením umožňuje vzájemné propojení jednotlivých poplachových a nepoplachových systémů pomocí jejich vstupů a výstupů (IN/OUT) a dalších rozšiřujících modulů sloužících pro připojení a ovládání dalších poplachových a nepoplachových aplikací. Hardwarový způsob integrace lze zajistit i automatizačním systémem budov s možností připojení a ovládání poplachových zabezpečovacích prvků.



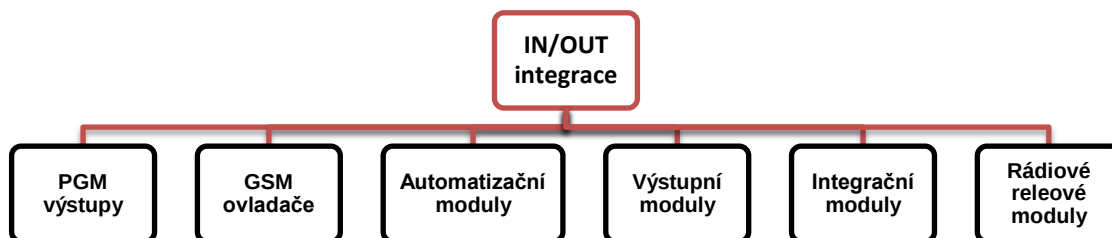
Obr. 10. Způsoby hardwarové integrace

1. Integrace IN/OUT

IN/OUT integrace je založena na vzájemném předávání ovládacích signálů mezi jednotlivými poplachovými a nepoplachovými aplikacemi prostřednictvím jejich vstupů a výstupů. Na základě těchto informací o jednotlivých aplikacích a předem definovaných akčních a reakčních událostech lze realizovat ovládání jiných systémů.

Tento typ integrace je vhodnější pro méně rozsáhlé objekty z důvodu jasně daného počtu PGM výstupů či modulů, vysokých nároků na kabeláž a při rostoucí složitosti

systému klesá přehlednost. V rámci IN/OUT integrace je možné využít PGM výstupy, GSM ovladače, automatizační moduly, výstupní moduly, integrační moduly a rádiové reléové moduly.

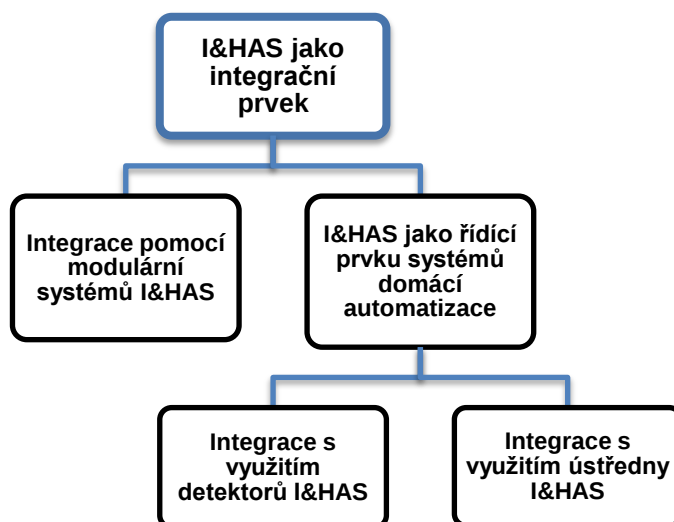


Obr. 11. Integrace IN/OUT

2. Poplachový zabezpečovací a tísňový systém jako integrační prvek

Hardwarová integrace pomocí poplachového zabezpečovacího a tísňového systému jako integračního prvku je založena na sběrnicovém výstupu z ústředny umožňující připojení a řízení činnosti modulů pro poplachové (systém kontroly vstupu, CCTV) a nepoplachové aplikace (automatizační prvky) nebo adresovatelné zabezpečovací komponenty. I&HAS jako integrační prvek lze využít pro řízení automatizačních prvků i generováním ovládacích signálů na základě stavu, požadavku, události, časového plánu prostřednictvím výstupu z ústředny I&HAS. [1]

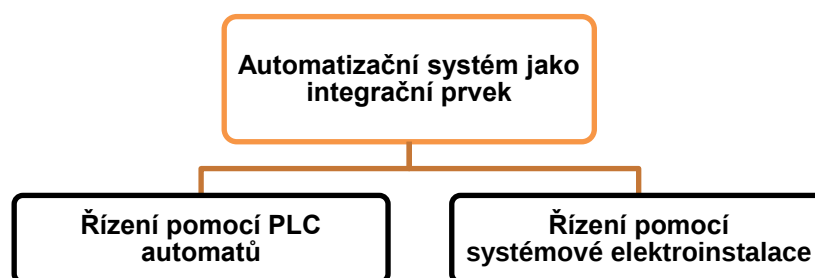
V obou typech řešení je centrální řídicí prvek realizován pomocí ústředny I&HAS, na kterou jsou implementovány další aplikace.



Obr. 12. I&HAS jako integrační prvek

3. Automatizační systém jako integrační prvek

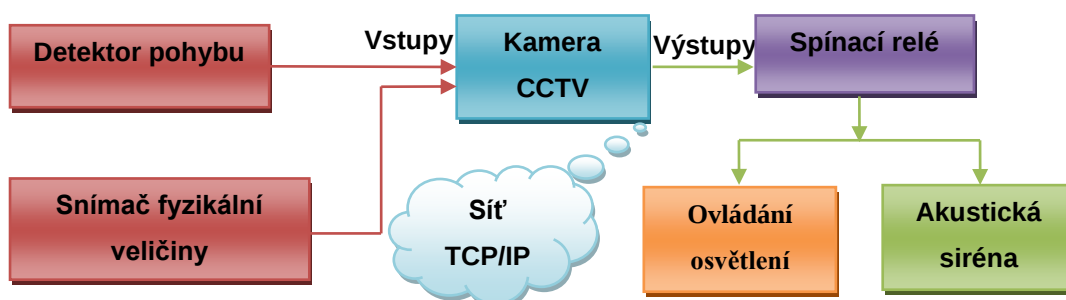
Další metodou hardwarové integrace je využití automatizačního systému jako integračního prvku k ovládání jak nepoplachových tak i poplachových aplikací. Centrální řídicí jednotku tvoří PLC automaty. V současnosti se začíná využívat technologie systémové elektroinstalace založená na principu sběrnice, na kterou je možné připojit snímací a akční členy. Nastavení vazeb mezi jednotlivými členy lze realizovat lokálně nebo dálkově přes vzdálené zařízení prostřednictvím GSM nebo internetu.



Obr. 13. Automatizační systém jako integrační prvek

4. Využití poplachových aplikací jako integračních prvků

V rámci poplachových aplikací nemusí tvořit vždy integrační prvek pouze ústředna I&HAS, ale i jednotlivé poplachové aplikace nebo jejich komponenty. Například kamerový systém, u kterého jsou pomocí digitálních vstupů připojeny jednotlivé detektory. Na základě jejich signálů jsou prostřednictvím digitálních výstupů přes spínací relé ovládána výstupní zařízení. Centrální řídicí prvek tvoří kamera a její ovládání je často realizováno za pomoci sítě TCP/IP, která může sloužit i jako CLOUD úložiště pro zachycené videosekvence (viz obr. 14). Způsobů využití aplikací je nepřehledné množství a záleží pouze na konkrétním typu využití a zpracovateli projektu. Je prakticky možné konfigurovat vstupní a výstupní zařízení dle potřeby a tím si přizpůsobit systém dle požadavků zákazníka.



Obr. 14. Poplachová aplikace jako integrační prvek

Dílčí závěr

Kapitola definuje základní pojmy z oblasti integrovaných systémů a jejich členění. V současnosti jsou při zavádění kladeny na integrované systémy vysoké požadavky, zejména na zvýšení bezpečnosti systému, zvýšení úspory na provoz zařízení a komfort zařízení.

Stále se rozvíjejícím trendem je ovládání systému realizované přes přenosná zařízení (notebook, smartphone či tablet), na kterých je instalována softwarová nástavba ve formě aplikací. Takovéto řešení může představovat přístup zaměstnance firmy ke své docházce v zaměstnání, kde si může vzdáleně plánovat dovolenou či komunikovat s nadřízenými prostřednictvím přenosného zařízení.

Integrovaný poplachový systém lze realizovat softwarovým nebo hardwarovým způsobem. U softwarového řešení jde o vzájemné propojení systémů pomocí nastavbových programů a následné definování vzájemných vztahů a pravidel. Principem hardwarového řešení je využití propojení systémů pomocí jejich vstupů a výstupů a přídavných modulů, čímž jsou definovány vzájemné vztahy. V reálném zapojení jde většinou o kombinace hardwarového a softwarového řešení.

2 TECHNICKÉ POŽADAVKY NA INTEGROVANÉ POPLACHOVÉ SYSTÉMY

V rámci aplikace integrovaných poplachových systémů je nutné, aby pro každou aplikaci systému byly použity příslušné normy. Všeobecnými požadavky na integrované poplachové systémy se zabývá **technická norma ČSN CLC/TS 50398 Poplachové systémy – kombinované a integrované systémy – Všeobecné požadavky**. Tato norma klade požadavky na integraci několika aplikací (poplachových i nepoplachových) do společného integrovaného systému. Obsahem normy je vymezení základních pojmů z oblasti integrovaných poplachových systémů, jejich konfigurace a informace o jeho návrhu. V této kapitole budou řešeny pouze konfigurace a technické požadavky na integrované poplachové systémy.

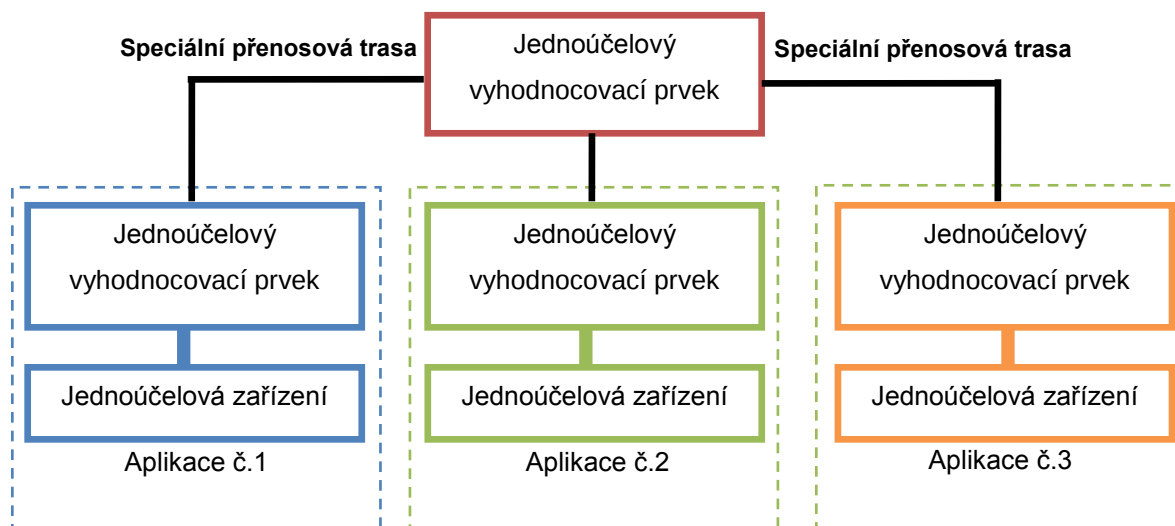
Zařízení sdílené jednou nebo více aplikacemi (společné zařízení) musí vyhovovat všem vyžadovaným aplikačním normám. U těchto společných zařízení je nutné, aby plnili funkce, pro které jsou primárně konstruovány a současně musí být odolné vůči vlivům, které by mohli ovlivnit jejich správnou funkci. Pro zařízení určené pro jednu funkci (jednouúčelová zařízení) je nutné plnění příslušných aplikačních norem.[6]

2.1 Konfigurace integrovaných poplachových systémů

Norma ČSN CLC/TS 50398 specifikuje 3 konfigurace či typy integrovaných poplachových systémů. Typ 1, typ 2A a typ 2B.

2.1.1 TYP 1

Tento typ konfigurace je kombinací dvou a více jednouúčelových systémů (poplachové, nepoplachové) připojené ke společnému doplňkovému zařízení (zařízení sdílené jednou nebo více aplikacemi, ale není vyžadováno normou). Společné doplňkové zařízení může představovat PC, zobrazovací zařízení aj. a její propojení je zajištěno doplňkovou přenosovou trasou. Zařízení typu 1 nesmí být v žádném provozním stavu ohroženo nebo nepříznivě ovlivněno jinými jednouúčelovými zařízeními nebo doplňkovými zařízeními (zajištění integrity systému).[6]



Obr. 15. Příklad konfigurace 1 s CCF třídy 1 [6], upravil Pavlínek, 2014

2.1.2 TYP 2

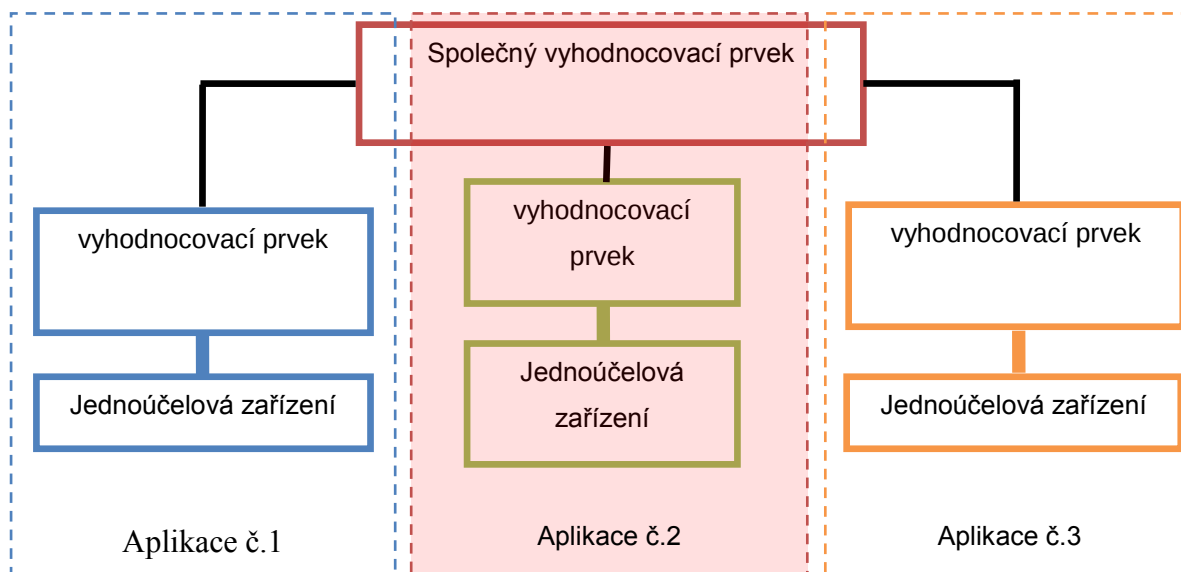
Typ konfigurace 2 je kombinací dvou nebo více jednoúčelových systémů, využívající normou vyžadující společné zařízení minimálně pro jednu aplikaci. Typ dvě je klasifikován do dvou podskupin 2A a 2B.

a) TYP 2A

Typ 2A je využitelný pro integraci poplachových a nepoplachových systémů. Využívají společné přenosové trasy, zařízení a vybavení. Při vzniku poruchy v kterékoliv části systému nesmí dojít k poruše jiné aplikace, což zajistíme redundancí potřebných prvků či přenosových tras (nesmí být nepříznivě ovlivněna integrita zařízení).

b) TYP 2B

Typ 2B je využitelný taktéž pro integraci poplachových a nepoplachových systémů. Využívají společné přenosové trasy, zařízení a vybavení. Na rozdíl od typu A při vzniku poruchy v kterékoliv části systému může mít negativní vliv na jiné aplikace nebo dojít k jejich poruše (může být nepříznivě ovlivněna integrita zařízení).



Obr. 16. Konfigurace typu 2 [6], upravil Pavlínek, 2014

2.2 Přehled technických požadavků na integrované poplachové systémy

Tato kapitola vyčleňuje technické požadavky ze systémových požadavků normy ČSN CLC/TS 50398 a definuje jejich základní vlastnosti, se kterými by měli být všechny součásti ve shodě. Vyjadřuje podmínky pro výrobce, na které musí při výrobě zařízení dbát. Jsou to zejména:

- požadavky na společné ovládací zařízení,
- požadavky na signalizační zařízení,
- požadavky na centrální ovládací zařízení,
- požadavky na montáž a propojení jednotlivých aplikací,
- požadavky na napájecí zdroje,
- provozní kniha.

2.2.1 Požadavky na společné ovládací zařízení

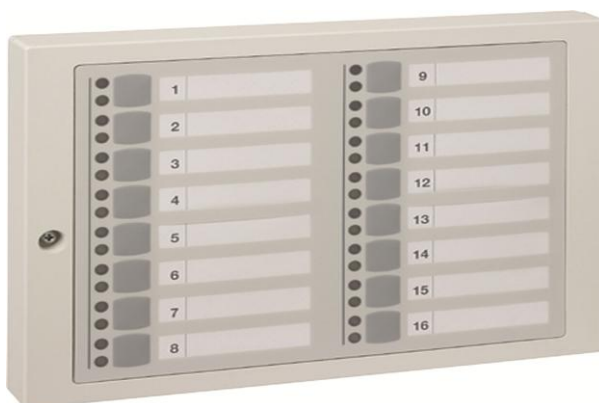
Norma ČSN CLC/TS 50398 klade technický požadavek, aby manuální ovládání systému bylo jednoznačné a jasné. Pokud je manuálním ovládacím zařízením ovládáno více aplikací, musí být jednoznačně a jasně indikováno, která zařízení jsou jednotlivými ovládacími prvky ovlivněny.

2.2.2 Požadavky na signalizační zařízení

Tato část vyjadřuje požadavky na výrobce signalizačního zařízení. Zejména optické a akustické signalizační zařízení.

a) Optické signalizační zařízení

Signalizační zařízení by podle normy mělo být vyrobeno tak, aby barva indikační kontrolky (například LED dioda) měla tak vysokou svítivost, aby nejkritičtější informace byla jasně viditelná za předpokládané úrovně osvětlení. Barvy signalizačních zařízení definované normou musí být respektovány. V případě neshody s danou normami musí být signalizační zařízení v souladu s normou **ČSN EN 60073 ed.2 Základní a bezpečnostní zásady pro rozhraní člověk-stroj, značení a identifikaci - Zásady kódování sdělovačů a ovládačů**. [6]



Obr. 17. LED přehledové tablo Honeywell [7]

b) Akustické signalizační zařízení

Akustické signalizační zařízení (například sirény) různých aplikací musí být logické dle různých podmínek dané normou.

2.2.3 Požadavky na centrální ovládací zařízení

Centrální ovládací zařízení (CCF) slouží k řízení či ovládání jednotlivých aplikací integrovaného systému nebo signalizaci stavových informací. CCF musí být jednoznačně zařazeno do příslušné třídy, jeho umístění musí být v souladu se specifikací výrobce zařízení a současně sloužit pouze pro ovládání integrovaného poplachového systému. CCF je klasifikováno do dvou tříd.

a) Třída 1

U třídy 1 se centrální ovládací zařízení využívá k zobrazování informací pouze v prostorách, kde na systém dohlíží obsluha a současně normou vyžadované signalizační zařízení musí být taktéž ve stejných prostorách s dohledem. Stejné umístění je zvoleno z důvodu výpadku či poruchy centrálního řídicího prvku. Tedy

poplach bude i při výpadku centrálního řídicího prvku indikován a povšimnut obsluhou. [6]

b) Třída 2

U třídy 2 se centrální ovládací zařízení využívá k zobrazování informací jako jediný informační displej v prostorách s dohledem provozní obsluhy. V případě, že dokáže kromě primární funkce zobrazování informací poskytovat i ovládání či nastavování stavů a parametrů ústředny (zastřeženo/odstřeženo) nebo konfiguraci zón (zapnutí/vypnutí) musí být systém v souladu s aplikačními normami. CCF třídy 2 často představují PC, které nemusí být v souladu s aplikačními normami za předpokladu, že nemůže negativně ovlivnit jednoúčelové poplachové zařízení. [6]

2.2.3.1 Požadavky na záložní napájení centrálního zařízení

Norma ČSN CLC/TS 50398 stanovuje, že každé centrální zařízení (CCF) musí obsahovat záložní zdroj. Typ záložního zdroje musí být navrhnout tak, aby dokázal zajistit napájení centrálního ovládacího zařízení po dobu k zajištění nejnutnějších postupů při poruše.

2.2.4 Požadavky na montáž a propojení jednotlivých aplikací

Propojování jednotlivých aplikací hardwarovým nebo softwarovým způsobem a definování vzájemných vazeb už je probráno v první části práce. V této části je rozebráno propojení z hlediska norem. Pokud připojíme jednu nebo více aplikací nesplňující požadavky aplikačních norem k zařízení splňující normy, je nutné splnit požadavky:

- 1) zařízení budou zpracovávat pouze povely ovládání poplachového systému povolené aplikačními normami,
- 2) pokud zařízení přijme neidentifikovatelný signál, nebude mít tento signál nepříznivý vliv na jednotlivé aplikace,
- 3) při úmyslném zasahování narušitele nesmí být narušena funkce poplachových aplikací nebo musí toto zařízení plnit požadavky sabotáže a monitorování dle příslušných aplikačních norem.

Z pohledu montáže za předpokladu sdílení společné kabeláže pro více subsystémů, musí tato kabeláž splňovat specifikace pro aplikační požadavky v nejvyšší integritě a provedení.

[6]

2.2.5 Požadavky na napájecí zdroje

Při použití společných nebo speciálních zařízení nesmí ohrozit požadavky na napájení příslušných aplikačních norem. V rámci použití společných a speciálních zařízení, nesmí docházet ke snížení pohotovostní doby pod dobu stanovenou aplikačními normami.

2.2.6 Provozní kniha

V souvislosti s technickými požadavky je součástí i provozní kniha sloužící pro vedení preventivních a nápravných záznamů jednotlivých aplikací i celého systému. Zapisovaná data v provozní knize by měla být vždy řazena chronologicky od nejstarších po nejnovější a současně by měla být vedena taktéž podle aplikačních norem. [6]

[illegible]

Obr. 18. Provozní kniha Eurosat [8]

Dílčí závěr

Technické požadavky by měly být vždy dostupné v (příslušných) relevantních normách. U integrovaných systémů je to norma **ČSN CLC/TS 50398 Poplachové systémy – kombinované a integrované systémy – Všeobecné požadavky**. Tato norma klade požadavky na integraci několika aplikací (poplachových i nepoplachových) do společného integrovaného systému. Projektant či systémový integrátor by měl mít ve svém zájmu vždy přehled o aktuálních normách v dané oblasti, respektovat je a řídit se jimi při vypracování projektu integrovaného systému. Takový přístup vede ke kvalitnímu zpracování projektu a eliminaci pozdějších neshod se zákonnými předpisy a současně zvyšuje statut projektanta.

3 TECHNICKÉ POŽADAVKY NA PŘÍSTUPOVÉ SYSTÉMY

Přístupové systémy (ACS) či systémy kontroly vstupů tvoří souhrn konstrukčních a organizačních náležitostí a zařízení potřebné k ovládání vstupů. Hlavním smyslem přístupových systémů je kontrola a evidence vstupu a rozhodnout o tom:

- **kdo** má povolen přístup,
- **kdy** je přístup povolen,
- **kde** může být přístup získán.

Tato opatření minimalizují riziko zabránění vstupu neoprávněných osob do střežených prostor. Často jsou přístupové systémy použity k zabránění přístupu k utajovaným informacím. Pomocí technických prostředků je možno rozlišit jednotlivé vstupující osoby, kontrolovat jednotlivé průchody či sledovat jejich pohyb po střeženém prostoru (v rámci jednotlivých zón) a na základě specifických identifikátorů provádět jejich vyhledávání. Technické prostředky mohou být představovány snímači identifikačních karet bez evidence až po sofistikovaný on-line systém s centrální evidencí či analýzou s integrací s dalšími aplikacemi.

Princip funkce spočívá ve schopnosti sejmut zakódované údaje pomocí čteček. Zakódované údaje dle stupně rizikovosti obsahující informace o uživateli a prostorové, časové či personální oprávnění. Dle požadované bezpečnosti se instalují přístupové systémy s různými stupni rizikovosti. Identifikační zařízení mohou představovat:

- klávesnice,
- kontaktní či bezkontaktní karty (s čárovým, magnetickým, čipovým či RFID kódem),
- kamerový systém s identifikací obličeje,
- biometrické systémy (využívající otisk prstu, hlas, oční duhovku, krevní řečiště, hlas uživatele).



Obr. 19. RFID karta [9]

Stále častější je integrace přístupového systému s jinými poplachovými či nepoplachovými aplikacemi. Nejrozšířenější variantou je kombinace ACS s docházkovým systémem či kamerovým systémem.



Obr. 20. Přístupový a docházkový terminál [10]

3.1 Analýza technických požadavků na přístupové systémy

Problematiku technických požadavků částečně vymezuje norma ČSN EN 50133-1 **Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky**. Dále normy ČSN EN 50133-2-1 **Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích- Část 2-1: Všeobecné požadavky na komponenty** a aplikační norma ČSN EN 50133-7 **Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace**. Základním kritériem při návrhu systému kontroly vstupu, jehož část tvoří zabezpečovací systém je nutnost splňovat všechny požadavky norem na zabezpečovací systémy. Přístupový systém se může skládat z libovolného počtu přístupových míst a tato norma se rovněž zabývá zabezpečovacími aplikacemi pro jednotlivá přístupová místa. Bezpečnost přístupového systému je založena na klasifikaci identifikace a klasifikace přístupů a je možno ji určit pro každé přístupové místo, odděleně pro vstup a výstup. S požadavky na různé stupně důvěrnosti přístupu jsou definovány třídy identifikace:

- **třída identifikace 0** (žádná přímá identifikace),
- **třída identifikace 1** (identifikace dle informace uložené v paměti),

- **třída identifikace 2** (identifikace dle identifikačního prvku či biometrie),
- **třída identifikace 3** (identifikace dle identifikačního prvku či biometrie spolu s informací uloženou v paměti). [11]

Současně musí být definována klasifikace přístupů, která se dělí:

- **třída přístupu A** (U přístupových míst této třídy není nevyžadováno ukládání přístupové transakce ani časový filtr),
- **třída přístupu B** (U přístupových míst této třídy jsou vyžadovány časové filtry a ukládání přístupové transakce. Platí i pro přístupová místa zahrnující pouze časové filtry bez funkce ukládání). [11]

3.1.1 Společné technické požadavky pro třídy přístupu A a B

Tyto technické požadavky jsou univerzální pro obě třídy přístupu nezávisle na časovém filtru a funkci ukládání.

3.1.1.1 Požadavky na hlášení

Přístupový systém musí disponovat prostředky sloužící pro zobrazení a výstrahy:

- otevření místa přístupu po uplynutí poskytnutého intervalu pro přístup,
- otevření místa přístupu bez odpovídajícího oprávnění,
- detekce sabotáže.

Současně musí být systém nastaven tak, aby ohlášení spuštění výstrahy bylo s maximálním možným zpožděním 10 sekund.

3.1.1.2 Požadavky na ovládání přístupových míst

Systém kontroly vstupu musí být konstruován tak, aby:

- byl vybaven rozhraním pro komunikaci s APAS (ovládací prvky a senzory místa přístupu) a rozhraní musí umožňovat ovládat a monitorovat stav zabezpečení APAS,
- svorkovnice rozhraní místa přístupu byla umístěna uvnitř skříně (umožňující detekci sabotáže),
- bylo znemožněno získání přístupu k obvodu uvolnění ze strany s nižší úrovní zabezpečení,
- byly stále monitorovány stavy APAS (uzavření/otevření),

- ovládací výstup rozhraní místa přístupu obsahoval alespoň jeden bezpotenciálový kontakt se jmenovitým zatížením minimálně 30VA,
- ovládací výstup rozhraní přístupového místa musí být sepnut při povoleném přístupu a musí být zrušen při uběhnutí definovaného časového úseku uvolnění APAS nebo při monitorování indikace APAS, že je otevřen. [11]

3.1.1.3 Požadavky na napájení

Přístupový systém musí být konstruován tak, aby při připojení či odpojení napájení nedošlo k chybnému uvolnění vstupu. Ale současně se nepožaduje napájení apasu systémem kontroly vstupu.

3.1.2 Doplnkové technické požadavky pro třídu přístupu B

3.1.2.1 Požadavky na hlášení

Pro všechny typy identifikace

Přístupový systém musí disponovat prostředky sloužícími pro ukládání následujících typů událostí do paměti:

- otevření místa přístupu bez poskytnutí přístupu (včetně uvedení místa přístupu),
- otevření místa přístupu po uplynutí povolené periody pro poskytnutí přístupu (včetně uvedení místa přístupu),
- vstup nebo výstup z režimu programování,
- detekce sabotáže včetně místa sabotáže.

Zaznamenaná událost včetně druhu, data a času musí být uložena maximálně do 60 sekund.

Pro identifikace typu 1, 2 a 3

Přístupový systém musí disponovat prostředky sloužící pro ukládání následujících typů událostí do paměti:

- transakce s odkazem na uživatele a místo,
- odmítnutý přístup pro uživatele patřícího do systému s odkazem na uživatele a místo.

Minimální kapacita pro ukládání událostí je 500. [11]

3.1.3 Technické požadavky na komponenty přístupových systémů

V této části jsou rozebrány jednotlivé požadavky na komponenty přístupových systémů. Základní rozdělení komponentů přístupových systémů se dělí na:

- pevné (zařízení připevněné k podložce či zajištěné na určitém místě),
- přemístitelné (zařízení, které nezůstává v provozu při změně umístění),
- přenosné (zařízení vytvořené pro provoz i pro přenášení).

3.1.3.1 Požadavky na vlivy prostředí

Pro komponenty přístupových systémů jsou definovány 4 třídy prostředí:

- I. vnitřní (obytné a kancelářské prostředí),
- II. vnitřní všeobecné (obchody, výrobní a montážní haly, skladové prostory),
- III. vnější (prostory chráněné přímému dešti a slunečním paprskům),
- IV. vnější všeobecné (ostatní nechráněné prostory).

Z nichž se používají pro komponenty třídy I. pro vnitřní a III. pro vnější.

3.1.3.2 Požadavky na elektromagnetickou kompatibilitu

Technické požadavky z hlediska splňování elektromagnetické kompatibility lze rozdělit do tří odvětví a musí splňovat následující normy:

- **Vyzařování** (55022, 61000-6-3, 61000-6-4)
- **Odolnost** (50130-4, 61000-6-1, 61000-6-2)
- **Požadavky elektrické bezpečnosti** (EN 60950, EN 60065) [11]

3.1.3.3 Požadavky na kabeláž

Kabeláž k přístupovým systémům by měla být navržena tak, aby byli co nejmenší vzdálenosti mezi zařízeními. Současně by měly být kabelové rozvody situovány tak, aby mohlo v budoucnu dojít k rozšiřování systému či změnám v umístění. S technického hlediska by se měly kabely volit dle požadavků příslušných předpisů s ohledem na bezpečnost, spolehlivost, útlum signálu či úbytků napětí. Z hlediska umístění by se měly kabelové rozvody umísťovat do krytých nebo těžko dostupných míst v zabezpečených prostorech. Při riziku mechanického poškození by měla být zajištěna odpovídající ochrana. U kabeláže používající malé napětí a u signálových kabelů se musí zabránit souběhu se síťovými kabely nebo s kabely generující rušení.[12]

3.1.3.4 Požadavky na kryty zařízení

Konstrukce přístupového systému musí být vyrobena tak, aby nebylo možné jeho otevření nebo oddálení z montážní polohy bez použití nástrojů (šroubováky, klíče, speciální nástroje). Současně nesmí být nastavovací součásti vně krytu komponentu. Kryt zařízení by měl poskytovat skryté kabelové průchody ze zadní strany zařízení, pokud tomu tak není, musí být tato skutečnost uvedena v dokumentaci výrobku.

Pro rozhranní místa přístupu platí, že:

- musí být umístěno uvnitř krytu vybaveného detekcí sabotáže,
- musí být umístěno uvnitř krytu s opatřením pro ukrytí kabelových průchodů či prostředků pro monitorování připojení (neplatí, pokud je v dokumentaci uvedeno použití na straně nižšího stupně zabezpečení nebo na nezabezpečené straně),
- kryty rozhranní místa přístupu v závislosti na třídě prostředí musí splňovat následující stupně krytí:
 - třída prostředí I, II IP 30,
 - třída prostředí III IP 32,
 - třída prostředí IV IP 34.

Pro identifikační zařízení platí stejné požadavky na stupně krytí i kabelové průchody. Rozdíl je pouze v tomto technickém požadavku: „*Pokud je možné poskytnutí přístupu jednoduchou manipulací (např. testovacím prvkem, servisním nástrojem, zkratem), musí být kryt identifikačního zařízení vybaveno detekcí sabotáže, která je aktivována při otevření krytu normálními prostředky*“.[13]



Obr. 21. Kryt se skrytým kabelovým průchodem [14]

3.1.3.5 Požadavky na napájecí zdroje

Kapacita napájecího zdroje musí být volena podle elektrické specifikace připojených komponentů při jejich největší předpokládané zátěži v normálních provozních podmínkách. Umístění napájecích zdrojů by mělo být vždy situováno v zabezpečeném prostoru, ale pokud to není možné či nepraktické, je nutné zajistit opatření ekvivalentní k úrovni zabezpečení střeženého prostoru. Dalším požadavkem je připojení napájecího zdroje k rozvodné síti samostatně jištěným přívodem. U všech komponentů systémů kontroly vstupů musí být vstupy a výstupy napájení chráněny proti zkratu. [12]



Obr. 22. Záložní napájecí zdroj [15]

3.1.3.6 Požadavky na identifikaci a značení

Komponenty přístupového systému musí být jednoznačně označeny prostřednictvím štítku, na kterém jsou zobrazeny informace o:

- jménu organizace, odpovědnou za shodu výrobku,
- typu výrobku,
- údaje o výrobci,
- další označení vyžadující normy či předpisy.

Označení na výrobku musí být pevně umístěny uvnitř nebo vně výrobku a současně snadno čitelné a odolné vůči specifickým povětrnostním podmínkám (trvanlivé). [12]



Obr. 23. Popis USB/RS 485 převodníku [16]

Dílčí závěr

Technickými požadavky na přístupové systémy se zabývají normy **ČSN EN 50133-1 (systémové požadavky)**, **ČSN EN 50133-2-1 (všeobecné požadavky na komponenty)** a **ČSN EN 50133-7 (pokyny pro aplikace)**.

Z těchto norem byly vybrány technické požadavky a jejich základní rozdělení. Zmíněné systémové požadavky na třídy přístupu a identifikace nejsou ryze technickými prostředky, ale jsou níže uvedeny z důvodu vzájemné vazby na jiné technické požadavky a z hlediska důležitosti při zařazení. Technické požadavky slouží jak pro výrobce zařízení jako průvodní dokument při výrobě zařízení, tak pro uživatele zařízení jako podklady informativního charakteru.

Všechny uvedené komponenty přístupových systémů před uvedením na trh podléhají provozním zkouškám na suché teplo, chlad, vniknutí vody, vibrace, poklesy a krátkodobá přerušení síťového napájecího napětí, ráz a změny síťového napájecího napětí. Tyto zkoušky by měly zaručit bezproblémovou funkci zařízení v běžných provozních podmínkách.

II. PRAKTICKÁ ČÁST

4 INTEGRACE PŘÍSTUPOVÉHO SYSTÉMU S DALŠÍMI APLIKACEMI

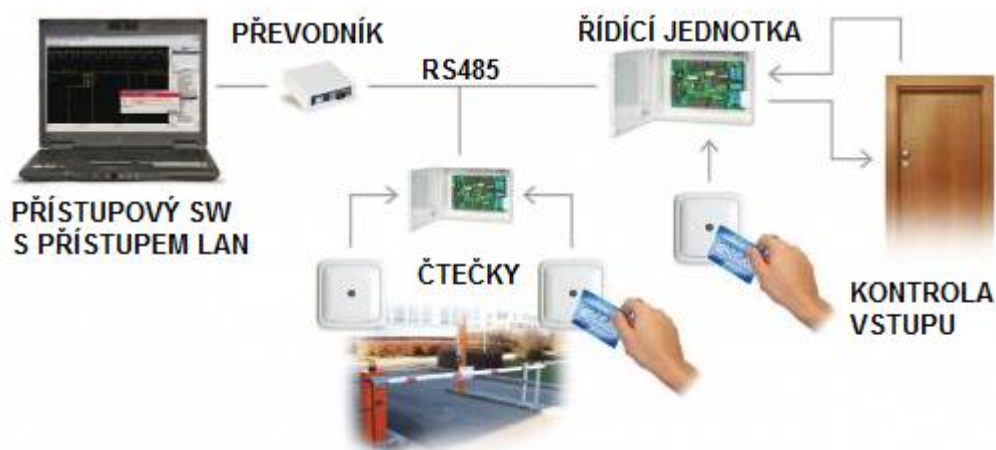
Z pohledu integrace přístupového systému s dalšími poplachovými a nepoplachovými aplikacemi je mnoho možností realizace. Všeobecně je cílem integrace vytvoření efektivnějšího celku na základě spojení menších součástí. Realizovat integrovaný systém lze pomocí hardwarového nebo softwarového řešení. V současných sofistikovanějších objektech je často realizováno softwarové řešení integrace, kde na základě stejného komunikačního protokolu jsou jednotlivé aplikace připojovány na společnou sběrnici připojenou k serverovému PC s nastavbovým softwarem. V nastavbových programech lze nastavovat vzájemné vazby mezi aplikacemi a tím zajistit vzájemnou integraci.

Všechny následující varianty integrace lze vyřešit softwarovou metodou, což však není cílem této práce. Náplní práce jsou zejména hardwarové řešení určené pro jednodušší objekty a zmínit příklady aplikace softwarové metody.

Integrace přístupového systému s poplachovými aplikacemi přináší především zvyšování bezpečnosti a naopak integrace s nepoplachovými aplikacemi se projevuje zejména zvyšováním komfortu užívání a snižování finančních nákladů na jejich provoz. Při propojování jednotlivých aplikací musí být splněny legislativní požadavky tvořené relevantními normami. Takovýto integrovaný systém pak tvoří komplexní systém prvků za účelem širšího využití, než pro který byl primárně vytvořen.

V závislosti na požadované složitosti integrovaného systému lze přístupové systémy strukturovat takto:

- **autonomní** - nejjednodušší varianta - pracují bez obslužného softwaru nezávisle na PC, programují se pomocí master karty),
- **skupinové (systémové)** - pokročilejší varianta – vzájemné propojení jednotlivých dveřních jednotek pomocí RS485 a následně připojené k PC pro nastavování práv a vlastností uživatelů a dveřních jednotek),
- **globální (sít'ovatelné)** - vlastnosti jako předchozí varianty s připojením k LAN s funkcí řízení přes internet. [17]

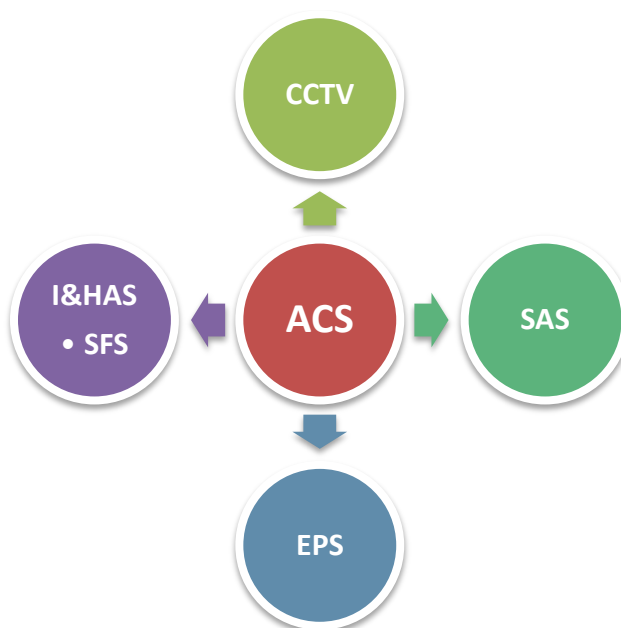


Obr. 24. Globální struktura přístupového systému [18]

4.1 Integrace přístupového systému s poplachovými aplikacemi

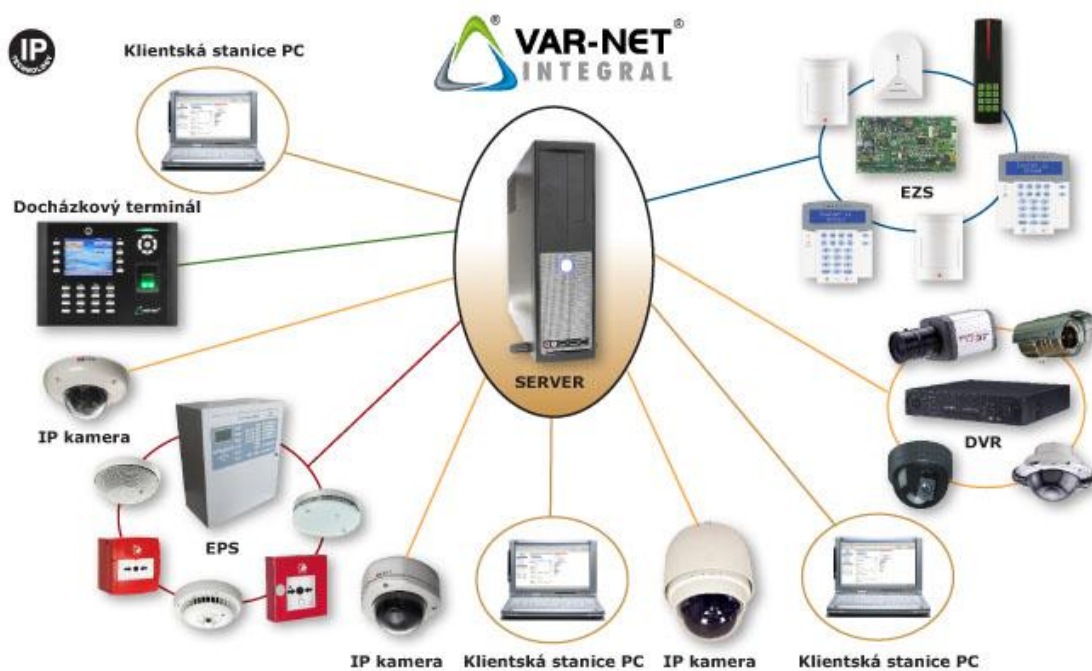
Jak již bylo zmíněno v úvodu, integrace přístupových systémů s poplachovými aplikacemi přináší zejména zvýšení bezpečnosti v daném odvětví. Pro reálné využití můžeme integrovat přístupové systémy zejména s:

- poplachovými zabezpečovacími a tísňovými systémy (I&HAS),
 - zamlžovacími systémy (SFS),
- elektrickou požární signalizací (EPS)
- kamerovými systémy (CCTV),
- systémy přivolání pomoci (SAS).



Obr. 25. Integrace přístupového systému s poplachovými aplikacemi

V rámci softwarové integrace poplachových aplikací lze znázornit řešení firmy VARIANT PLUS se systémem VAR-NET INTEGRAL, který spojuje přístupové systémy s poplachovými zabezpečovacími systémy, elektronickou požární signalizací, kamerovými systémy či docházkovými systémy. Výhodou je možnost vzdáleného přístupu a ovládání přes klientské PC stanice prostřednictvím internetu.



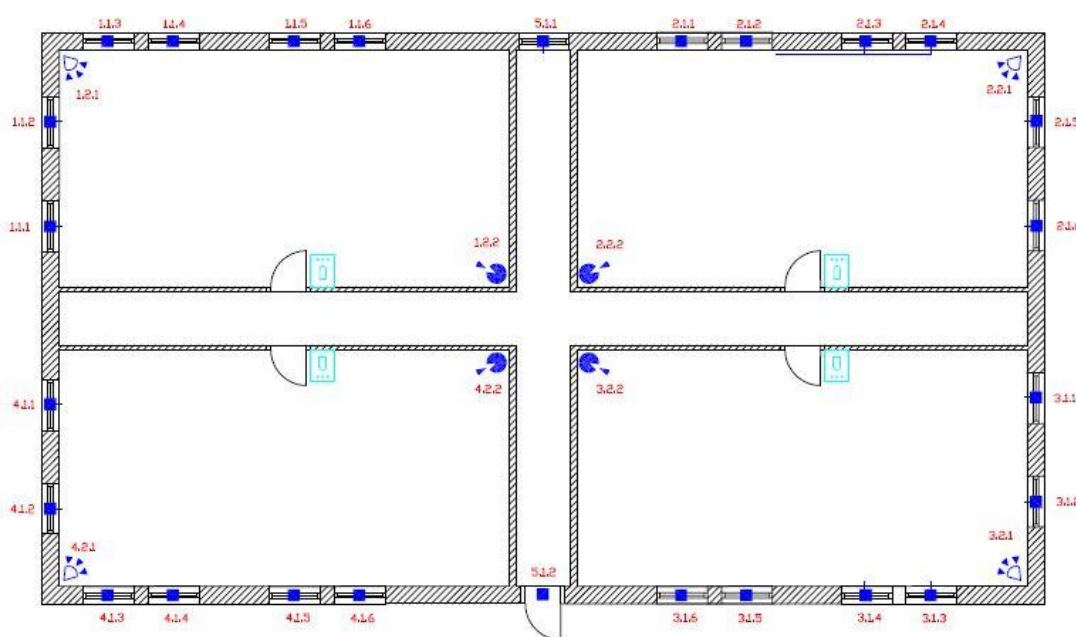
Obr. 26. Softwarové řešení integrace VAR-NET INTEGRAL [19]

4.1.1 Integrace přístupového systému s poplachovými zabezpečovacími a tísňovými systémy

Přístupový systém spolu s poplachovým zabezpečovacím systémem může být v budoucnu variantou integrace zejména ve firmách a větších podnicích, kde je objekt rozdělen na několik částí (zón), (viz obr. 27). Kdy například z důvodu několika směnného provozu je nutné zabezpečovat jen určité části objektu. Princip spočívá v přístupovém systému jako integračním prvku, kdy jednotlivým místnostem (zónám) jsou přiřazeny osoby, které do ní mají zpřístupněn vstup. Při vstupu se daná osoba musí identifikovat (např. RFID kartou) a přístupový systém vyšle signál ústředně k deaktivaci detektorů dané zóny. Při odchodu se tato osoba opět identifikuje a poté dojde k opětovné aktivaci dané zóny. Pro splnění funkčnosti tohoto řešení je nutné, aby přístupový systém disponoval pamětí indikující (přihlášení či odhlášení). Je tedy schopen rozlišit, zda je někdo přítomen v místnosti či ne.

Toto řešení je vhodné v rozsáhlých členitých objektech, kde je použit jeden poplachový zabezpečovací systém a mnoho dveřních jednotek. Výhodou je eliminace lidského faktoru (opomenutí osoby zastřežení či odstřežení dané zóny), čímž současně dochází k zamezení rizika vzniku planého poplachu. Tento princip současně plní funkci zamezení přístupu do dané sekce objektu.

V případě vyhlášení poplachu v dané sekci mohou být přístupové dveře do dalších částí objektu blokovány, tudíž narušiteli znemožněn další pohyb po objektu a signál z ústředny I&HAS odeslán na DPPC.

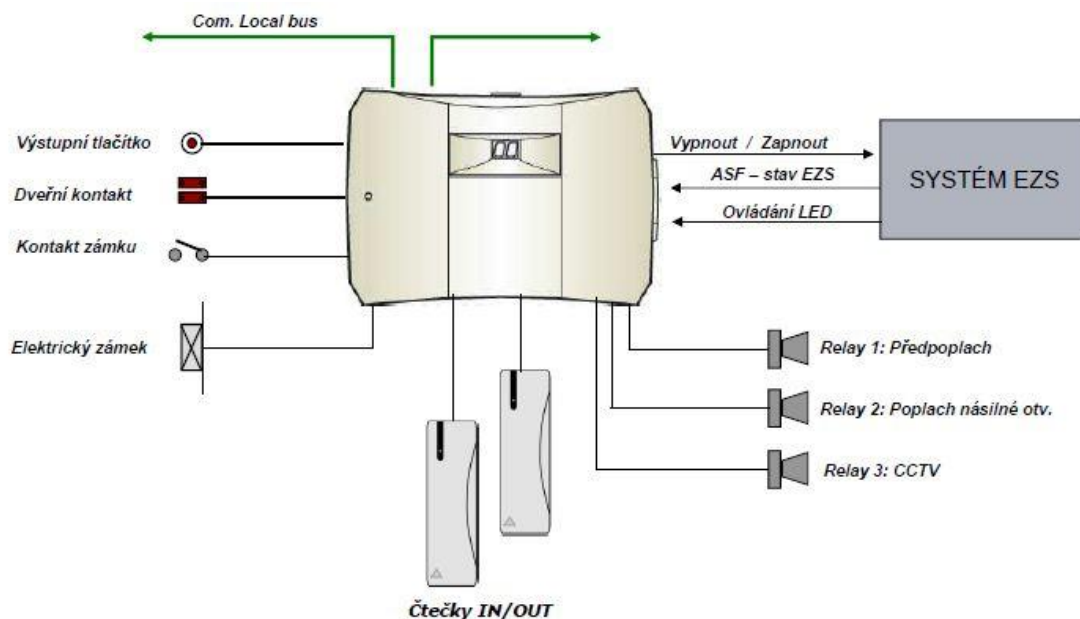


Obr. 27. Schéma integrace přístupového systému s I&HAS

Tísňový systém má velmi malý rozsah uplatnění v rámci integrace s přístupovým systémem. Reálné využití je možné na benzínových pumpách, kdy při napadení narušitelem a aktivování tísňového systému dojde k automatickému uzavření dveří. Avšak takové řešení není vhodné z důvodu vzniku velmi nebezpečné situace, kdy zůstane v objektu napadená osoba s narušitelem s nepředvídatelným chováním. Tudíž dle mého subjektivního názoru je tento typ integrace téměř nepoužitelný.

Siemens SiPaSS Entro

Praktický příklad využití lze nalézt u firmy Siemens se systémem SiPass, který kromě klasických funkcí přístupového systému umožňuje ovládat poplachový zabezpečovací systém. Využití dveřní jednotky Siemens DC22 lze vidět na následujícím schématu.



Obr. 28. Integrace přístupového systému s IAS [20]

Komunikaci mezi přístupovým systémem a poplachovým zabezpečovacím systémem zajišťuje systém ASF (alarm status feedback), který předává signál o svém stavu přístupovému systému. Na základě stavu přístupového systému po přiložení karty ke čtečce je pomocí bistabilního ovládání (zapnuto/vypnuto) spínán poplachový zabezpečovací systém. SiPass systém umožňuje i monostabilní bypass sloužící k přemostění vstupu poplachového zabezpečovacího systému na zvolenou dobu určenou k otevření dveří. Stav poplachového zabezpečovacího systému je signalizován pomocí LED diody na čtečce přístupového systému. Čtečka zobrazuje i předaktivační upozornění a aktivace poplachového zabezpečovacího systému lze realizovat na základě časového programu či ruční aktivace. Z hlediska uživatelských práv k ovládání IAS je možné definovat osoby s možnostmi:

- zapnutí i vypnutí IAS,
- pouze vypnutí IAS,
- pouze zapnutí IAS,
- bez možnosti ovládat IAS.

Ve variantě řešení ovládání IAS prostřednictvím přístupového systému by mohl nastat problém z hlediska norem, kdy stav IAS by nikdy neměl být ovládán jinou aplikací. Avšak z praktického hlediska, za předpokladu splňování stejného stupně zabezpečení, je takové řešení proveditelné a používané.[20]

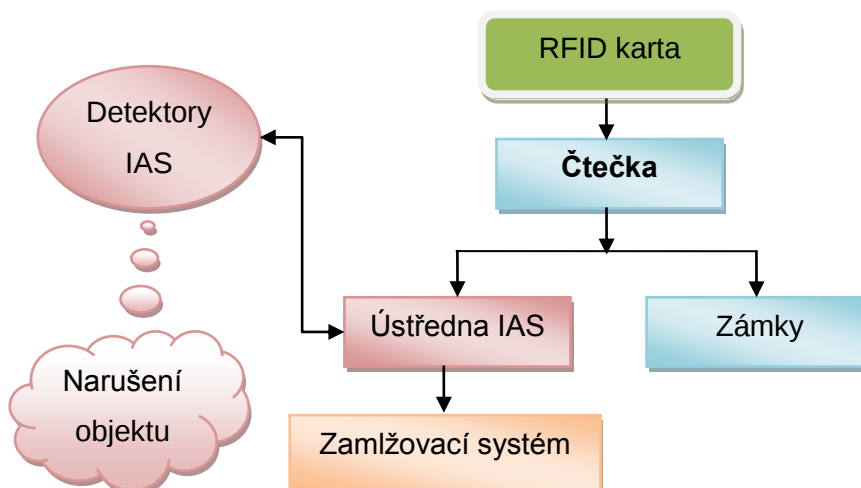
4.1.1.1 Integrace přístupového systému se zamlžovacími systémy

Zamlžovací systémy jsou zařízení tvořené generátorem husté mlhy za účelem dezorientace a vystrašení narušitele střeženého objektu. Aktivace zamlžovacího systému probíhá na základě vyhlášení poplachu poplachovým zabezpečovacím systémem. Zamlžovací systémy jsou vhodné k zabezpečení kanceláří, obchodů, lékáren či benzinových pump, kdy během několika sekund od spuštění poplachu dochází k vytváření husté mlhy a během 20 sekund je místnost zaplněna mlhou. V takto zamlžené místnosti je narušiteli znemožněna orientace a tím i snížena možnost pohybu.



Obr. 29. Zamlžovací systémy [21]

Princip použití může být založen na přiložení identifikačního média (např. RFID karty) ke čtečce, čímž dojde k zastřežení či odstřežení poplachového zabezpečovacího systému a na jejím základě je zapnut zamlžovací systém. Při narušení objektu dojde k aktivaci detektorů poplachového zabezpečovacího systému, které předají aktivační signál prostřednictvím ústředny IAS zamlžovacímu systému. Praktický příklad je stejný jako v případě integrace přístupového systému s IAS (Siemens SiPass), ale přes PGM výstup je k ústředně IAS připojen zamlžovací systém (viz obr. 30).



Obr. 30. Integrovaný přístupový systém se zamlžovacím systémem

4.1.2 Integrace přístupového systému s elektrickou požární signalizací

Elektrická požární signalizace v kombinaci s přístupovým systémem tvoří poměrně dobrý způsob realizace únikového systému. Při vzniku požáru, hlásiče elektrické požární signalizace vyšlou signál přímo na vstup do čtečky či klávesnice nebo na ústřednu EPS, která předá signál přístupovému systému, který automaticky otevře všechna přístupová místa. Tato přístupová místa mohou tvořit vstupní turnikety, elektrické zámky na dveřích či otevření bran a zvednutí závor. V případě elektrických zámků je nutné použít reverzní elektrické zámky, které jsou při přivedení napětí zamknuté, a po přerušení napětí dojde k odblokování. Tento typ zámku se používá z důvodu zajištění odblokování přístupových míst při porušení napájení při požáru. V případě použití obousměrných turniketů je nutné zajistit, aby v případě požáru byly povoleny oba směry otevírání z důvodu evakuace osob a současného přístupu hasičského záchranného sboru.

Přístupový systém s použitím Sebury K3

Takový způsob řešení je možné realizovat například čtečkou karet s klávesnicí SEBURY K3 s jedním vstupem, který využijeme pro neadresné požární hlásiče zapojené na společný vodič. Na výstup jsou zapojeny všechny elektromechanické zámky v objektu. Při vzniku požáru dojde k sepnutí NC vstupu čtečky a na základě naprogramování k sepnutí výstupu, na který jsou na společný vodič napojeny všechny elektromechanické zámky, čímž dojde k otevření všech dveří. Ostatní čtečky jsou taktéž zapojeny na jednotlivé zámky, a slouží k otvírání jednotlivých dveří na základě přidělených práv.

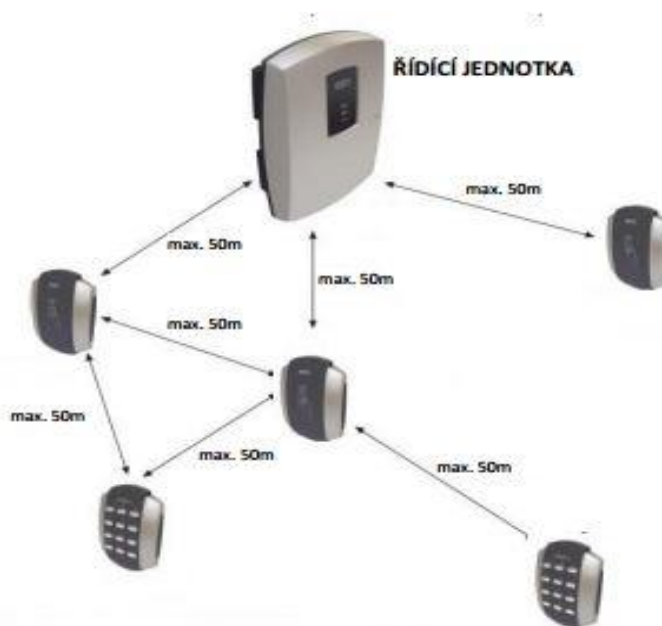


Obr. 31. Přístupový systém s neadresnými hlásiči

Při použití adresovatelných hlásičů požáru zjistíme přibližnou polohu vzniku požáru a dle požadavků je možné ovládat konkrétní přístupové místa. Pro toto řešení je ale nutné použití systémových či síťovatelných čteček, které lze vzájemně propojit a spolupracují s nastavbovým programem na základě shodného protokolu a v případě vzniku požáru, jsou automaticky otevřeny všechny přístupové body.

Bezdrátový přístupový systém Variant GSD

Tento příklad realizace lze nalézt u firmy Variant u bezdrátového přístupového systému GSD. Vhodné řešení pro objekty s požadavky na řízení přístupu osob a v případě, kdy není možné jednotlivé dveře drátově propojit do jednoho místa. V případě použití samostatných čteček je nutné, aby byli uživatelé do každé čtečky přidáni zvlášť. Při použití řídicí jednotky se provádí pouze centrální programování a data se následně bezdrátově rozešlou mezi jednotlivé čtečky či klávesnice. Vzdálenost mezi jednotlivými čtečkami, klávesnicemi či řídicí jednotkou by neměla přesáhnout 50 metrů v závislosti na překážkách. Každá čtečka přitom slouží jako opakovač, tedy zesiluje signál a je možné vytvořit řadu čteček dlouhou i několik set metrů. [22]



Obr. 32. Bezdrátový přístupový systém GDS [19]

Sestava se skládá z řídicí jednotky, bezdrátové čtečky karet, bezdrátové klávesnice a bezdrátové čtečky s klávesnicí. Řídicí jednotka komunikuje s klávesnicemi či čtečkami bezdrátově a má 4 programovatelné vstupy, na které mohou být připojeny různé aplikace.

V tomto případě detektory EPS do 4 smyček, podle kterých lze rozlišovat místo vzniku požáru. Řídící jednotka obsahuje i 4 programovatelné výstupy, na které mohou být připojeny prvky akustické a optické signalizace spínané při detekci požáru. Při detekci požáru hlásičem EPS jsou na základě naprogramování jednotky automaticky uvolněny buď elektrické zámky v dané zóně, nebo všechny elektrické zámky v objektu.

Programování řídicí jednotky je prováděno přes PC prostřednictvím rozhraní RS232 do vzdálenosti 10 metrů nebo v případě dálkového programování je nutno použít převodník z RS232 na LAN. Programovatelné vstupy na řídicí jednotce je možné využít i pro vybrané detektory poplachového zabezpečovacího systému, kdy v případě detekce vniknutí do střeženého objektu dojde k sepnutí programovatelného výstupu, které automaticky zamkne elektromagnetické zámky a aktivuje připojenou sirénu. Tímto řešením dojde ke znemožnění pohybu narušitele po objektu a činnost akustické signalizace slouží k vystrašení.



Vstupní turniket El.zámek zóna č.1 El.zámek zóna č.2 El.zámek zóna č.3

Obr. 33. Přístupový systém s adresnými hlásiči požáru

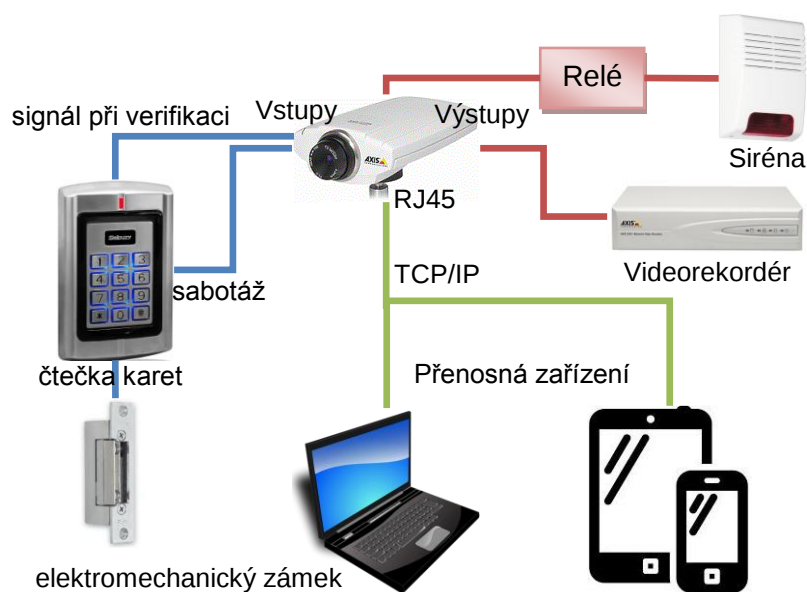
4.1.3 Integrace přístupového systému s uzavřeným kamerovým systémem

Integrace kamerových systémů s přístupovými systémy jsou v dnešní době poměrně rozšířeným a často realizovaným řešením. Kamerový systém instalovaný u přístupového místa může mít pouze informativní charakter pro administrátora přístupového místa nebo může tvořit verifikační prvek, na jehož základě se rozhodne povolit či zamítnout přístup do objektu.

Integrace přístupové systému pomocí síťové kamery AXIS 210

Pro integraci s jinými systémy je vhodná síťová kamera Axis 210 z důvodu osazení I/O vstupy pro připojení dalších aplikací (viz obr. 34). Prvním příkladem realizace přístupového systému s kamerovým systémem je připojení na vstupy síťové kamery výstupy ze čtečky přístupového systému a na výstupy kamery připojit přes relé sirénu a videorekordér sloužící k nahrávání záznamu. Kamera Axis 210 je vybavena konektorem RJ45 sloužícím pro připojení k internetu, jehož prostřednictvím je možné provádět vzdálenou kontrolu objektu.

Funkce systému je založena na verifikaci uživatele při přístupu do objektu, kdy dojde na základě naprogramování k sepnutí výstupu přístupového systému. Tento signál je přenesen přes digitální vstupy do síťové kamery, která sepne dané výstupy a začne automaticky nahrávat zvolenou sekci na videorekordér. Další vstup kamery je použit pro případ sabotáže přístupového systému, kdy v případě pokusu o překonání přístupového místa dojde k zablokování zámku a vyslání signálu prostřednictvím kamery k aktivování sirény či předání výstražné zprávy majiteli přes internet prostřednictvím protokolu TCP/IP.

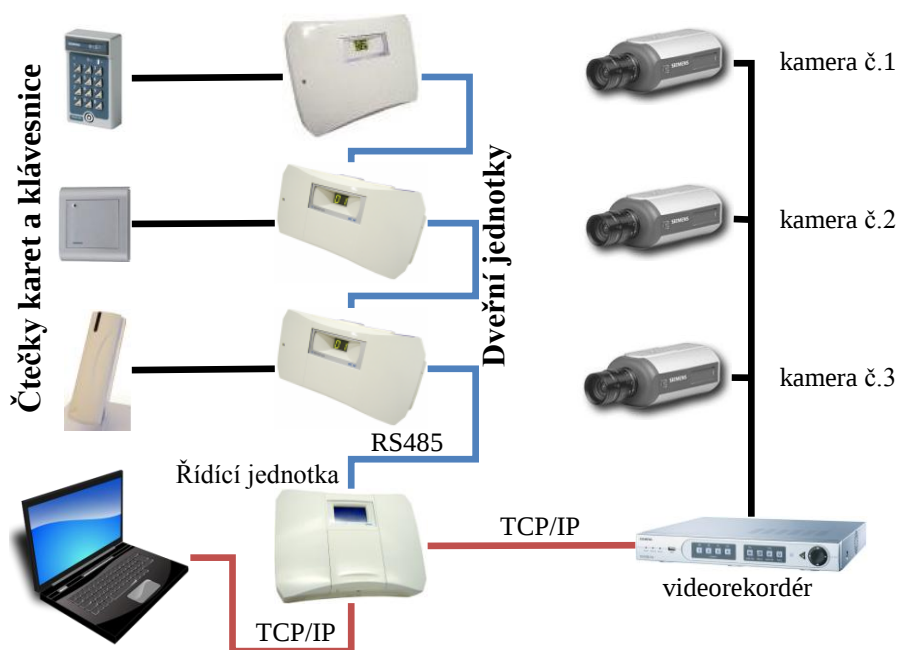


Obr. 34. Integrace přístupové systému pomocí kamery AXIS

Síťová kamera Axis 210 nabízí mnoho alternativních řešení použití vstupů a výstupů. Jedno z nich může být vybavenost kamery funkcí pohybu v obraze (motion detection), kdy na základě pohybu pachatele ve střeženém místě vyhodnotí stav narušení a může pomocí výstupů ovládat elektromechanické zámky či aktivovat výstražná zařízení.

Integrace přístupového systému s kamerovým systémem SIEMENS

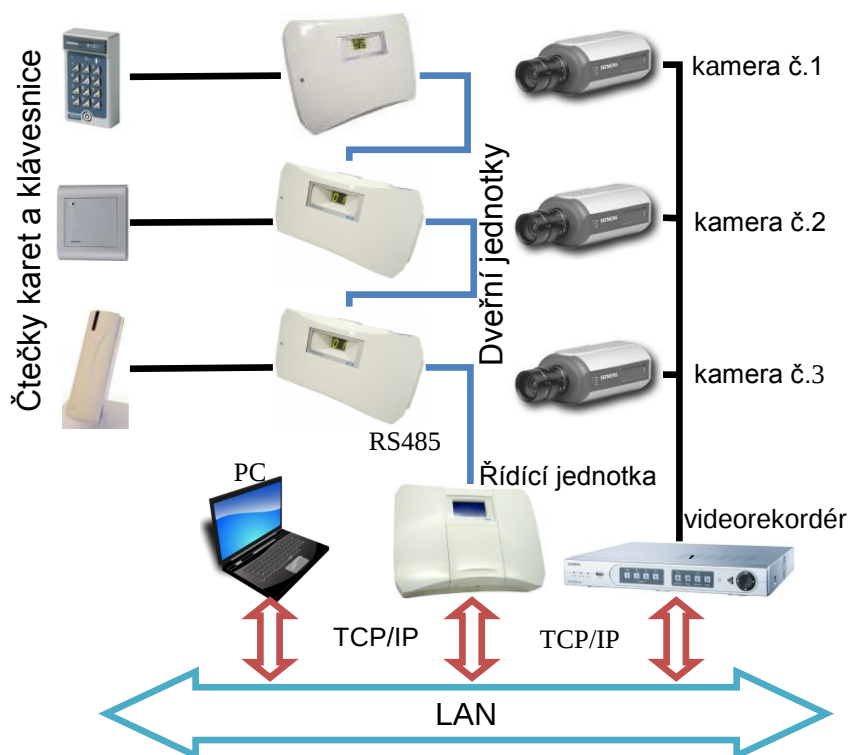
Siemens SiPass Entro umožňuje integrovat přístupový systém s kamerovým systémem prostřednictvím digitálního videorekordéru Siemens SISTORE AX. Na základě identifikace uživatele na určitém přístupovém místě, dojde v tomto místě k aktivaci kamery. Řízení celého systému je realizováno prostřednictvím řídicí jednotky Siemens SR34i, která umožňuje přímou komunikaci s digitálními záznamovými zařízeními SISTORE řad AX, CX, MX přes protokol TCP/IP. V tomto případě tvoří řídicí jednotka přístupového systému integrační prvek systému.



Obr. 35. Integrace pomocí digitálního videorekordéru Siemens

Pomocí protokolu TCP/IP je možné připojit místní nebo vzdálené PC pro správu systému a zobrazování událostí z jednotlivých kamer.

Alternativní způsob integrace pro rozsáhlejší řešení je v použití LAN jako sběrnice, na niž se připojují jednotlivé videorekordéry s kamerami a řídicí jednotky s dveřními jednotkami a jednotlivými čtečkami či klávesnicemi.



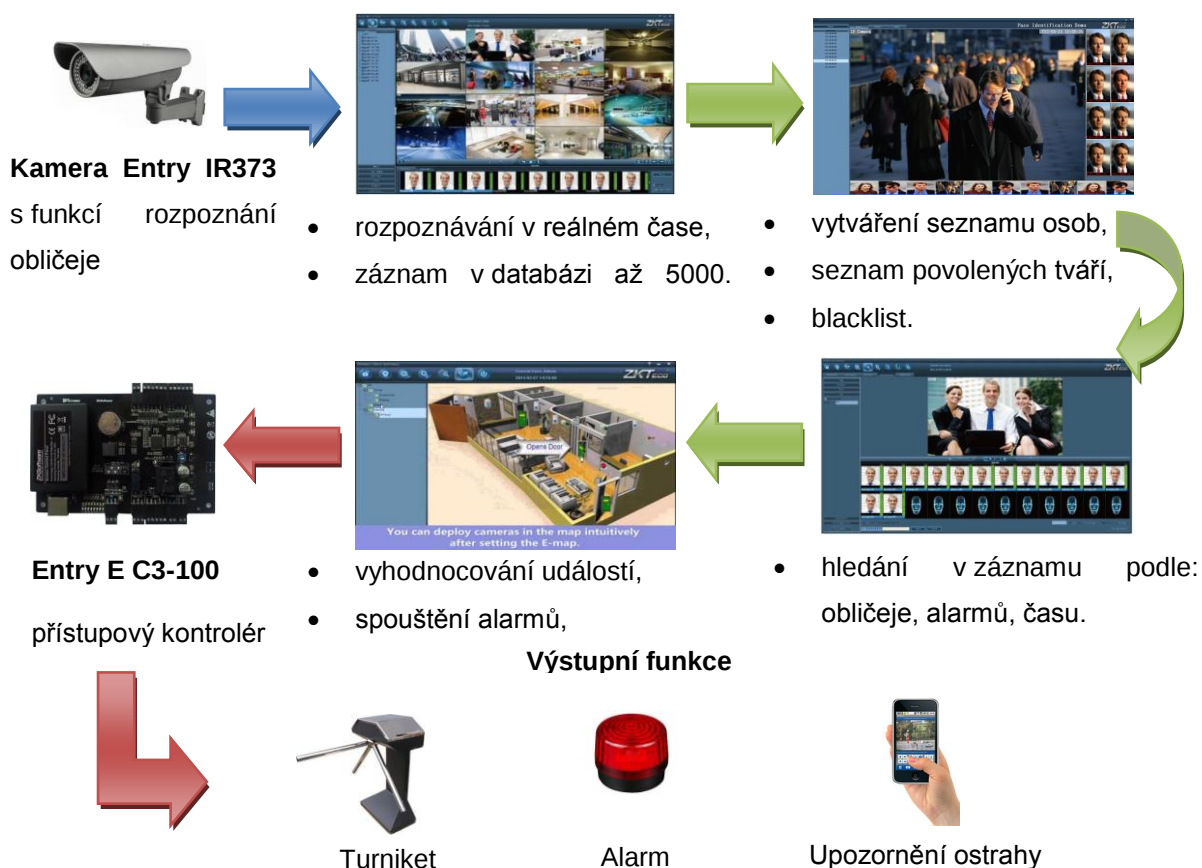
Obr. 36. Siemens SiPass Entro s využitím LAN

Aktivace přístupového systému na základě rozpoznání tváře

V rámci kamerových systémů se v současnosti stále zlepšuje inteligence zpracování obrazu. Jednou z těchto funkcí využitelnou v rámci přístupových systémů je na základě rozpoznání obličeje osoby povolit či zamítnout vstup do objektu. Takové řešení je vhodné zejména pro:

- bezdotykové otevírání dveří detekcí obličeje,
- zamezení vstupu nežádoucích osob (na blacklistu),
- upozornění pohybu nežádoucí osoby v monitorovaném sektoru,
- povolení vstupu rodičům do areálu školy, školky,
- rozpoznávání VIP zákazníků při vstupu do objektu.[22]

Základem systému je kamera Entry IR343 napájená přes síťový kabel (PoE Power of Ethernet) s integrovanou funkcí motion detection. Zpracování a detekce obličejů probíhá na softwaru ZKiVision a na jeho základě jsou přes výstupy Entry kontrolerů ovládány výstupní zařízení (dveře, brány, turnikety, alarm, odeslání upozornění ostraze).



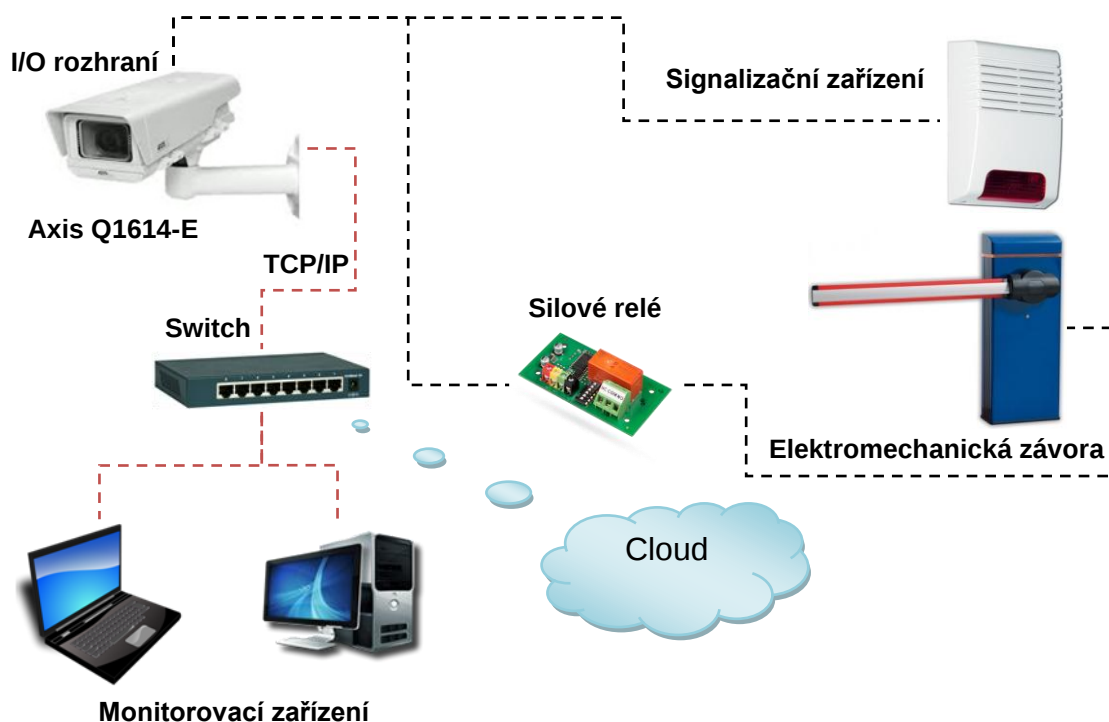
Obr. 37. Přístupový systém s funkcí rozpoznávání obličeje [22], upraveno Pavlínek, 2014

Kamerový systém Axis s aplikací počítání počtu automobilů.

U velmi frekventovaných neplacených parkovišť, kde není možné používat funkci závary pro každý automobil z důvodu zpomalování provozu a tvoření kolon je možné využít kamerový systém od firmy Axis s integrovanou aplikací počítání objektů v daném sektoru. Systém postupně počítá a odečítá automobily a udržuje si jejich aktuální počet. V případě, že dojde k zaplnění kapacity parkoviště, dojde k sepnutí výstupu kamery a k zavření závary příjezdové cesty až do okamžiku, kdy se parkovací místa uvolní.

Axis vyvíjí aplikace s inteligentními funkcemi, které lze po zakoupení snadno nainstalovat do paměti kamery. Současně do kamery může být instalována aplikace s inteligentním pohybovým detektorem schopným v nočních hodinách, kdy je prostor parkoviště pro veřejnost uzavřen, hlídat chráněný prostor a v případě narušení dojde k vyhlášení poplachu a přenosu na dohledové přijímací centrum.

Toto řešení v sobě nezahrnuje přístupový systém, ale z důvodu přehledu o počtu automobilů a použití elektromechanické závary je s ním v přímé souvislosti (viz obr. 38).



Obr. 38. Použití Axis kamery s videoanalytickými aplikacemi

Pro použití je vhodná jakákoliv venkovní síťová kamera Axis vybavena programovatelným výstupem s možností instalovat aplikace. Software s funkcí počítání prvků v obraze je vytvořen firmou Cognimatics a je plně kompatibilní s kamerami Axis.

4.1.4 Integrace přístupového systému se systémem přivolání pomoci

V současnosti není forma integrace přístupového systému se systémem přivolání pomoci rozšířená, ale pro objekty ve kterých se vyskytují starší osoby (například domovy pokojného staří) je zavedení vhodné. Systémy přivolání pomoci mimo primární funkci rychlého přivolání pomoci často nabízí sekundární funkce jako detekce úniku plynu, vody, kouře, monitoring denních aktivit, detekce vniknutí cizí osoby či připomínání odběru léků.

Princip funkce by mohl být založen na vzájemné komunikaci mezi jednotlivými centrálními jednotkami systému přivolání pomoci a řídicí jednotkou přístupového systému řídicí jednotlivé dveřní jednotky. Pro účely identifikace má každá osoba přiděleno číslo jednotky systému přivolání pomoci a přístupový bod místnosti, kterou obývá. V případě stlačení tlačítka žádosti o pomoc nebo detekci pádu osoby, dochází k detekci přibližného aktuálního místa osoby a automatickému otevření elektromechanických zámků v příslušné místnosti. V tomto případě musí mít celý objekt sofistikovaný přístupový systém umožňující sledovat pohyb dané osoby na základě paměti událostí přístupových míst.

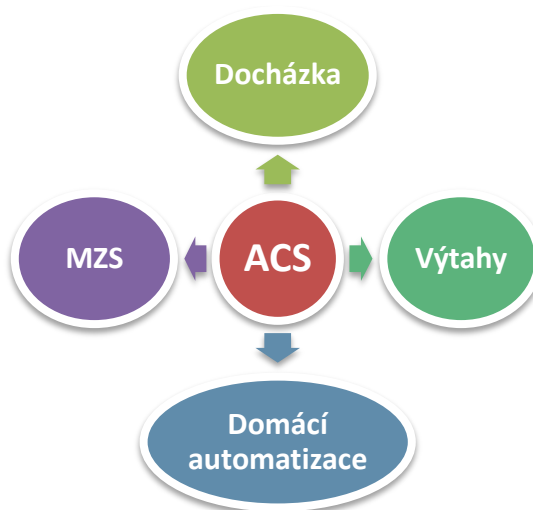
V případě úniku plynu, vody či kouře také systém přivolání pomoci předá signál přístupovému systému k otevření příslušných přístupových míst.

Z technického hlediska je nutné, aby řídicí jednotka přístupového systému byla schopná přijímat signály z jednotlivých systémů přivolání pomoci a současně přijímala signály z dveřních jednotek a na jejich základě dle definovaných pravidel ovládala příslušné elektromechanické zámky. Současně musí být přístupový systém vybaven tablem či panelem pro signalizaci místa volání o pomoc.

4.2 Integrace přístupového systému s nepoplachovými aplikacemi

V rámci integrace systémů s nepoplachovými aplikacemi dochází zejména ke zvyšování komfortu při užívání a snižování energetických a finančních nároků spojených s jejich užíváním. V případě integrace přístupového systému s nepoplachovými aplikacemi jde především o:

- docházkové systémy,
- mechanické zábranné systémy,
- výtahy,
- prvky domácí automatizace.



Obr. 39. Integrace přístupového systému
s nepoplachovými aplikacemi

4.2.1 Integrace přístupového systému s docházkovým systémem

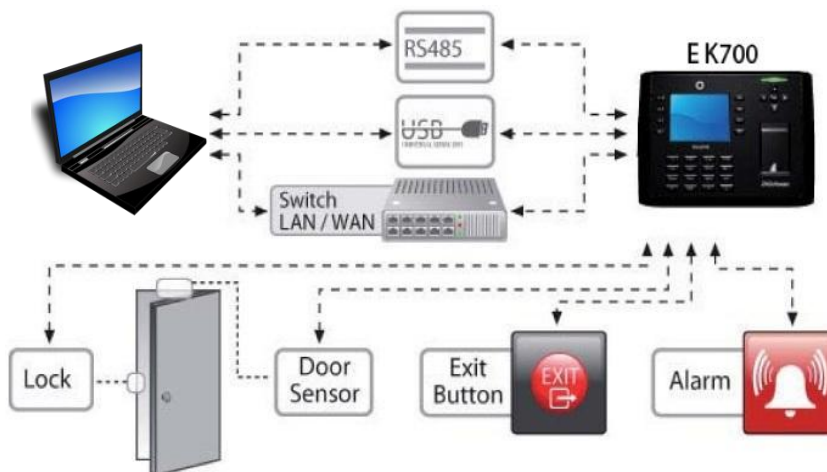
Kombinace přístupového a docházkového systému je v současnosti v rámci nepoplachových aplikací nejčastěji instalovaným integrovaným systémem zejména

v komerčních objektech, kde je nutné řídit vstup do objektu a současně evidovat a kontrolovat činnost zaměstnanců. Realizace integrovaného docházkového systému je většinou řešena pomocí docházkového terminálu připojeného na PC s nastavbovým softwarem umožňující přidávání a editace osob, zpracování docházky, přehled odpracovaných hodin zaměstnanců či kontrolu jejich přítomnosti. Prostřednictvím vstupů a výstupů terminálu jsou ovládány jednotlivé dveřní jednotky, zámky, odchodové tlačítka či alarm.

IP docházkový terminál Entry E K700

Příkladem integrace docházkového a přístupového systému je IP docházkový terminál E K700 od firmy Entry vybavený bezdotykovou RFID čtečkou se standardem EM 125 kHz a snímačem otisku prstu s kapacitou 8000 otisků. Pro dodatečné ověření osoby je v krytu terminálu zabudovaná kontrolní kamera. Vizualizační rozhraní mezi kontrolovanou osobou a terminálem tvoří 3,5" barevný TFT displej. Komunikace s PC je realizována přes TCP/IP protokol, RS 232 nebo RS 485. Integrovaný USB slot v terminálu je možné využít pro přidávání uživatelů. Funkce přístupového systému plní:

- 1x NO/NC relé zámku,
- 1x NO/NC vstupní relé dveřního senzoru,
- 1x NO/NC výstupní relé alarmu,
- 1x NO/NC vstupní relé odchodového tlačítka,
- 1x kontakt přivolání obsluhy,
- 1x WIEGAND vstup pro připojení externí RFID čtečky,
- 1x WIEGAND výstup pro připojení do přístupového kontroléru.[22]



Obr. 40. Integrovaný docházkový systém s přístupovým systémem

Docházkový terminál Entry E K700 komunikuje s nastavbovými přístupovými softwary Entry Access nebo pokročilým docházkovým softwarem Edo.

Docházkový systém Alveno s externí čtečkou otisků prstů

Propojením docházkového systému a externí čtečky na otevírání dveří vznikne nástroj pro snadnou evidenci a zpracování docházky zaměstnanců, tak i pro zabezpečení vstupu do místnosti, oddělení či jednotlivých budov. Pro otvírání dveří a docházkový systém lze využívat stejný otisk či čipovou kartu. Oba systémy jsou propojené a vzájemně kompatibilní a umožňují komunikaci s nastavbovým docházkovým softwarem Alveno, pomocí něhož lze snadno vést záznamy o průchodu jednotlivých zaměstnanců společně s evidencí docházky.



Obr. 41. Docházkový systém s externí čtečkou otisku prstů Alveno [23]

Pro zajištění zabezpečení přístupu do PC na biometrické úrovni, umožňuje systém Alveno připojení stolní čtečky otisku prstu. Docházkové čtečky se k PC připojují přes switch prostřednictvím TCP/IP protokolu. Z důvodu použití rozhraní RS485 může být vzdálenost externí čtečky otisků prstů od docházkové čtečky až 800 m. Zajištění bezporuchového chodu ve venkovním prostředí zajišťuje krytí přístroje IP 65.

Hlavní výhodou použití elektronických identifikačních systémů je v tom, že pro účely identifikace není nutné nosit klíče, u kterých je možnost vytvoření kopie a tím pádem umožněn neoprávněný přístup do střeženého objektu. [23]

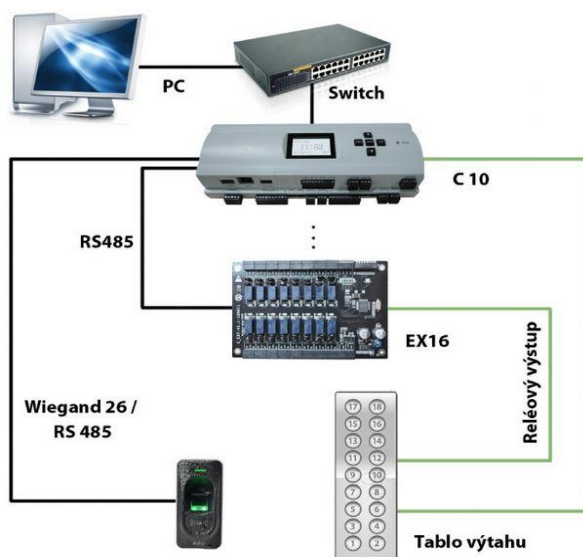
4.2.2 Integrace přístupového systému s výtahy

V objektech vybavených výtahy, u kterých je potřeba zajistit provozování pouze oprávněnými osobami je nutné integrovat přístupový prvek. Důvodem může být požadavek, aby na základě nastavených práv uživatelů došlo při identifikaci osoby k aktivaci či deaktivaci tlačítek a tím ke znemožnění přístupu do jednotlivých pater. Přístupový prvek může tvořit RFID karta či biometrický systém a může být dle požadavků umístěn před vstupem do výtahu nebo přímo ve výtahu.

IP kontroléry ovládání výtahů Entry

Základním prvkem systému je IP přístupový kontrolér ovládání výtahů Elevator C10, na který se pomocí protokolu Wiegand26 připojí biometrická či RFID čtečka. Pro ovládání volby pater slouží 10 x NO/NC relé. Pomocí rozhraní RS 485 je kontrolér propojený s rozšiřujícími moduly Elevator EX16 obsahující 16 x NO/NC relé připojené na tablo výtahu. Maximální počet rozšiřujících modulů připojitelných do přístupového kontroléru jsou 3 a je tedy schopen ovládat až 58 pater.

Nastavování a ovládání systému je realizováno softwarem ZKAccess 5.2 a fyzické propojení s PC je realizováno prostřednictvím protokolu TCP/IP přes switch.



Obr. 42. Ovládání výtahů na základě přístupového systému [22]

4.2.3 Integrace přístupového systému s prvky domácí automatizace

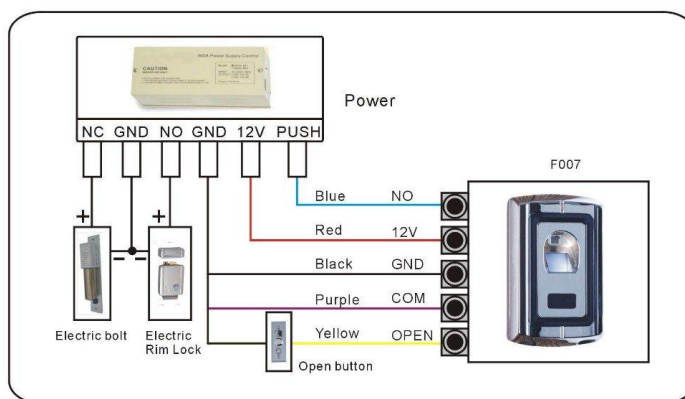
Jedním z aktuálních trendů v oblasti integrace nepoplachových aplikací je vytváření domácí automatizace, představující řídicí systém skládající se ze vzájemně propojených aplikací se společným ovládáním. Možnosti ovládání a řízení prvků domácí automatizace

se rozšiřuje a jednou z možností je zakomponovat do něj přístupový systém. Správným a efektivním řízením prvků domácí automatizace lze snižovat náklady na provoz systému při zvýšení komfortu obsluhy.

Hlavní funkce domácí automatizace jsou:

- řízení osvětlení v objektu,
- řízení topení či klimatizace,
- řízení žaluzií či rolet,
- řízení ventilace,
- řízení zavlažování,
- ovládání audio/video zařízení aj.

Nejjednodušším způsobem jak integrovat přístupový systém s prvky domácí automatizace je použití jejich vstupů a výstupů. Výhoda takového systému je v jednoduchosti zapojení a možností využít aplikace od různých výrobců (viz obr. 43). Schéma zapojení čtečky otisku prstů. Největší nevýhoda spočívá v nemožnosti nastavení složitějších vazeb a aktivačních a reakčních událostí.

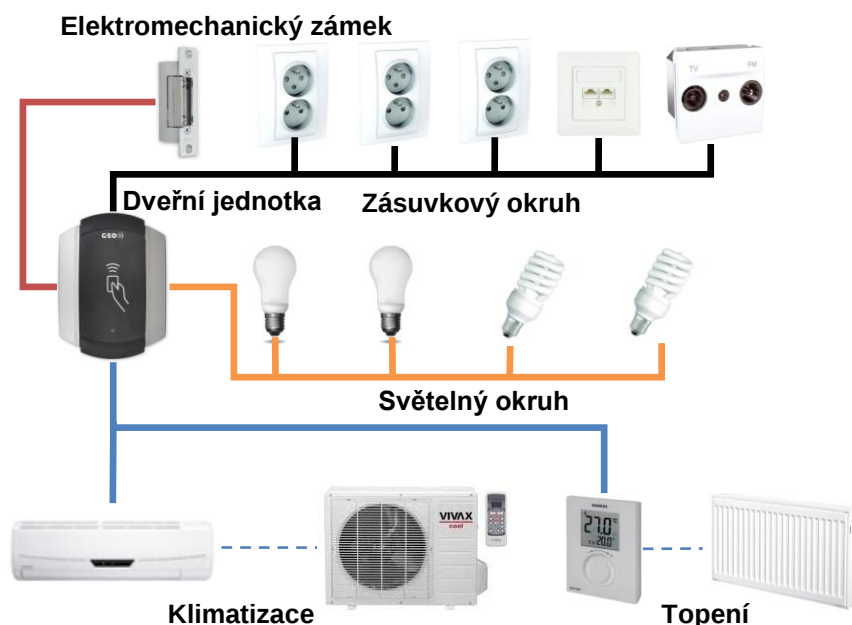


Obr. 43. Schéma zapojení čtečky otisku prstů [24]

Příklad řešení lze uvést na přístupovém systému, ve kterém na základě identifikace osoby dojde k automatickému zapnutí osvětlení, vytápění či chlazení nebo pomocí ventilačního zařízení obměnit vzduch v objektu.

Často se lze setkat s takovým řešením v hotelových apartmá se čtečkami karet. Během nepřítomnosti osob v pokoji jsou všechna světla vypnuta, ventilátory neaktivní a teplota v místnosti je konstantně udržována na specifické teplotě. V okamžiku přiložení správné identifikační karty dojde vlivem sepnutí elektromagnetického zámku k otevření dveří a současně rozsvícení světla ve vstupní místnosti do pokoje z důvodu snadné orientace.

Následně dochází k aktivaci světelných a zásuvkových okruhů v apartmá a je možné pomocí termostatu nastavovat teplotu či měnit úroveň cirkulace vzduchu.



Obr. 44. Domácí automatizace s použitím I/O

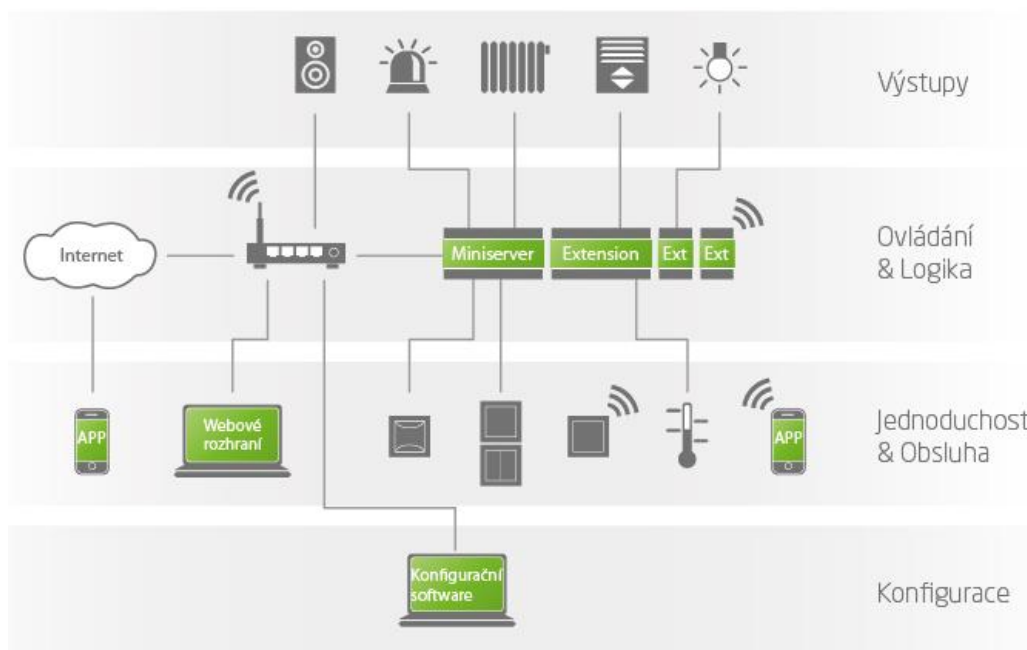
Dalším, používanějším řešením je použití centrálního serveru domácí automatizace, na který lze pomocí sběrnice připojit přístupový systém či další libovolné aplikace. Hlavními přednostmi řešení s centrálním serverem jsou snadná rozšiřitelnost, jednoduché nastavení vzájemných vazeb a velmi často vizualizační prostředí pro snadnou správu systému. Nevýhodou oproti I/O integraci (vstupně/výstupní) je poměrně vysoká cena za zavedení systému.

System domácí automatizace Loxone

Jádrem systému Loxone je miniserver tvořící centrální prvek celé domácí automatizace. Miniserver disponuje vstupem pro KNX®/EIB, Loxone sběrnici, LAN konektor a analogovými a digitálními vstupy a výstupy. Pomocí nástavbového softwaru lze nastavit vzájemné vazby mezi jednotlivými připojenými aplikacemi.

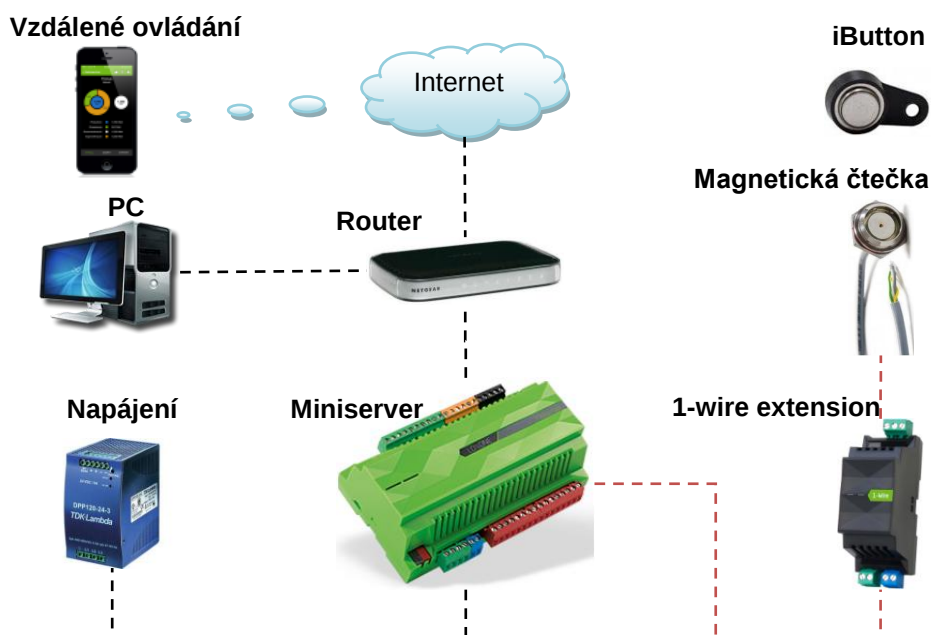
System Loxone je schopen ovládat a řídit:

- osvětlení a topení,
- stínění,
- audio či video,
- poplachové aplikace včetně **přístupového systému**. [25]



Obr. 45. Systém domácí automatizace Loxone [25]

V rámci integrace přístupového systému je nutné připojit rozšiřující modul (1-wire extension) umožňující připojit magnetickou čtečku elektronického klíče označovaného jako iButton (viz obr. 46). Jednotlivým osobám mohou být přiřazeny elektronické klíče s přidělenými právy. Na rozšiřující modul 1-wire extension lze připojit pouze jednu magnetickou čtečku elektronického klíče. V případě připojení více čteček na společný vstup není možné rozlišit jednotlivá přístupová místa. Při požadavku rozlišení jednotlivých přístupových míst je nutné použít další rozšiřující moduly.



Obr. 46. Realizace přístupového systému Loxone

Dílčí závěr

Integrace přístupových systémů je častěji realizována softwarovým způsobem zejména u sofistikovanějších objektů z důvodu snadnější instalace a následné správy systému. Komfort ovládání systému a úspora nákladů spojených s užíváním a instalací systému je charakteristickým rysem integrace s nepoplachovými aplikacemi a integrace s poplachovými aplikacemi vede ke zvyšování bezpečnosti systému.

Návrh i realizace integrovaného systému by měla být vždy v souladu s normativními požadavky. Integrovaný přístupový systém s poplachovým systémem by měl být vždy navržen tak, aby poplachový zabezpečovací systém byl ovládacím prvkem a nikoliv ovládaným. V praxi takový způsob lze nalézt u SiPass Entro od firmy Siemens, kdy čtečka karet ovládá stavy ústředny. Avšak běžně se takové řešení používá za předpokladu, že oba systémy splňují stejný stupeň zabezpečení. Pomocí tohoto řešení lze snadno eliminovat lidský faktor, kdy dojde k zapomenutí aktivace poplachového systému po odchodu z objektu.

V rámci integrace přístupového systému s elektrickou požární signalizací by mělo současně docházet k ovládání protipožárních klapek pro zamezení požáru a deaktivace vzduchotechniky, která by při špatném nastavení mohla podporovat průběh požáru.

Současnými trendy poplachových aplikací jsou zejména zamlžovací systémy a využívání umělé inteligence u zpracování snímané scény. Příkladem je aktivace přístupového systému na základě rozpoznání obličeje.

Přístupový systém s docházkovým systémem je nejčastěji realizovaným způsobem integrace. Společnost Alveno vytvořila nevšední nápad využít externí čtečku otisku prstů umístěnou před vchodovými dveřmi, která slouží jako přístupový prvek do objektu.

U objektů s vyšším stupněm rizika je možné zkombinovat řízení výtahů s přístupovým systémem, kdy na základě přidělených práv jsou osoby oprávněny přistupovat pouze do jednotlivých pater. Takovýto způsob integrace vede zejména ke zvyšování bezpečnosti střežených aktiv v objektu.

Realizace integrace přístupového systému s nepoplachovými aplikacemi pomocí programovatelných vstupů a výstupů vede u rozsáhlejších řešení ke složitému zapojení a problémovému rozšiřování aplikací. Proto se často tento problém řeší instalací centrálního prvku (serveru), na který se pomocí expanderů a přídavných zařízení připojují jednotlivé aplikace. Následná správa a rozšiřitelnost systému o další aplikace je velmi jednoduchá.

5 NÁVRH INTEGRACE PŘÍSTUPOVÉHO SYSTÉMU

Tato část diplomové práce bude věnována návrhu přístupového systému integrovaného s ostatními poplachovými a nepoplachovými aplikacemi na konkrétním objektu komerčního typu. Návrh systému upravují aplikační normy ČSN EN 50131-7, 50132-7 a 50133-7.

Všeobecným cílem etapy návrhu systému je stanovení rozsahu integrovaného poplachového systému a volba komponentů splňujících odpovídající kritéria funkčnosti, stupně zabezpečení a třídy prostředí a zpracování návrhu řešení systému.[26]

Návrh bude zpracován pro rozsáhlejší objekt obchodní společnosti pracující s kovovým materiálem a z důvodu složitosti bude použita softwarová metoda integrace řízena centrálním prvkem ve formě serverového PC. Vzájemné vztahy mezi připojenými aplikacemi budou definovány prostřednictvím nastavbového softwaru firmy VARNET INTEGRAL.

5.1 Bezpečnostní posouzení objektu

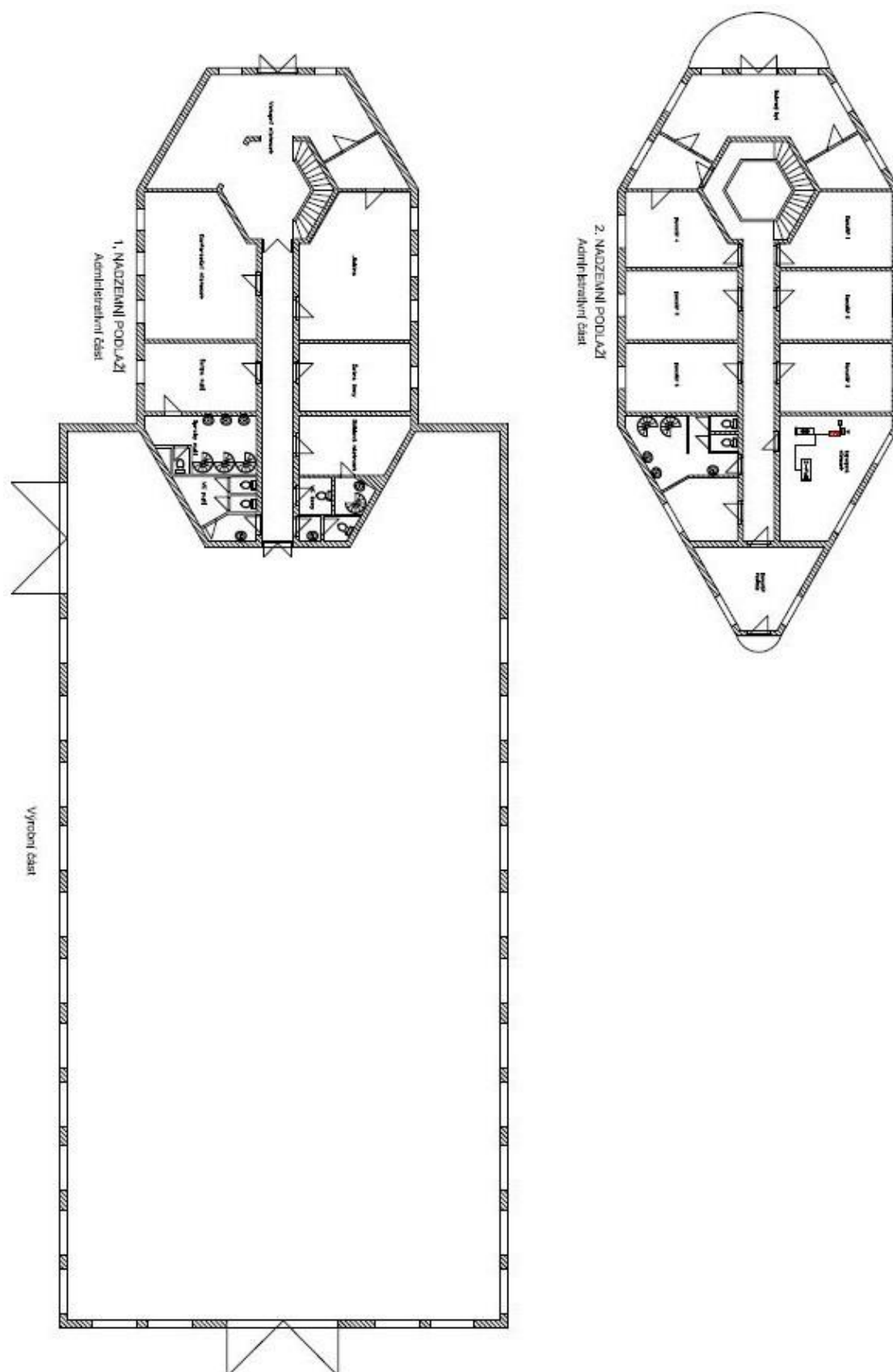
Bezpečnostní posouzení objektu vyjadřuje proces analýzy faktorů ovlivňujících návrh poplachových systémů. Hlavním cílem je zjištění a definování faktorů mající vliv na volbu komponentů a jejich umístění a na jejich základě stanovit požadovaný stupeň zabezpečení.[27]

5.1.1 Popis objektu

Zabezpečovaný objekt představuje firma RPKOVO s.r.o. Adresa objektu je Kyjovská 710, 687 09 Boršice. Firma se zabývá výrobou průmyslových filtrů pro odsávání a filtraci vzduchu z důvodu problémů spojených s čistotou ovzduší a současně i s plněním hygienických předpisů a norem.

Objekt je rozdělen na výrobní a administrativní část. Ve výrobní části je provozován vlastní proces výroby a administrativní část je rozdělena do dvou pater. Ve spodním patře je technické zázemí pro pracovníky a v horním patře se nachází kanceláře a soukromý byt vlastníka objektu.

Celkový půdorys objektu



Obr. 47. Celkový půdorys objektu

5.1.2 Analýza rizik

Analýza rizik je způsob posouzení zabezpečovaných aktiv a budovy s cílem stanovení odpovídajícího stupně zabezpečení.

5.1.2.1 Zabezpečované hodnoty

Tato část bezpečnostního posouzení je věnována zabezpečovaným aktivům nacházející se uvnitř nebo vně areálu, které mohou být ohroženy potencionálními pachateli.

Druh a hodnota majetku

V administrativní části objektu se nachází několik kusů starožitného nábytku, jehož celková cena je odhadována na 400 tisíc korun. Tento starožitný nábytek je převážně ceněným rodinným dědictvím a majitelé k němu mají velmi silný vztah. Největší část tohoto majetku je umístěna v soukromém bytě majitele objektu. V objektu se nachází také větší množství moderní elektroniky a kancelářské techniky v celkové hodnotě asi 500 tisíc korun. Jedná se dvě velkoplošné televize, 10 stolních počítačů, průmyslovou kopírku, domácí telefony, audio systém, průmyslovou pračku a vestavěnou myčku a mikrovlnou troubu. V interiéru administrativní budovy jsou umístěny dekorativní prvky v hodnotě 50 tisíc korun.

Ve výrobní části objektu se nachází zejména profesionální nářadí od firem Narex, Makita a Bosch v celkové hodnotě 350 tisíc korun. Dále deset svářecích zařízení v hodnotě 150 tisíc korun a velké množství spojovacího materiálu v ceně 200 tisíc korun. Čtyři profesionální šicí stroje v hodnotě 120 tisíc korun sloužící k výrobě filtračních tašek. V areálu se nachází i velmi drahé zařízení jako laser pro řezání kovů, ohraňovací lis či mechanické ohýbačky, jejichž odhadovaná cena je několik milionů korun, ale z hlediska jejich rozměrů, hmotnosti a složitosti odcizení nepředmětné.

V objektu se pracuje převážně s poměrně levnou ocelí, avšak často se používají i drahé kovy jako hliník, měď či nerezová ocel a v objektu je dlouhodobě skladován materiál v hodnotě 1 milion korun.

Velikost a množství majetku

U administrativní části budovy se z hlediska možného odcizení, přepravy a následného zpeněžení se jeví jako nepravděpodobnější cíle pro potenciálního pachatele moderní elektronika a kancelářská technika, zejména stolní počítače a širokoúhlé televize. Následně

dekorativní prvky ve formě obrazů či ozdobných předmětů. Jde o skladný, prostorově nenáročný, snadno přepravitelný majetek, který lze poměrně snadno zpeněžit.

Dále z výrobní části objektu z hlediska rozměrů a snadnosti odcizení je to drahé ruční nářadí, popřípadě svářečské zařízení a velké množství skladovaného nerezového materiálu a barevných kovů. Velkou hodnotou disponují zejména laser na řezání materiálu, ohraňovací a vyrážecí lisy či mechanické ohýbačky, ale především díky své vysoké hmotnosti a neskladnosti představují problém při přemísťování a přepravě, u kterých je zapotřebí speciální techniky a atraktivita jejich krádeže je výrazně nižší. U krádeže předmětů s velkými rozměry a hmotností platí, že složitost a čas k odcizení stoupá. Tento problém se vyskytuje i u vestavěných spotřebičů, kdy musí být připočítán čas na demontáž zařízení ze stálého místa.

Dům v současnosti nemá žádné střežené prostory a tedy pachatel, který bude znalý poměrů v domě, do něj může bez problémů proniknout a tedy i krást. Pouhá obhlídka objektu pachatelem mu umožní přes velké prosklené dveře nahlédnout do přízemí, kde je uloženo velké množství domácí elektroniky, zejména v obývacím pokoji. Díky situování domu lze z větší dálky přes okna vidět i do prvního patra, kde jsou také uložena velká aktiva.

V objektu ani v jeho blízkém okolí nejsou zaznamenány žádné případy krádeží či jiných trestných činů nebo závažných přestupků. Povaha majetku znemožňuje jeho zneužití proti jiným osobám či okolí.

Historie krádeží

V minulých letech nejsou známy v okolí žádné vloupání do podobných objektů, a tudíž není možné odvodit způsoby vniknutí potencionálních pachatelů.

Nebezpečnost majetku pro okolí

V objektu se nachází menší sklad barev, ředidel a jiných těkavých látek a tlakové láhve potřebné pro svařování a běh laseru. Povaha ostatního majetku v objektu není nebezpečná pro své okolí a znemožňuje jeho zneužití proti jiným osobám či okolí.

Poškození majetku

Veškerá aktiva podniku jsou umístěna uvnitř areálu, tudíž nepřipadá v úvahu jakékoliv poškození cizí osobou. Avšak budova má novou fasádu a nová plastová okna a mohla by

být poškozena vlivem vandalství, kdy by mohlo dojít k posprejování či jinému úmyslnému znečištění zdi objektu či velkých prosklených oken.

5.1.2.2 Budova

Tato část bezpečnostního posouzení je věnována objektu, ve kterém bude instalovaný zabezpečovací a tísňový systém a vyhodnocení souvisejících faktorů.

Konstrukce budovy

Hlavní obvodové zdi budovy jsou tvořeny převážně z pálených cihel s železnými výztuhami a vnitřní zdi jsou taktéž tvořeny pálenými cihlami s nižší šířkou. Pálené cihly se vyznačují vysokou mechanickou odolností a dlouhou trvanlivostí. Střecha administrativní části budovy je tvořena betonovými panely pokrytými vlnitým plechem. Střecha výrobní haly je tvořena pouze vlnitým plechem v kombinaci se zakřiveným tvrzeným lexanem. Objekt je částečně podsklepený a podlahy jsou tvořeny kvalitním litým betonem.

Otvory budovy

Design u administrativní budovy jsou navrženy tak, aby do objektu prostupovalo co nejvíce světla. Z přední a bočních částí objektu jsou prosklené vstupní dveře a několik velkých oken. V horním patře jsou přední a zadní posuvná francouzská okna sloužící pro vchod na balkón a zadní terasu.

Po pravé straně a ze zadní části výrobní haly jsou umístěny vjezdová vrata a po stranách výrobní haly je taktéž několik velkých prosklených oken. Střecha budovy je vybavena elektricky poháněnými větracími otvory.

Největším nebezpečím jsou zejména vchodové dveře z přední strany administrativní a výrobní části budovy umožňující snadný přístup do objektu a také všechny přízemní prosklené otvory. Nepravděpodobný je přístup do objektu přes francouzská okna z přední a zadní části administrativní budovy z důvodu umístění v patře objektu.

Provozní režim objektu

Ve firmě je zaveden jednosměnný provoz pro zaměstnance od 6:00 do 15:00 s hodinovou obědovou přestávkou. Personál v administrativě tvoří 10 zaměstnanců a ve výrobě je zaměstnáno 39 osob a jedna recepční. Za zajištění otvorů proti vniknutí do areálu po pracovní době zodpovídá recepční, která má povinnost zůstat jako poslední osoba v objektu.

Držitelé klíčů

Klíče od vstupních a bočních dveří má recepční, mistr výroby, ředitel a majitel firmy. Rezervní klíče jsou uloženy na hlavní budově v Praze, Dlouhá 515, PSČ 11000.

Lokalita objektu

Objekt je situován v oblasti s velmi nízkou kriminalitou a i nízkým dopravním ruchem. V blízkosti se nacházejí pouze tři spolupracující firmy zabývající se elektroinstalacemi, obráběním kovů a stolářstvím. Ve vzdálenějším okolí je pak několik hospod, restaurace a škola. Policejní stanice se nachází ve vedlejší vesnici Buchlovice vzdálené asi 3 kilometry, takže případný zásah policistů by měl být do pěti minut.

Stávající zabezpečení

V objektu je v současnosti instalovaný poměrně zastaralý zabezpečovací systém s PIR detektory. V areálu objektu jsou vnitřní kamery sloužící pouze jako dohled ředitele firmy nad zaměstnanci a venkovní kamery s malým rozlišením a bez infračerveného přísvitů umístěné před každým vstupem do objektu. Záznamy z venkovních kamer jsou ukládány na digitální videorekordér, který se automaticky po 3 dnech přemazává.

Historie krádeží a výhružek

V objektu ani v jeho blízkém okolí nejsou zaznamenány žádné případy krádeží či jiných trestných činů nebo závažných přestupků. Podnik má přátelské vztahy s obcí, pro kterou v nedávné době vyrobil několik zastávek pro veřejnou dopravu. Problém by mohl vzniknout pouze vzájemnou konkurencí okolních firem.

Místní legislativa a správní předpisy

V okolí nejsou definovány zvláštní požadavky na systém či jiné správní předpisy.

Prostředí střeženého objektu

Objekt se nachází v koncové části Boršic směrem na obec Stříbrnice s řidší výstavbou rodinných domů a leží na rovném povrchu. Vedle objektu vede pozemní komunikace č. 422 II. třídy. Z dalších stran je dům obklopen třemi výše zmíněnými firmami a rodinnými domy. Z levé části teče potok Dlouhá řeka s vysokými břehy, tudíž nehrozí nebezpečí povodně.

5.1.3 Ostatní vlivy

V následující části bezpečnostního posouzení budou rozebrány vnější a vnitřní vlivy, které mohou negativně ovlivňovat činnost jednotlivých detektorů a tím i celého integrovaného systému.

5.1.3.1 *Vlivy působící na zabezpečovací systém a mající původ uvnitř střeženého objektu*

V této podkapitole budou analyzovány faktory mající původ uvnitř střežených prostorů, které mají negativní vliv na činnost integrovaného systému. Negativní faktory pocházející zevnitř střeženého prostoru jsou většinou ovlivnitelné a cílem je pokusit se o jejich eliminaci nebo alespoň o redukci.

Vodovodní potrubí

V celém areálu je kovové vodovodní potrubí vedené převážně podlahou a nemělo by mít žádné negativní vlivy na činnost použitých detektorů poplachové zabezpečovací signalizace ani jiných zařízení.

Vytápění, vzduchotechnika a klimatizace

Vytápění administrativní budovy je realizováno prostřednictvím ústředního topení. PIR detektory v objektu by neměly být nasměrovány na tepelné zdroje. V kancelářích jsou instalované klimatizační jednotky, a tudíž by se měly brát na vědomí při instalaci detektorů poplachové zabezpečovací signalizace. Výrobní hala je vytápěna pomocí teplovzdušných jednotek a taktéž by proti nim neměly být směřovány PIR detektory.

Vývěsné štíty, závěsné předměty

V objektu jsou umístěny pouze pevně umístěné dekorativní předměty, které by neměly clonit nebo aktivovat svým náhodným pohybem detektory pohybu.

Výtahy

V objektu se nenachází žádné výtahy, ale zdrojem otřesů či vibrací může být vyřezací lis umístěný v zadní části výrobní haly.

Zdroje světla

Osvětlení v celé administrativní i výrobní části objektu je realizováno pomocí trubicových zářivek, které se vyznačují elektromagnetickým rušením, avšak z praktického hlediska při používání stávajících PIR detektorů nedocházelo k falešným poplachům.

Elektromagnetické rušení

V objektu se mohou vyskytovat zařízení, která svým elektromagnetickým rušením (interferencí) mohou negativně ovlivňovat detektory. Avšak každé elektrického zařízení, které má být uvedeno na trh, musí projít certifikací a současně testem na elektromagnetickou kompatibilitu a tudíž by nemělo svou činností negativně působit na jiná zařízení.

Vnější zvuky

V objektu se nachází několik filtrů na filtrování znečištěného vzduchu a kompresory na stlačený vzduch, které by mohly mít negativní vliv na činnost ultrazvukových detektorů.

Divoká nebo domácí zvířata

Objekt je oplocen pouze vysázenými tújemi, stromy a živým plotem a vzniká tedy riziko vzniku domácích či divokých zvířat. Ovšem z historie objektu nikdy tato situace nenastala.

Průvan

Z důvodu opatření výrobní haly několika vjezdovými vraty roste pravděpodobnost vzniku průvanu. Je tedy nutné věnovat pozornost na rozmísťování jednotlivých detektorů. Tato situace není možná v administrativní části budovy.

Uspořádání skladovaných předmětů

Tento aspekt v minulosti tvořil velký problém, protože často docházelo k zakrytí zorného pole detektorů různým kovovým materiálem.

Stavební konstrukce střežených objektů

Z důvodu kvalitně navržené a postavené budovy nemají teplotní změny žádný vliv a tento aspekt lze zcela vyloučit.

5.1.3.2 Vlivy působící na zabezpečovací systém a mající původ vně střežených objektů

Vnější vlivy na rozdíl od vnitřních jsou většinou neovlivnitelné a je nutné s nimi počítat při návrhu systému.

Dlouhodobě působící faktory

V budoucnosti se nepočítá s výstavbou ani opravou stávajících silnic ani jiných technických úprav v okolí zabezpečovaného podniku.

Krátkodobě působící faktory

V krátké budoucnosti se počítá pouze s menšími úpravami fasád sousedních domů, což však nebude mít žádný vliv na činnost integrovaného systému.

Vlivy počasí

V oblasti jižní Moravy nedochází k výrazným výkyvům počasí (silný vítr, vysoký výskyt bouřek či srážek).

Vysokofrekvenční rušení

V okolí objektu se nevyskytují žádné zdroje vysokofrekvenčního rušení, které by mohly mít negativní vliv na činnost systému a lze bez problémů instalovat i bezdrátové systémy.

Sousední objekty

V blízkosti do 50 metrů od areálu podniku nejsou postaveny žádné budovy a tudíž nemohou mít negativní vliv na činnost systému.

Vlivy klimatických podmínek

V dané lokalitě nedochází k závažným výkyvům teplot. Venkovní teploty se během roku pohybují v rozmezí přibližně -30 až 40°C.

5.2 Návrh skladby integrovaného systému kontroly vstupů

Tato část práce je věnována návrhem skladby systému integrovaného systému kontroly vstupu s dalšími poplachovými aplikacemi na modelový objekt komerčního typu. Cílem je navrhnout komplexní integrovaný systém a splnění všech požadavků definovaných zadavatelem projektu při splnění všech relevantních norem a předpisů.

5.2.1 Údaje o klientovi a střežených objektech

Zadavatelem projektu na zpracování návrhu integrovaného poplachového systému je soukromý vlastník objektu ing. Michal Novotný s bydlištěm Dlouhá 515 Praha 1 11000.

Mezi základní požadavky zákazníka bylo inovovat stávající zastaralý docházkový a zabezpečovací systém a nahradit jej integrovaným systémem složeným z **přístupového a docházkového systému, poplachového zabezpečovacího systému, kamerového systému a ovládání osvětlení a topení** v objektu, schopným nastavovat vzájemné vazby a vytvoření akčních a reakčních událostí mezi jednotlivými připojenými aplikacemi. Další významné požadavky tvoří v případě potřeby snadná rozšiřitelnost systému o další

poplachové a nepoplachové aplikace a centrální řízení a správa všech aplikací na jednom zařízení. V neposlední řadě výměna stávajících detektorů poplachového zabezpečovacího systému a vytvoření spolehlivé ochrany před potencionálními pachateli.

5.2.2 Stanovení stupně zabezpečení

Z výše provedeného bezpečnostního posouzení objektu a na základě tabulky úrovně střežení (viz obr. 49), bylo vyhodnoceno zařazení objektu do **stupně zabezpečení 2 (nízké až střední riziko)**. Tohle rozhodnutí bylo učiněno na základě potřeby střežit všechna okna, dveře a ostatní vstupy do objektu a nasazení detektorů poplachového zabezpečovacího systému v prostorech místností s vysokou pravděpodobností detekce.

Tab. 1. Tabulka úrovně střežení [27], upraveno Pavlínek, 2014

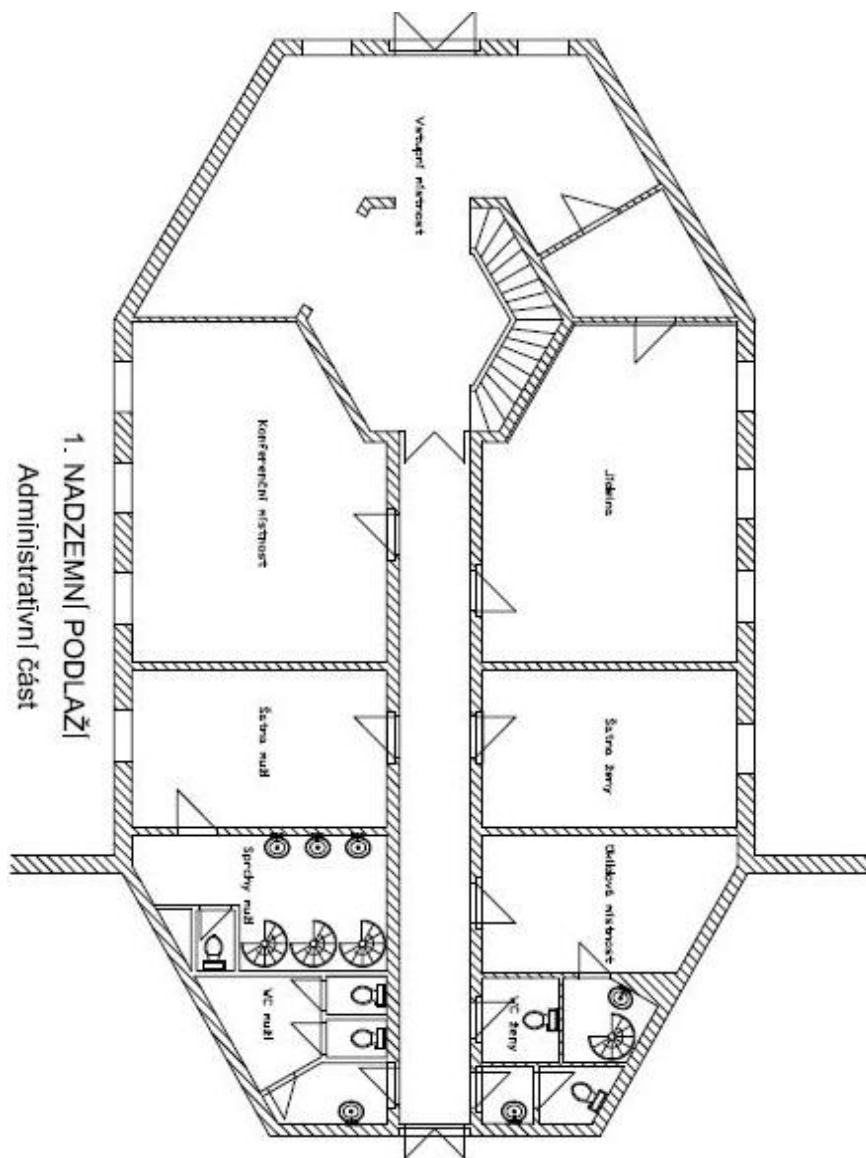
Vzít v úvahu	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Obvodové dveře	O	O	O+P	O+P
Okna		O	O+P	O+P
Ostatní otvory		O	O+P	O+P
Stěny				P
Stropy nebo střechy				P
Podlahy				P
Místnosti	T	T	T	T
Předmět (vysoké riziko)			S	S
Klíč: O = Otevření P = Průnik (tj. dohled na stavební komponenty pro detekci narušení nebo pokusu o narušení) S = Objekt vyžadující zvláštní pozornost T = Past (tj. dohled ve vybraných prostorech, v nichž je vysoká pravděpodobnost detekce)				

5.2.3 Stanovení třídy prostředí

Z důvodu toho, že administrativní i výrobní části objektu jsou stále vytápěny a jejich teplota přes letní i zimní období neklesne pod 15°C jsme zvolili pro všechny vnitřní detektory a systémy **třídu prostředí I. vnitřní**, která je definována jako vytápěné prostory, u nichž se celoročně pohybuje teplota v rozmezí 10°C až 40°C.

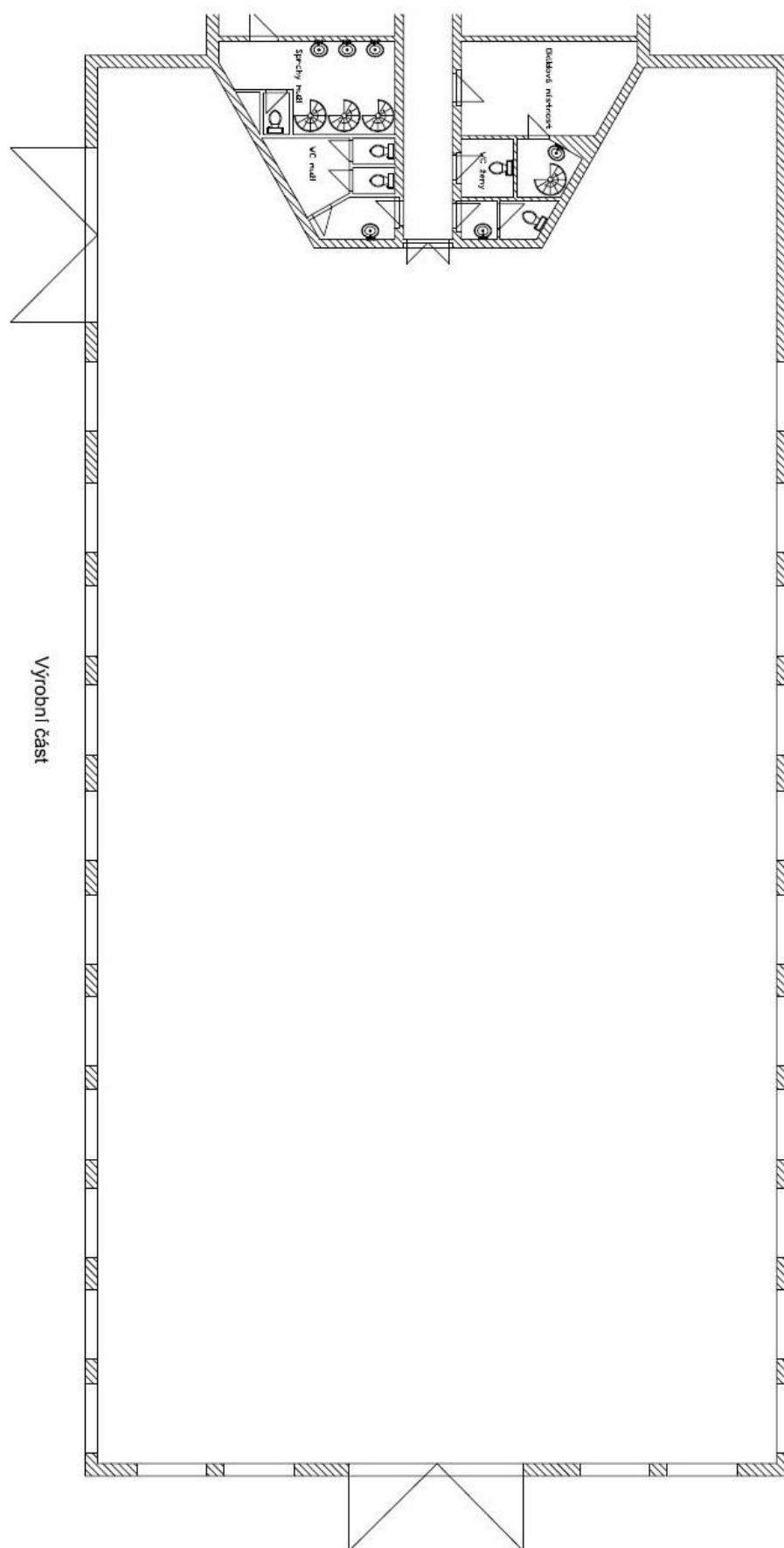
Pro venkovní kamerové systémy jsme zvolili třídu prostředí **IV. venkovní všeobecné** z důvodu celoročního vystavení povětrnostním vlivům. Teploty definované pro třídu prostředí IV. se pohybují v rozmezí -40°C v zimním období až +50°C v letním období.

5.2.4 Půdorysy objektu a popis místností

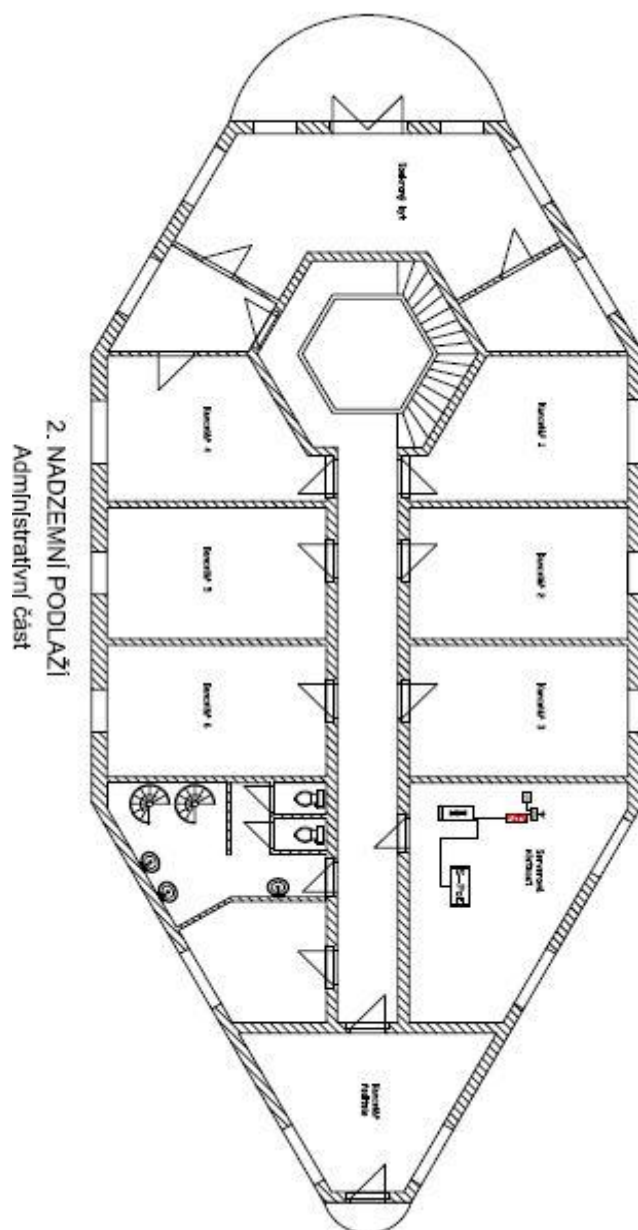


Obr. 48. První nadzemní podlaží (Administrativní část)

V prvním nadzemním podlaží administrativní části se nachází vstupní místnost, konferenční místnost, jídelna, úklidová místnost, chodba a sociální zařízení. Z chodby je přístup do výrobní haly. V druhém nadzemním podlaží administrativní budovy jsou jednotlivé kanceláře, serverová místnost, kuchyňka, kancelář ředitele společnosti, chodba, sociální zařízení a soukromý byt majitele objektu.



Obr. 49. První nadzemní podlaží (výrobní část)



Obr. 50. Druhé nadzemní podlaží (Administrativní část)

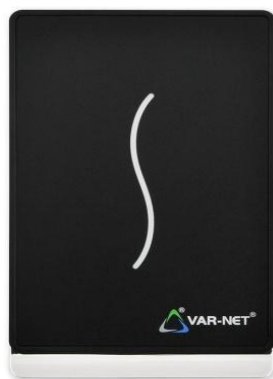
5.2.5 Přehled zařízení

Jedny z hlavních požadavků zadavatele projektu na integrovaný systém byla centrální správa a ovládání všech poplachových aplikací a snadná rozšiřitelnost systému o další prvky a aplikace. Z těchto důvodů byla vybrána softwarová metoda integrace s centrálním prvkem tvořící serverový počítač s nastavbovým softwarem VAR-NET INTEGRAL, na něž jsou připojeny prostřednictvím rozhraní další aplikace. VAR-NET INTEGRAL od firmy VARIANT s.r.o. splňuje všechny výše zmíněné požadavky a tvoří vhodné řešení pro budoucí systém. VAR-NET systém dokáže připojit až 6 typů bezpečnostních technologií.[19]

PŘÍSTUPOVÝ SYSTÉM

Přístupový terminál SCR 100

Přístupový systém umožňující kontrolu a řízení pohybu osob v objektech. Je vhodný do menších a středních firem či průmyslových budov. Maximální možný počet je 99 čteček a až 30 000 uživatelů. Propojení s PC je realizováno po sběrnici TCP/IP. Systém nemá centrální jednotku a každá čtečka pracuje samostatně. Při zajištění napájení je provoz čteček nezávislý na sběrnici, která slouží pro nastavování, programování a stahování událostí do nastavbového softwaru. Čtečka zajišťuje kompletní ovládání dveří, obsahuje relé pro otevření, vstup pro odchodové tlačítko a poplachový výstup pro případ násilného otevření dveří.



Obr. 51. SCR100[19]

Prívěšek Sebury 125 kHz

Prívěšek Sebury pracující na frekvenci 125 kHz sloužící pro přístup do jednotlivých místností v objektu



Obr. 52. Prívěšek Sebury 125 kHz[19]

Odchodové tlačítko - BT 004 EXIT

Odchodové tlačítko s NO kontakty v nerezovém kovovém provedení s piktogramem otevření dveří.



Obr. 53. Odchodové tlačítko[19]

DOCHÁZKOVÝ SYSTÉM

Docházkový terminál s kamerou – TAC 07 IDF/C

Docházkový terminál kombinující v sobě docházkový terminál a výstup pro ovládání dalšího zařízení v našem případě turniketu. Disponuje funkcí ukládání fotografií při pokusu o identifikaci a obsahuje barevný LCD pro možnost prohlížení historie. Pro snadné užívání a programování je terminál vybaven ikonovým menu a funkčními klávesnicemi. Autorizace uživatele je možná kódem, kartou, otiskem. V našem případě z důvodu zvýšení bezpečnosti půjde o kombinaci zadání přiděleného kódu a přiložení otisku prsu.



Obr. 54. Docházkový terminál TAC 07[19]

Turniket TRM 01

Jde o elektromechanický turniket určený pro napojení na zařízení pro podmíněný průchod. Lze nastavit povolení levého či pravého průchodu přímo z turniketu. Zpětný průchod může být volný nebo také podmíněný. Turniket je vybavený funkcí antipanik, kdy při výpadku napájení dojde k automatickému sklopení ramena a následnému uvolnění průchodu bez zábran. Tato funkce je vyžadována hasiči při kolaudaci objektu. Vynucené sklopení může být realizováno i vzdáleným tlačítkem, v našem případě na recepci. Turniket obsahuje

světelnou indikaci směru průchodu. Turniket bude instalovaný jako nástěnný a nemusí být doplněn o stojan. V našem případě bude povolení průchodu turniketem probíhat na základě identifikace v docházkovém terminálu. Zpětný průchod přes turniket z objektu bude volný.



Obr. 55. Turniket TRM 01[28]

POPLACHOVÝ ZABEZPEČOVACÍ A TÍSNOVÝ SYSTÉM

Ústředna IAS - Digiplex EVO 192+ BOX S-40 +TM 40 - bílá

Se systémem VAR-NET integral je plně kompatibilní pouze ústředna Digiplex EVO 192, která je však pro naše potřeby zabezpečení naprosto vyhovující a splňuje třídu zabezpečení II. nízké až střední riziko. Na ústřednu je možné připojit až 192 jednotlivých zón a rozdělit objekt na 8 samostatně ovládaných podsystémů.

Ústředna obsahuje sběrnici, na kterou je možné připojit až 254 modulů a 5 PGM výstupů, na které lze prostřednictvím silových relé připojit jiné nepoplachové systémy. Ústředna se dodává i ve výhodném setu obsahující box pro upevnění ústředny, trafo 40VA a dotykovou klávesnici TM 40. [19]



Obr. 56. Set s ústřednou EVO 192[19]

*Výpočet kapacity základního zdroje***a) Stanovení celkového odběru systému***Tab. 2. Výpočet proudových odběrů komponentů I&HAS*

Komponent	Počet	Minimální odběr	Maximální odběr
Magnetický kontakt	57	5mA	15mA
Magnetický kontakt vratový	2	5mA	15mA
PIR detektor	11	13mA	24mA
PIR detektor stropní	4	26mA	32mA
Detektor tříštění skla	26	20mA	37mA
Kouřový detektor	1	0,03mA	55mA
Tísňové tlačítko	2	2mA	6mA
Základní deska ústředny	1	100 mA	100 mA
Modul PRT 3	1	60 mA	60 mA
GSM/GPRS komunikátor	1	100 mA	450 mA
Celkový odběr		1326 mA	2916 mA

b) Stanovení typu zdroje, stupně zabezpečení a určení minimální dobu zálohování pro zadaný systém.

Zvolíme např. zdroj typu A, stupeň zabezpečení 2, kdy je stanovena doba zálohování 12h a požadavek dobíjení náhradního zdroje na 80% jeho maximální kapacity je 72h.

c) Výpočet kapacity záložního akumulátoru

$$KNZ = (T - 0,25) \cdot I_k + 0,25 \cdot I_p \quad [35]$$

$$KNZ = (12 - 0,25) \cdot 1,326 + 0,25 \cdot 2,916$$

$$\underline{KNZ = 16,31Ah}$$

Zvolíme zdroj s nejbližší vyšší kapacitou zdroje, tedy 18Ah/12V.

d) Stanovení doby napájení napájecím zdrojem

$$T = \frac{KNZ + 0,25 \cdot I_k - 0,25 \cdot I_p}{I_k}$$

$$T = \frac{18 + 0,25 \cdot 1,326 - 0,25 \cdot 2,916}{1,326}$$

$$\underline{T = 14,37h}$$

I_k	[A]	proud systému odebíraný v klidovém stavu
I_p	[A]	proud systému odebíraný v poplachovém stavu
T	[h]	doba provozu systému na náhradní zdroj (akumulátor)
KNZ	[Ah]	jmenovitá kapacita akumulátoru (náhradního zdroje)

Zvolený napájecí akumulátor – AKKU SMART 12V/18Ah

Akumulátor s napětím 12V s nominální kapacitou 18 Ah a maximálním dobíjecím proudem 6,5 A. Hmotnost akumulátoru je 6,5 kg.



Obr. 57. AKKU SMART 12V/18Ah[19]

Integrační modul - PRT3

Pro účely propojení ústředny EVO 192 a počítače se nastavbovým softwarem VAR-NET potřebným pro vzájemnou spolupráci dalších technologií v objektu je nutný integrační modul PRT3 umožňující správu stavů ústředny a její ovládání prostřednictvím speciálních příkazů a znaku ASCII/E-BUS. I přes implementaci integračního modulu je zachována integrita a uzavřenost systému jako celku. Přenos informací mezi integračním modulem s počítačem je realizován prostřednictvím sériového nebo paralelního rozhraní.[19]



Obr. 58. Integrační modul PRT3[19]

Doplňkový sběrníkový zdroj – PS 17

Doplňkový zdroj PS17 tvoří spínaný zdroj 1,7 A sloužící k posílení napětí na BUS sběrnici ústředny. Stejně jako ústředna má tento zdroj možnost připojit záložní akumulátor, který v případě výpadku napájení zajistí napájení všech připojených komponentů na

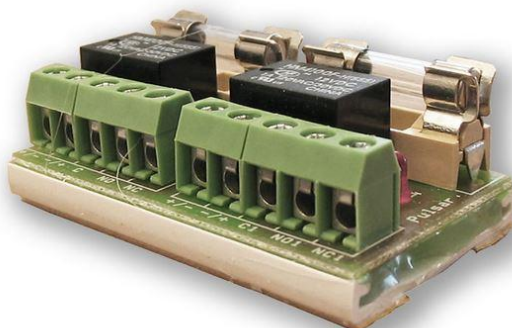
sběrnici. Zdroj PS 17 obsahuje programovatelný výstup pro ovládání přídatného zařízení. Pro instalaci je nutné zvlášť použít transformátor.



Obr. 59. Doplnkový BUS zdroj[19]

Relé pro PGM výstup – Modul PU2

Relé PU2 slouží pro posílení a galvanické oddělení dvou PGM výstupů. Modul je osazen dvěma samostatnými relé a aktivace každého relé je signalizována červenou LED diodou. Výstupní kontakt je chráněn tavnou pojistkou.



Obr. 60. Relé PU2 [19]

GSM/GPRS komunikátor – PC S250

GSM komunikátor obsahuje zabudovaný GSM modul pro ústředny Paradox v plastovém boxu. GSM komunikátor slouží k zajištění přenosu kódovaných datových formátů ústředny na PCO v hlasovém pásmu GSM nebo přes přijímač IPR512 v pásmu GPRS. Integrovaná GSM brána je schopná posílat uživateli SMS zprávy s identifikací poplachů na konkrétní zóně včetně popisů, zprávy SMS o zapnutí, vypnutí, poruchy a obnovy systému IAS. K systému je možné připojit i hlasový modul VDMP3 pro přenos hlasové zprávy o vzniku poplachu a dálkové uživatelské ovládání ústředny. Přímé připojení k ústředně lze

realizovat do vzdálenosti 2 metrů. Při požadavku připojení na větší vzdálenosti (až 300 metrů) je nutné použít modul CVT485. [19]



Obr. 61. PC S250[19]

PIR detektor – DM 50

Duální infrapasivní detektor DM 50 pracuje plně digitálním zpracováním signálu. Detektor je adresovatelný s jedinečnou adresou a připojuje se přímo na sběrnici BUS a komunikuje obousměrně s ústřednou DIGIPLEX EVO. Montážní výška detektoru je od 2 do 2,7 metru od podlahy a dokáže pokrýt prostor do vzdálenosti až 12 metrů.



Obr. 62. PIR DM 50[19]

PIR detektor stropní - DG 467 Paradome

Stropní duální infradetektor DG 467 Paradome se vyznačuje elipsovitou 360 stupňovou charakteristikou. Dokáže plně digitálně zpracovávat signály a disponuje digitální softwarovou teplotní kompenzací, softwarovou ochranu „SHIELD“ a digitálním automatickým čítačem pulsů. Vyznačuje se velmi vysokou odolností proti rádiovému rušení. Detektor má velkou plochu záběru pro různé instalační výšky se zachováním dostatečné citlivosti. [19]



Obr. 63. Stropní PIR DG467[19]

Detektor rozbití skla – DG 457 Glasstrek

Detektor tříštění skla DG 457 glasstrek je založen na snímání projevů tříštění skla (úder do skla představuje nízkofrekvenční fázi a následné tříštění skla představuje vysokofrekvenční fázi). Při splnění obou fází v určitém časovém rozmezí, dojde k vyhlášení předání poplachového signálu do ústředny. Díky této technologii je imunní vůči mnohým falešným poplachům. Detektor disponuje nastavitelnou citlivostí ve dvou stupních s dosahem 4,5 nebo 9 m. Hlídaná skleněná plocha musí být větší než 40 x 60 cm, strop musí být nižší než 5 m a místnost musí být větší než 3 x 3 m.



Obr. 64. Glasstrek 457[19]

Magnetický kontakt – ZC1

Díky adresovatelnosti tohoto typu magnetického kontaktu odpadá nutnost připojení na omezené drátové výstupy ústředny a taky složité správy systému. Sběrníkový magnetický kontakt je připojitelný přímo na BUS sběrnici ústředny. V systému DIGIplex EVO 192 je počet instalovaných magnetických kontaktů omezen na 254 modulů na sběrnici BUS ústředny.



Obr. 65. Magnetický kontakt ZC1[19]

Venkovní siréna – BELL TEC-Mini

Miniaturní venkovní zálohovaná siréna s akustickou a optickou signalizací. Zálohování je zajištěno pomocí Ni-MH akumulátoru, který je součástí dodávky. U tohoto typu sirény je oddělená signalizace reproduktoru a blikače. Blikač je v provedení LED a snese i dlouhodobý provoz. Obsahuje integrovanou záložní baterie NiMH 6 V/250 mAh



Obr. 66. Siréna BELL [19]

Tísňové tlačítko – PANIC Emergency

Tísňové tlačítko malých rozměrů v bílé barvě se stříbrnou aktivní plochou a s červeným nápisem EMERGENCY.



Obr. 67. Tísňové tlačítko – Panic Emergency[19]

Opticko kouřový detektor – FDR-26-S

Opticko-kouřový požární detektor je určen jako doplňková signalizace k systémům IAS. Pracuje na principu vniknutí kouře do vyhodnocovací komůrky, která je prosvětlována IR diodou a tento svit je zpětně vyhodnocován. Na přítomnost kouře reaguje detektor svitem LED diody a překlopením relé.[19]



Obr. 68. FDR-26-S [19]

Kabeláž PTZS – VD 04- 4x0.5/100

VD stíněný kabel typu „drát“, 4 žíly, průměr drátu 0,5 mm, pro slaboproudé rozvody EZS v balení po 100m délky, značení délky na plášti kabelu. Tento typ kabelu je použitý pro vytvoření BUS sběrnice a propojení jednotlivých komponentů I&HAS. [19]



Obr. 69. I&HAS kabeláž [19]

KAMEROVÝ SYSTÉM***Venkovní Dome kamera – ACTi E82***

ACTi E82 je venkovní IP dome kamera vybavená antivandal krytem a varifokálním objektivem s infračerveným filtrem a přísvitkem schopným osvětlit objekty až do vzdálenosti 15metrů. Kamera je vybavena kompresními formáty H.264/ MJPEG, rozlišení kamery 3Mpix (2048x1536) s frekvencí až 15 snímků/s. Kamera umožňuje dual streaming

a obsahuje funkci WDR zajišťující vysoké zlepšení obrazu za zhoršených viditelnostních podmínek. Napájení je realizováno přes Ethernet (PoE) a z důvodu krytí IP 66 je kamera vhodná i pro venkovní použití. [19]



Obr. 70. Dome kamera ACTi E82[19]

PoE switch - 8x10/100 8xPoE

Hlavní výhodou tohoto switch je napájení přes síťový kabel a odpadá nutnost přivádět napájení. Jedná se o výkonný 8 portový switch 10/100, PoE na všech 8 portech, pro napájení zařízení dle normy IEEE 802.3af (max.123W). Kompaktní kovové provedení. Výrobce uvádí spolehlivost až 190 000 hodin.



Obr. 71. PoE switch 8/8[19]

Záznamové zařízení – VS2008 PRO

Jde o záznamové zařízení přizpůsobené pro připojení 8 kamer s možností přímého připojení monitoru s Full HD (1080p) rozlišením pro zobrazování živého obrazu či následného záznamu. Umožňuje vzdálený přístup, správu a nastavení přes internetové prohlížeče, software i mobilní aplikace. Je kompatibilní se dvěma SATA disky s kapacitou až s 2 TB. Umožňuje připojení USB myši a klávesnice k ovládání. Tento typ záznamového

zařízení je vhodný z důvodu zpracování a zobrazení dat ve vysokém rozlišení. Záznamové zařízení jsme použili jako záložní zařízení z důvodu výpadku či zničení serverového PC. V takovém případě budou stále uchovány obrazové informace z kamer. Propojení se serverem je realizováno prostřednictvím TCP/IP protokolu.



Obr. 72. Záznamový systém VS-2008 PRO[19]

Pevný SATA Disk – WD RE4 2TB

pevný disk, HDD, 3.5", SATA 6Gb/s, 2TB, 7200 ot./min., 64MB cache, raid edition - disk vhodný pro nepřetržitý provoz např. servery, disková pole, dual processor technologie pro maximální výkon, Western Digital [30]



Obr. 73. WD RE 4 [29]

Kabeláž Lynx STP kabel CAT 5E venkovní PE 305m

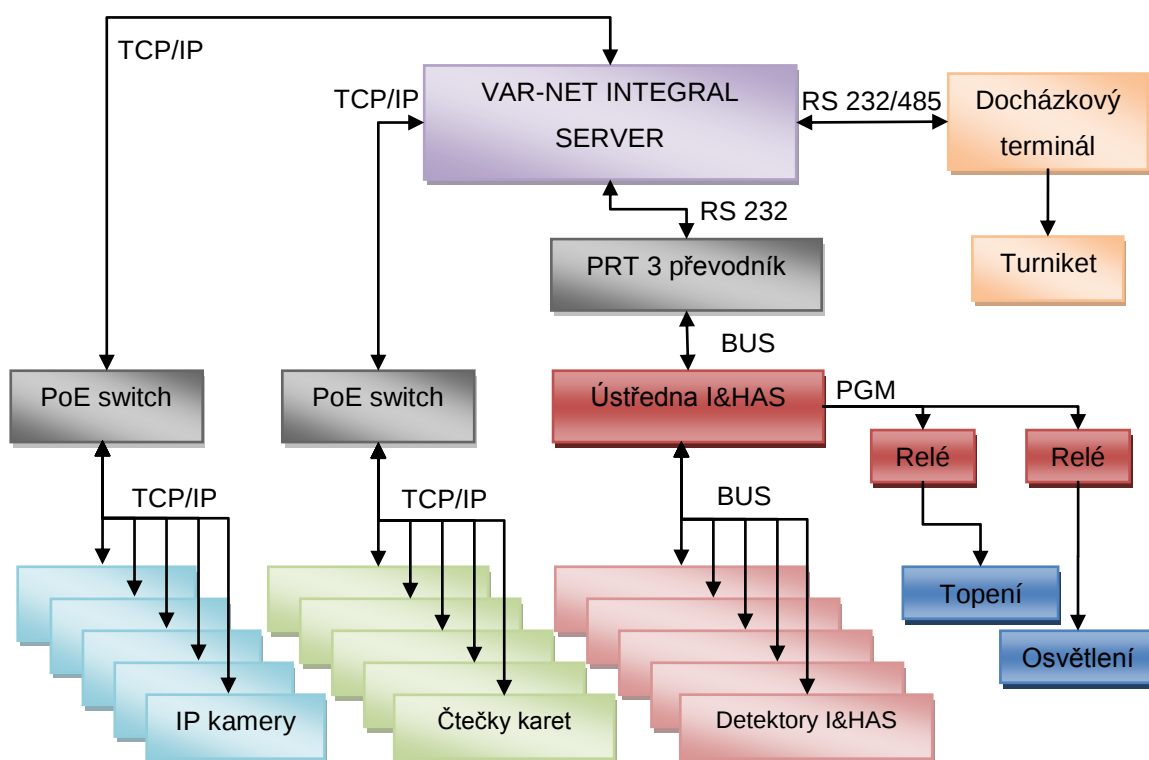
Kabel pro použití LYNX STP kategorie 5E kabel drát - venkovní provedení s PE pláštěm dvojitým. Materiál vodiče: měď 24 AWG. Materiál pláště: LDPE, tloušťka 0,5mm. Tento typ kabelu je použit pro přístupové systémy a kamerové systémy.[30]



Obr. 74. STP kabel LYNX [30]

5.2.6 Konfigurace systému

Centrální jednotku celého systému tvoří počítač s nastavbovým integračním softwarem VAR-NET. Pomocí rozhraní a speciálních modulů jsou k počítači připojeny jednotlivé aplikace. Zabezpečení výsledné vzájemné integrace jednotlivých systémů zajišťuje zmíněný software VAR-NET INTEGRAL (viz obr. 75).



Obr. 75. Schematické znázornění zapojení IPS

Čtečky přístupového systému jsou vzájemně propojeny přes TCP/IP a následně připojeny přes PoE switch k PC. Konfigurace probíhá prostřednictvím nastavbového softwaru VAR-NET docházka a přístup (licence pro 50 osob v objektu). V horním patře administrativní části objektu se nachází 9 čteček a ve spodním patře 1 čtečka SCR100 pro jednotlivé kanceláře, serverovou místnost a soukromý byt majitele objektu, které fungují nezávisle na

sobě. Každé čtečce jsou přes přístupový software přiděleny přístupová práva pro jednotlivé osoby a nastaven příslušný časový harmonogram.

Docházkový systém

Docházkový systém v sobě kombinuje i turniket, tvořící hlavní přístupový prvek do objektu. Docházkový terminál TAC 07 IDF/C je instalovaný v přední části administrativní budovy vedle recepce. Na výstup terminálu je připojen turniket TRM01, který na základě přijaté či odmítnuté autorizace terminálu povolí či zamítne přístup do dalších částí objektu. Každému zaměstnanci objektu jsou sejmuty otisky prstů a uloženy do databáze a na jejím základě jsou později porovnávány otisky prstů vstupujících osob.

Systém je nakonfigurován tak, aby zaměstnanci výrobního úseku budovy neměli přístup do jednotlivých kanceláří, serverové místnosti ani do soukromého bytu majitele. Osoby pracující v administrativní části se zapisují do docházkového systému přiložením prstu na čtečku otisku prstu a současně vlastní identifikační předmět (karta či přívěšek) pomocí kterého mají přístup do konkrétní kanceláře či serverové místnosti. Osoby zaměstnané ve výrobní části nevlastní žádný identifikační předmět a jejich identifikace probíhá pouze v rámci docházkového systému.

Kamerový systém

Kamerový systém je v objektu realizován 7 IP PoE kamerami (napájenými přes ethernet). Jednotlivé kabely od kamer jsou připojeny do PoE switchu a následně připojen k internetu nebo PC. Ke switchi je připojen přes ethernet kabel i záznamový systém VS-2008PRO umožňující zaznamenávat obraz z jednotlivých kamer na vnitřní pevné disky.

Poplachový zabezpečovací a tísňový systém

Ústředna Paradox EVO 192 umožňuje rozdělit objekt až na 8 podsystémů. V rámci tohoto projektu však bude zapotřebí pouze 4 samostatných podsystémů.

Podsystém 1 – První patro administrativní budovy

Do této části patří celkem 9 místností a chodba spodní patro, chodba horní patro (vstupní místnost s recepcí, jídelna, konferenční místnost, šatny ženy, šatny muži, sprchy ženy, sprchy muži, WC ženy, WC muži. V rámci technického zabezpečovacího vybavení zahrnuje první podsystém 12 magnetických kontaktů, 3 PIR detektory, 1 PIR detektor stropní, 5 detektorů tříštění skla, tísňové (panic) tlačítko a opticko-kouřový hlásič.

Podsystém 2 – Druhé patro administrativní budovy

Do této části objektu patří celkem 10 místností (kanceláře č.1,2,3,4,5,6 kancelář ředitele, serverová místnost, společné WC a malá kuchyňka). V rámci technického zabezpečovacího vybavení zahrnuje druhý podsystém 12 magnetických kontaktů, 8 PIR detektorů, 9 detektorů tříštění skla.

Podsystém 3 – Soukromý byt majitele objektu

Do této části objektu patří 3 místnosti (soukromý byt majitele objektu a dvě malé postranní místnosti). V rámci technického zabezpečovacího vybavení zahrnuje třetí podsystém 7 magnetických kontaktů, 1 stropní PIR detektor, 4 detektory tříštění skla a tísňové (panic) tlačítko.

Podsystém 4 – Výrobní část objektu

Do této části objektu patří pouze jedna místnost (výrobní hala). V rámci technického zabezpečovacího vybavení zahrnuje čtvrtý podsystém 26 magnetických kontaktů, 2 vratové magnetické kontakty, 8 detektorů tříštění skla a 2 stropní PIR detektory.

Tab. 2. Rozdělení objektu na podsystémy

Číslo podsystému	Místnosti	Seznam detektorů
1	Vstupní místnost, Jídelna, Konferenční místnost, Šatny ženy, Šatny muži, Šatny muži, Sprchy ženy, Sprchy muži, WC ženy, WC muži, úklidová místnost, chodba spodní patro, chodba horní patro.	12 x Magnetický kontakt 3 x PIR detektor 1 x PIR detektor stropní 5 x Detektor tříštění skla 1 x tísňové tlačítko 1 x opticko-kouřový hlásič
2	Kanceláře č.1,2,3,4,5,6, kancelář ředitele, serverová místnost, Společné WC, kuchyňka	12 x Magnetický kontakt 8 x PIR detektor 9 x Detektor tříštění skla
3	Soukromý byt majitele podniku	7 x Magnetický kontakt 1 x PIR detektor stropní 4 x Detektor tříštění skla 1 x tísňové tlačítko
4	Výrobní hala	26 x Magnetický kontakt 2 x Vratový mag. kontakt 2 x Stropní PIR detektor 8 x Detektor tříštění skla

Tab. 3. Podsystem 1 – zóny

Podsystem 1			
Číslo zóny	Místnosti	Seznam detektorů	Typ zóny
1	Vstupní místnost	3 x Magnetický kontakt 1 x PIR detektor stropní	Zpožděná
2		1 x Detektor tříštění skla	Okamžitá
3		1 x tísňové tlačítko	24 hodinová
4	Jídelna	3 x Magnetický kontakt 1 x PIR detektor 1 x Detektor tříštění skla 1 x kouřový detektor	Okamžitá
5	Šatny ženy	1 x Magnetický kontakt 1 x Detektor tříštění skla	Okamžitá
6	Chodba spodní patro	1 x Magnetický kontakt 1 x PIR detektor	Okamžitá
7	Šatny muži	1 x Magnetický kontakt 1 x Detektor tříštění skla	Okamžitá
8	Konferenční místnost	3 x Magnetický kontakt 1 x Detektor tříštění skla	Okamžitá
9	Chodba horní patro	1 x PIR detektor	Okamžitá

Tab. 4. Podsystem 2 - zóny

Podsystem 2			
Číslo zóny	Místnosti	Seznam detektorů	Typ zóny
1	Kancelář č.1	1 x Magnetický kontakt 1 x PIR detektor 1 x Detektor tříštění skla	Okamžitá
2	Kancelář č.2	1 x Magnetický kontakt 1 x PIR detektor 1 x Detektor tříštění skla	Okamžitá
3	Kancelář č.3	1 x Magnetický kontakt 1 x PIR detektor 1 x Detektor tříštění skla	Okamžitá
4	Serverová místnost	2 x Magnetický kontakt 1 x PIR detektor 1 x Detektor tříštění skla	Okamžitá
5	Kancelář ředitele	3 x Magnetický kontakt 1 x PIR detektor 1 x Detektor tříštění skla	Okamžitá
6	Kuchyňka	1 x Magnetický kontakt 1 x Detektor tříštění skla	Okamžitá
7	Kancelář č.4	1 x Magnetický kontakt 1 x PIR detektor 1 x Detektor tříštění skla	Okamžitá
8	Kancelář č.5	1 x Magnetický kontakt 1 x PIR detektor 1 x Detektor tříštění skla	Okamžitá
9	Kancelář č.6	1 x Magnetický kontakt 1 x PIR detektor 1 x Detektor tříštění skla	Okamžitá

Tab. 5. Podsystem 3 - zóny

Podsystem 3			
Číslo zóny	Místnosti	Seznam detektorů	Typ zóny
1	Soukromý byt (plášťová ochrana)	7 x Magnetický kontakt	Okamžitá
2	Soukromý byt (prostorová ochrana)	1 x PIR detektor stropní 4 x Detektor tříštění skla	Okamžitá (s funkcí STAY)
3	Soukromý byt	1 x tísňové tlačítko	24 hodinová

Tab. 6. Podsystem 4 – zóny

Podsystem 4			
Číslo zóny	Místnosti	Seznam detektorů	Typ zóny
1	Výrobní hala (levá strana)	11 x Magnetický kontakt 4 x Detektor tříštění skla	Okamžitá
2	Výrobní hala (pravá strana)	12 x Magnetický kontakt 4 x Detektor tříštění skla 1 x PIR detektor stropní	Okamžitá
3	Výrobní hala (zadní strana)	5x Magnetický kontakt 1 x PIR detektor stropní	Okamžitá

Ovládání poplachového zabezpečovacího a tísňového systému je realizované přes tablo umístěné na recepci ve vchodové místnosti. Vchodová místnost má definovaný zpožděný typ zóny na 30 sekund z důvodu času potřebného pro odstřežení systému. Nastavování a ovládání systému lze realizovat i přes PC umístěný v serverové místnosti. Recepční objektu je vždy v objektu první a jako poslední opouští objekt.

Konfigurace vzájemných vazeb mezi aplikacemi

Poplachový zabezpečovací systém je nakonfigurován tak, aby při zastřežení objektu byli přes programovatelné výstupy sepnuty relé ovládající osvětlení a topení. Při zastřežení se automaticky vypne vnitřní osvětlení a dle světelných podmínek zapne venkovní osvětlení sloužící odstrašujícím efektem a zlepšující světelné podmínky pro kamerový systém. Současně se nastaví teplota na definovanou udržovací teplotu, čímž snížíme energetické nároky budovy. V závislosti na ročním období, světelných podmínkách a venkovní teplotě při odstřežení se vypne venkovní osvětlení a teplota se automaticky nastaví na požadovanou úroveň. Ovládání jednotlivých zón podsystemu 2 poplachového zabezpečovacího systému v jednotlivých kancelářích ve druhém patře administrativní budovy je realizováno na základě přidělených práv prostřednictvím čteček karet přístupového systému. Systém je nastaven tak, že při identifikaci je automaticky odstřežena kancelář a při aktivování odchodového tlačítka je automaticky zastřežena daná

kancelář. Tímto nastavením znemožníme přístup nepovolaných osob do kanceláří a zajistíme vysokou bezpečnost.

Podsystem 3 poplachového zabezpečovacího systému má možnost být nastaven na režim STAY pomocí nastavbové aplikace iParadox v chytrém telefonu, aby byly vyřazeny z činnosti detektory prostorové ochrany a zůstaly aktivní detektory plášťové ochrany. V soukromém bytě a na recepci jsou nainstalovány tísňové tlačítka pro případ přepadení.

V rámci zabezpečovacího systému je objekt vybaven dvěma venkovními zálohovanými sirénami nasměrovanými na okolní objekty.

Kamerový systém je stále aktivní, ale při zastřežení poplachového zabezpečovacího systému bude nakonfigurován tak, aby byla aktivována funkce pohybu v obraze. Při pohybu osob okolo objektu v době zastřežení dojde k automatickému odesílání upozornění a videosekvence na vzdálené zařízení. Záznam z kamer bude uchován po dobu dvou dnů a poté bude automaticky přemazáván novým záznamem.

Docházkový systém spolu s turniketem udržuje neustále přehled o osobách nacházejících se v objektu a nedovolí zastřežit poplachový zabezpečovací systém dokud není objekt prázdný. Docházkový systém je propojený se softwarovou nástavbou zajišťující stravování a mzdový systém.

5.2.7 Cenová kalkulace

Tato podkapitola zahrnuje cenovou kalkulaci navrhovaného integrovaného poplachového systému. Cenová kalkulace je provedena pro hardwarové komponenty a zvláště pro zakoupené softwarové licence potřebné pro vzájemné propojení systémů.

Tab. 7. Cenová kalkulace za software

Výrobek	Popis	Počet kusů	Cena za kus bez DPH	Celková cena bez DPH
INTEGRAL (Jádro)	Licence k základnímu softwaru	1	5 998 Kč	5 998 Kč
INTEGRAL (CCTV)	Licence pro 10 kamer	1	5 998 Kč	5 998 Kč
INTEGRAL(Návštěvy)	Licence pro 1 recepci	1	4 198 Kč	4 198 Kč
INTEGRAL (stravování)	Licence pro stravovací modul a kalkulaci výdeje stravenek	1	7 798 Kč	7 798 Kč
VAR-NET PLUS (Docházka, přístup)	Licence pro 50 osob	1	27 598 Kč	27 598 Kč
Celkem bez DPH				51590 Kč
Celkem s DPH				61908 Kč

Tab. 8. Cenová kalkulace za hardware

Výrobek	Popis	Počet kusů	Cena za kus bez DPH	Celková cena bez DPH
Ústředna	EVO 192	1	3 239 Kč	3 239 Kč
Klávesnice	TM 40	1	3 239 Kč	3 239 Kč
Box	M40	1	899 Kč	899 Kč
Záložní zdroj	AKKU 18Ah	1	1 199 Kč	1 199 Kč
Komunikátor	PC S250	1	6 359 Kč	6 359 Kč
Doplňkový zdroj	PS 17	2	2 399 Kč	4 798 Kč
Integrační modul	PRT 3	1	4 319 Kč	4 319 Kč
Venkovní siréna	BELL-mini	2	959 Kč	1 918 Kč
Relé	PU 2	1	227 Kč	227 Kč
PIR	DM 50	11	642 Kč	7 062 Kč
Detektor tříštění skla	DG 457	26	599 Kč	15 574 Kč
PIR stropní	DG 467	4	839 Kč	3 356 Kč
Magnetický kontakt	ZC 1	59	839 Kč	49 501 Kč
Kouřový detektor	FDR 26-S	1	839 Kč	839 Kč
Tisňové tlačítko	PANIK	2	78 Kč	156 Kč
Čtečka karet	SCR 100	10	4 799 Kč	47 990 Kč
EM přívěšek	EM 125kHz	10	62 Kč	620 Kč
Odchodové tlačítko	BT 004	10	358 Kč	3 580 Kč
IP kamera	ACTi E82	7	13 990 Kč	97 930 Kč
Switch	PoE 8/8	2	4 558 Kč	9 116 Kč
Záznamové zařízení	VS 2008 PRO	1	10 798 Kč	10 798 Kč
Harddisk	WD RE 4	1	2 530 Kč	2 530 Kč
Kabel CCTV+ACS	LYNX STP	420m	3 107 Kč/300m	4349 Kč
Kabel IAS+Docházka	4x0,5/100	450m	614 Kč	2 763 Kč
Celkem bez DPH				282 361Kč
Celkem s DPH				338 833 Kč

5.2.8 Rozmístění komponentů

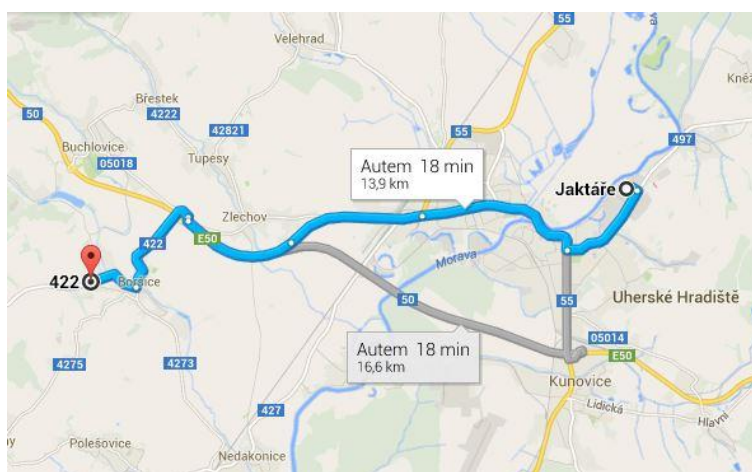
Schéma s rozmístěním komponentů je umístěné v příloze diplomové práce ve formátu PDF. Soubor umožňuje aktivaci a deaktivaci jednotlivých hladin (I&HAS, CCTV, ACS, Docházka), čímž lze snadno a přehledně zobrazit zapojení jednotlivých systémů. Součástí přílohy je i blokové schéma s podrobným zapojením ústředny Digiplex EVO 192 pro modelový objekt.

5.2.9 Hlášení poplachu

V objektu je poplach vyhlášený pouze dvěma venkovními sirénami nasměřovanými na okolní objekty. Vzdálené hlášení je realizováno prostřednictvím GSM/GPRS komunikátoru na bezpečnostní agenturu.

Pro střežení našeho objektu jsme si vybrali Soukromou bezpečnostní agenturu GAN a.s. od společnosti SYNOT. Dohledové poplachové a přijímací centrum (DPPC) firma provozuje od roku 1995. V současnosti monitoruje přes 700 objektů v regionu Uherského Hradiště. Poplachové a přijímací centrum je homologováno NBÚ a ČAP odpovídá rizikům v kategoriích objektů, jako jsou peněžní ústavy, klenotnictví atd. Hlídky nevykonávají jinou činnost, jsou tedy plně k dispozici k ostraze objektů připojených na DPPC. [31]

GAN a.s. sídlí na adrese Jaktáře 1475, 686 01 Uherské Hradiště – Mařatice vzdálené od chráněného objektu 13,9 km, což je poměrně daleko a rychlost zásahu není tak okamžitá jako v případě městské lokality.



Obr. 76. Vzdálenost DPPC od chráněného objektu[32]

Měsíční paušál za připojení střeženého objektu na DPPC je okolo 500 Kč. V případě požadavku na informování majitele v případě narušení objektu může být odesláno upozornění zvoleným osobám ve formě SMS.

5.2.10 Legislativa, normy a další předpisy

Pro navrhnuté komponenty I&HAS, CCTV, ACS aj. musí být v souladu v požadavky stanovenými v relevantních normách. Současně musí tyto systémy splňovat požadavky na zvolený stupeň zabezpečení a musí k nim být vydány prohlášení o shodě a popřípadě certifikáty.

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

Technické normy řady ČSN EN 50 131 – Poplachové systémy - Poplachové zabezpečovací a tísňové systémy,

Technické normy řady ČSN EN 50 132 – Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích,

Technické normy řady ČSN EN 50 133 – Poplachové systémy – Systémy kontroly vstupu pro použití v bezpečnostních aplikacích,

Technické normy řady ČSN EN 50 136 – Poplachové přenosové systémy a zařízení

Zákon č. 22/1997 Sb., o technických požadavcích na výrobky,

Nariadení vlády č. 616/2006 Sb., základní technické požadavky na výrobky z hlediska elektromagnetické kompatibility,

Nariadení vlády č. 17/2003 Sb., základní technické požadavky na elektrické zařízení nízkého napětí.

5.2.11 Zásah, údržba a opravy

Celý integrovaný systém bude instalovaný firmou GAN a.s. zabývající se montáží a servisem zabezpečovacích, přístupových a kamerových systémů. Na základě písemné smlouvy budou zajištěny pravidelné kontroly, servisní prohlídky systémů a případné opravy komponentů.

Intervaly pro pravidelnou kontrolu jsou stanoveny na jedenkrát za dva měsíce a servis a kompletní údržba bude probíhat v šestiměsíčních intervalech.



Obr. 77. Logo společnosti GAN a.s. [31]

Dílčí závěr

V souvislosti s požadavky zadavatele projektu na vytvoření snadno rozšiřitelného integrovaného systému složeného z poplachových aplikací a provedeného bezpečnostního posouzení objektu bylo rozhodnuto použít softwarový typ integrace od společnosti VARIANT plus, jejíž největší výhodou je snadné nastavení vzájemných vazeb bez nutnosti zasahovat do hardwarové části. Centrální jednotku a současně integrační prvek tvoří server, na něhož jsou připojeny jednotlivé systémy. V systému byly použity pouze komponenty kompatibilní s nastavbovými softwary INTEGRAL a neměly by nastat žádné problémy s jeho funkcí.

Nastavení vazeb mezi systémy závisí pouze na požadavcích klienta, ale systém je navržen tak, aby přístupový, kamerový i docházkový systém byl ve vazbě s poplachovým zabezpečovacím systémem. Přístupový systém hraje poměrně důležitou roli v integrovaném systému z důvodu ovládání jednotlivých kanceláří (zón) poplachového zabezpečovacího systému prostřednictvím jednotlivých čteček karet.

Ovládání nepoplachových aplikací (topení a osvětlení v objektu) je realizováno prostřednictvím programovatelných výstupů ústředny a přes přídatné relé.

Poplachový zabezpečovací systém je napojen na nejbližší poplachové přijímací centrum bezpečnostní firmy GAN a.s., které sídlí v Uherském Hradišti s poměrně dlouhou příjezdovou dobou. Tento aspekt by mohl být rozhodující v podnikatelském záměru pro vznik nové bezpečnostní agentury.

Společnost GAN a.s. současně provádí instalaci celého integrovaného systému a na základě písemné smlouvy následné pravidelné servisní kontroly a údržbu všech systémů.

6 NOVÉ TRENDY V OBLASTI PŘÍSTUPOVÝCH SYSTÉMŮ

V poslední kapitole diplomové práce budou rozebrány vývojové trendy z oblasti integračních technologií přístupových systémů. V současné době se zlepšujícími technologiemi jde i vývoj přístupových systémů dopředu. Požadavky ze strany zákazníků na zlepšování a inovace stále stoupají a výrobci jsou nuceni na ně odpovídat. V poslední době jsou kladeny požadavky zejména na přehledné a logické prostředí a intuitivní ovládání systémů pro místní či vzdálené ovládání. Asi nejrychleji rozvíjejícím se technologickým odvětvím, ve kterém se výrobci stále předhánají je vývoj aplikací pro ovládání systémů přes mobilní telefony či tablety.

Přístupové systémy se musí vyznačovat velmi nízkou pravděpodobností vyhlášení falešných poplachů, což je ale v dnešní době běžnou vlastností většiny systémů. Z hlediska bezpečnosti jsou současné systémy vybaveny několikanásobnou verifikací, zvyšující bezpečnost nebo slouží jako alternativní řešení při ztrátě identifikačního média. Jednou z možností přídavné verifikace je implementace miniaturní kamery do těla hlavního přístupového či docházkového terminálu snímající obličej verifikovaných osob. Na trhu se objevují i komplexní bezdrátová řešení přístupových systémů s hlavní výhodou eliminace instalačních prací kabelových vedení.

Dalším výrazným trendem současnosti je použití mobilního telefonu s technologií NFC jako identifikační a současně programovací médium přístupových systémů.

6.1 Správa přístupových systémů pomocí nástavbových softwarů

Z hlediska správy a ovládání přístupových systému integrovaných s jinými poplachovými a nepoplachovými aplikacemi se velmi často využívá serverový počítač tvořící centrální mozek celého integrovaného systému. Propojení a nastavování vazeb mezi jednotlivými aplikacemi a definování akčních a reakčních událostí probíhá prostřednictvím nástavbových softwarů. Hlavní část vždy tvoří softwarové jádro zajišťující základní funkce systému a rozšiřování pro jednotlivé aplikace (přístupové systémy, kamerové systémy, poplachové zabezpečovací systémy) se realizují dokoupení licencí. Vhodným softwarovým prvkem je zakoupení vizualizačního softwaru umožňující vytvoření půdorysu objektu a rozdělit jej na podsystémy, zóny a vytvářet značky a popisy. Vzdálený uživatelský přístup k serveru probíhá pomocí klientského programu instalovaných na klientských stanicích.

Výhodou softwarového řešení je velmi snadná implementace a rozšiřitelnost systému o další prvky či aplikace. Příkladem může být nastavbový software VAR-NET INTEGRAL od společnosti VARIANT PLUS.



Obr. 78. Typy nastavbových softwarů IPS

6.2 Vzdálené ovládání přístupových systémů pomocí mobilních aplikací

Softwarové nástavby k integrovaným systémům nebo systémům domácí automatizace umožňují vzdálenou správu, ovládání a monitoring jednotlivých technologií buď přes počítač, tablet či chytré telefony. Podmínkou je vlastnit chytrý telefon s operačním systémem Android nebo iOS (v případě zařízení Apple) a zakoupení licence nebo v případě freeware verze stáhnout z Google play nebo AppStore. Aplikace většinou nabízí intuitivní uživatelské prostředí prostřednictvím, kterého lze snadno ovládat jednotlivé poplachové i nepoplachové aplikace a mít stále přehled o situaci v objektu a stavu jednotlivých komponentů.

Jedním z příkladů tvoří systém Loxone s aplikací LOXONE APPS umožňující ovládání prvků přístupového systému a dalších poplachových a nepoplachových aplikací (viz obr. 79). Je schopný zobrazit stav přístupového systému, jednotlivých čteček a indikovat otevření jednotlivých přístupových míst a v případě instalace kamerového systému je schopen zobrazit i záběry z vybraného místa v reálném čase.



Obr. 79. Loxone APPS[25]

Dalšími tvůrci aplikací určených pro správu, řízení či monitoring jsou Inels s aplikací INNELS CONTROL či Variant plus s aplikací paradox.

6.3 Přístupový systém s technologií NFC

Technologie NFC (Near Field Communication) byla v počátku vytvořena k bezdrátové komunikaci mezi elektronickými zařízeními na velmi krátkou vzdálenost (několik centimetrů). NFC tvoří vylepšenou RFID technologii o obousměrnou komunikaci a šifrovaný přenos dat. V počátcích se tato technologie využívala pouze pro bezkontaktní platební styk, později se technologie začala implementovat do mobilních telefonů, kde sloužila jako nástroj pro rychlou výměnu dat.

V současnosti se využívá i jako identifikační prvek pro přístupové systémy zejména ve formě mobilního telefonu. Mobilní telefon s NFC technologií lze využít pro přístupové systémy dvěma způsoby.

a) Jako identifikační médium přístupového systému

Přiložením mobilního telefonu s NFC technologií s přidělenými přístupovými právy a časovým harmonogramem ke NFC čtečce přístupového systému lze ovládat jednotlivá přístupová místa objektu.

b) Jako programovací jednotka přístupového systému

Mobilní telefon s technologií NFC lze využívat i v režimu čtečka sloužící pro editaci přístupových práv a pro účely programování systému. Pro správu a editaci přístupového systému je nutná instalace příslušné mobilní aplikace.[33]

Většina aplikací pro přístupové systémy je vyvinuta pro operační systémy pro chytré telefony s operačním systémem Android nebo iOS. Bezpečnost technologie NFC je na velmi vysoké úrovni a například firma PATRONPRO vyrábí čtecí terminál certifikovaný NBÚ na stupeň IV. přísně tajné (viz obr. 80).



Obr. 80. NFC technologie u přístupových systémů [33]

6.4 Zvýšení bezpečnosti přístupových terminálů

Z důvodu obrovského počtu aktivních identifikačních médií je jejich bezpečnost velmi diskutovaným tématem. Dřívější a ještě dnes používané karty byly zabezpečeny systémem MIFARE classic, který však v současnosti není považován bezpečný. V České republice se tento zranitelný systém používal u městských karet (OpenCard), které byly snadno kopírovatelné a byla možnost uměle navyšovat stav elektronické peněženky. Později se začal používat bezpečnostní systém MIFARE PLUS (DESfire EV1, HID i class) využívající technologie kryptování AES-128 a používá bezpečnostní standardy k autentizaci, šifrování přenosu dat, kontrole integrity dat. Odhady potvrzují, že bezpečnostní standard s použitou technologií šifrování AES-128 bude odolný vůči dešifrování dalších 15 až 20 let.

V současné době se vyrábí identifikační karty s technologií MIFARE plus ale terminály pro čtení karet jsou zpětně kompatibilní i s MIFARE classic.

U většiny systémů kontroly vstupu není přenos dat přes rozhraní wiegand mezi snímačem karet a rozhraním přístupového systému nijak chráněný a proto byly vyvinuty snímače s funkcí šifrování dat založené na principu AES-128 a dekodéry komunikace umístěné v chráněném prostoru u rozhraní systému kontroly vstupu.

Oddělením spínacího členu od čtečky a jeho umístění uvnitř chráněného prostoru znemožňuje vniknutí do objektu za použití hrubé síly (rozbitím čtečky). [34]

6.5 Integrovaný přístupový systém s kamerovým systémem

Na trhu se objevují přístupové nebo docházkové systémy vybavené integrovanou kamerou v těle terminálu sloužící pro kontrolu v reálném čase administrátorem či jako další verifikační metoda sloužící pro zvýšení bezpečnosti. Další alternativou je použití externí kamery snímající obličej osoby a na základě shody s uloženými snímky je povolen či zamítnut přístup.

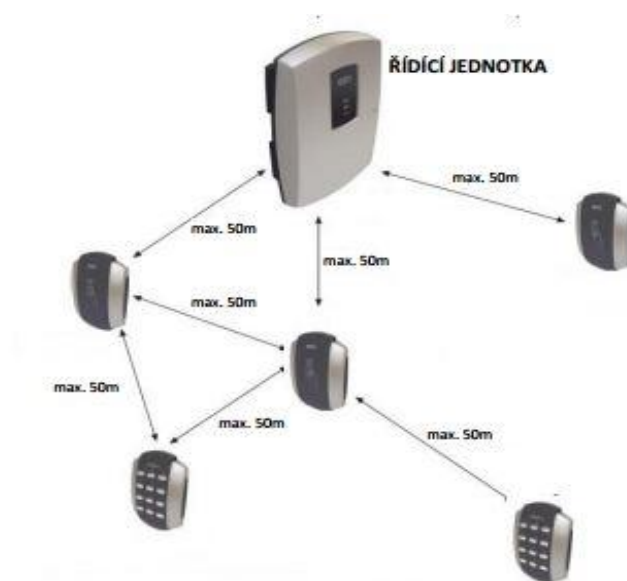
Další vývojový trend je v použití externí kamery s instalovanou aplikací sloužící pro počítání osob či automobilu a při dosažení definovaného počtu je zamítnut přístup až do odchodu dalších osob. Tímto způsobem je možné regulovat počet osob či automobilu v objektu a definovat jeho kapacitu. Realizovat systém počítání osob lze i za pomoci přídatného modulu s vestavěným ethernet portem pro připojení k webovému serveru (viz obr. 81). Modul umožňuje nastavit detekční prahy a velikosti vyhodnocovaných objektů.



Obr. 81. Externí modul pro počítání osob[14]

6.6 Bezdrátová komunikace prvků přístupového systému

V rámci implementace přístupového systému do integrovaného systému je poměrně časově a finančně náročné přivést k jednotlivým čtečkám napájecí a signálové kabely. Dalším důvodem proč použít bezdrátové komponenty přístupového systému je instalace do stávajícího zařízeného objektu, kde není možné zasahovat do jeho stěn a vybavení. Z těchto důvodů se stalo poměrně oblíbené propojení komponentů přístupového systému prostřednictvím bezdrátové technologie. Hlavní nevýhodou tvoří poměrně nízká životnost baterií, které je nutné v určitých časových intervalech vyměňovat. Většina čtecích zařízení je vybavena indikací stavu kapacity baterie a v případě nízkého stavu baterie opticky nebo akusticky signalizuje obsluhu systému.



Obr. 82. Bezdrátový přístupový systém GSD[19]

Moderní docházkové systémy mohou být vybaveny Wi-Fi modulem pro připojení k místní bezdrátové síti.

6.7 Několikanásobná verifikace osob

Jedním z hlavních faktorů vypovídající o bezpečnosti přístupových systémů je kvalita a způsob verifikace osob. Kvalita snímání se bere v potaz u biometrických přístupových systémů, kde je identifikována osoba na základě biometrických či behaviorálních znaků s určitou mírou přesnosti.

Současné biometrické čtečky mají udávaný parametr FAR (false acceptance rate) vyjadřující pravděpodobnost, že neautorizovaná osoba je považována za autorizovanou a její hodnoty jsou menší než 0,0001%. Dalším významným parametrem je FRR (false rejection rate) vyjadřující pravděpodobnost, autorizovaná osoba bude považována za neautorizovanou a systém odmítne přístup a její hodnoty jsou menší než 0,01%. FAR parametr je vázaný na bezpečnost uživatele a FRR parametr je vázaný na pohodlí uživatele. Cílem je najít ideální bod EER (equal error rate) mezi jednotlivými parametry (FAR a FRR) a vytvořit rychlý a bezpečný přístupový systém.

Další aspekt ovlivňující bezpečnost přístupových systémů je počet verifikačních metod pro přístup. Biometrické čtečky často kombinují zadání PINu s otiskem prstu či srovnání obličeje použitím integrované kamery. Platí, že čím více bude použito verifikačních metod, tím je přístupový systém bezpečnější, ale současně klesá pohodlí uživatele a prodlužuje se čas každého přístupu do objektu.

Dílčí závěr

V době stále se zlepšujících technologií a inovací se tento trend rozšířil i do bezpečnostních technologií, respektive přístupových systémů. Nejnovější sofistikované systémy mohou být vzdáleně ovládány přes počítače, notebooky či tablety. S rostoucím pokrytím světa vysokorychlostním mobilním internetem rostou i možnosti vzdáleně, z jakéhokoli místa ovládat chytrým telefonem či tabletem přístupové prvky prostřednictvím instalovaných aplikací vydávaných výrobcem systému.

S zavedením NFC systému do chytrých telefonů se naskytla možnost použít tuto technologii pro přístupové systémy. Chytrý telefon může plnit funkci služebního telefonu pro pracovní potřeby a současně může sloužit jako identifikační médium nebo konfigurační prvek přístupového systému. Tyto systémy v sobě kombinují NFC a bezkontaktní čtečky a jsou kompatibilní se staršími stávajícími systémy, kde je pouze část uživatelů vybavena NFC telefony.

Přístupové systémy přináší i bezpečnostní rizika projevující se nízkou bezpečností identifikačních médií. Dřívější systémy využívaly technologii MIFARE classic, které byly překonány a v současnosti jsou nahrazovány technologií MIFARE plus (Desfire).

Na trhu se objevují speciální moduly s kamerou schopné počítat osoby či objekty a tím regulovat kapacitu osob či objektů v objektu. Takové řešení je vhodné do objektů, kde je nutné řídit kapacitu a není nutné znát identitu osob. Alternativou je přístupový systém s kamerovým systémem umožňujícím aktivaci či deaktivaci přístupového systému na základě porovnání snímku obličeje se snímkem uloženým v databázi.

S zvýšením bezpečnosti souvisí i několikanásobná verifikace osob u přístupového terminálu, kdy je nutné použít několik metod identifikace. Často se využívá kombinace pinu a otisku prstu nebo skenování obličeje.

ZÁVĚR

Stěžejním cílem diplomové práce bylo navrhnout integrovaný přístupový systém na modelový objekt komerčního typu. Návrh systému byl zpracovaný pro objekt pracující s kovovým materiálem, u kterého bylo zpracováno podrobné bezpečnostní posouzení a následně navržen vhodný integrovaný systém.

Úvodní část je zaměřena na oblast integrovaných poplachových systémů a zhodnocení jejich výhod a nevýhod. Z kapitoly vyplývá vyšší rozšířenost softwarové metody integrace u rozsáhlejších sofistikovaných objektů a naopak realizace hardwarové metody integrace je vhodná pro menší objekty a méně rozsáhlé systémy.

V následující části následovala analýza technických požadavků na integrované a přístupové systémy. Technické požadavky tvoří pro projektanta či systémového integrátora důležité podklady potřebné pro tvorbu kvalitního projektu. Znalost technických požadavků a předpisů minimalizuje riziko neshod v projektu a současně vede k zvýšení statutu projektanta.

Následuje kapitola zaměřená na technické způsoby integrace přístupových systémů s ostatními poplachovými a nepoplachovými aplikacemi. V současnosti je v rámci poplachových aplikací nejrozšířenější integrace přístupového systému s poplachovým systémem, kde je na základě čtečky karet ovládán přístupový systém v celém objektu nebo v jednotlivých místnostech. U tohoto typu zapojení se vyskytuje častý problém v rozporu s normou. Dle normy nesmí být poplachový zabezpečovací systém ovládaným zařízením, avšak tento aspekt se v praxi toleruje v případě shodného stupně zabezpečení. Další možností integrace je využití požárních hlásičů. V případě vzniku požáru dojde k přenosu signálu na přístupový systém a automaticky jsou otevřeny všechny přístupové body.

Moderní integrované přístupové systémy s poplachovými systémy jsou vybaveny zamlžovacími systémy tvořící účinný aktivní prvek při vloupání pachatele do objektu. V rámci nepoplachových aplikací je rozšířena kombinace s docházkovým systémem, výtahovým systémem a prvky domácí automatizace. Na trhu se vyskytují výrobci jako Loxone, u kterých je celý integrovaný systém postaven na miniserveru a na něho jsou následně připojeny prvky přístupového systému.

Poslední kapitola je zaměřena na nové trendy v oblasti přístupových systémů. Nejvýznamnější inovací je vzdálené ovládání pomocí aplikací chytrých telefonů, zvýšení bezpečnosti změnou bezpečnostní technologie a několikanásobné verifikace, použití NFC

technologie v rámci přístupových systémů či použití speciálních modulů s integrovanou kamerou sloužících pro počítání osob či objektů.

Dle mého názoru se použití NFC technologie u přístupových systémů bude výrazně zvyšovat z důvodu implementace této technologie do všech novějších telefonů. Chytrý telefon může v budoucnu tedy sloužit pro pracovní potřeby, bezkontaktní platby, přenos souborů, vzdálenou správu integrovaného systému a současně jako identifikační prvek přístupového systému.

Práce může sloužit jako podklad pro výuku studentů v oblasti projektování integrovaných systémů, přehled nových trendů integrovaných přístupových systémů či jako podklad pro další rozpracování problematiky této oblasti.

ZÁVĚR V ANGLIČTINĚ

The main goal of the thesis was to create a integrated Access control system on model commercial building. The design of the system was worked out for a smaller company working with metal, within which a detailed safety assessment was made and based on that a appropriate integrated system was created.

The introductory is focused on the installation into the area of integrated alarm systems and an evaluation is done on the pros and cons. The chapter results identify the fact that software methods of integrated systems are more used in sophisticated buildings/properties, however on the other hand, the realization of hardware integrated methods are mostly used in smaller buildings/properties and less extensive systems.

The following part defines technical conditions for integrated systems and access control systems. The technical conditions create important materials for designers or system integrators to create a project of good quality. The knowledge of the technical conditions and regulations decrease the risk of disagreements in the project and together lead the increase of the designer's status.

Next, the chapter is about the technical ways of integration of access control systems with other alarm and non-alarm systems. Currently, the most widely used alarm application is the integrated check entrance system with the alarm system, where a reading card is used for controlling the whole system in the building or in separate rooms. However, this type of safety systems is usually confronted by issues with given standards. The standards state that a alarm safety system cannot be used by a controlling device, however this aspect is tolerated by a similiar level of safety precautions. Another option is an integration of the usage of fire alarms. In case of a fire, a signal is sent to the entrance system and all entrance points are automatically opened.

Modern integrated Access control systems with an alarm are equipped with fogging systems that create an active element in case of burglary. In the case of non-alarm systems, the most used combinations are with attendance systems, elevator systems and elements of household automation. The market includes producers like Loxone, whose whole integrated system is built on a miniservier and other elements of entrance systems are connected.

The last chapter discusses the new trends in the access control systems area. The most important innovation is a remote control as an application in smart phones, increase of

safety due to changes in the safety technologies and multiple verifications, usage of NFC technologies in the area of access control systems or the usage of special modules with an integrated camera, that is used for counting people or buildings.

In my opinion, the usage of NFC technologies in entrance systems shall pronouncedly increase due to the implementation of these technologies into all newer phones. In the future, the smart phone can then be used for work necessities, pay-pass, file transmission, remote management of a integrated system and currently as an identifying element of the entrance system.

Thesis can serve as a basis for teaching students in designing integrated systems, an overview of new trends in integrated access systems or as a basis for further elaboration of the problem this area.

SEZNAM POUŽITÉ LITERATURY

- [1] VALOUCH, Jan. *Projektování integrovaných systémů*. Vydání 1. Zlín: Univerzita Tomáše Bati, 2013. ISBN 978-80-7454-296-1.
- [2] 3D security system: *intruder-cctv-access control* [online]. 2014 [cit. 2014-05-04]. Dostupné z: <http://www.3dsecurity.ie/3d-security/Main/Home.htm>
- [3] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I*. Vydání 1. Zlín: VeRBuM, 316 s. ISBN 978-80-87500-05-7.
- [4] JOURA, Karel. Informační zabezpečovací komunikační technologie a systémy [online]. 2013 [cit. 2013-12-10]. Dostupné z: <http://www.joura.cz/zabezpecovaci-zarizeni/4-Zabezpecovaci-technika/8-Zamlzovaci-systemy>
- [5] WIKIPEDIE: Otevřená encyklopedie: Komfort [online]. c2013 [citováno 11. 12. 2013]. Dostupný z WWW: <http://cs.wikipedia.org/w/index.php?title=Komfort&oldid=10453650>
- [6] ČSN CLC/TS 50398. *Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky*. Praha: Český normalizační institut, 2009. 20 s. Třídící znak 33 4597
- [7] HONEYWELL [online]. 2014 [cit. 2014-05-04]. Dostupné z: http://honeywell.com/Worldwide/Pages/czech_republic-cz.aspx
- [8] EUROSAT [online]. 2014 [cit. 2014-05-04]. Dostupné z: www.eurosat.cz
- [9] JABLOTRON: Creating Alarms [online]. 2014 [cit. 2014-05-04]. Dostupné z: <http://www.jablotron.com/cz/>
- [10] AKTION [online]. 2010 [cit. 2014-05-04]. Dostupné z: <http://shop.efg.cz/>
- [11] ČSN EN 50133-1. *Poplachové systémy: Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky*. Praha: Český normalizační institut. 2001. 28 s. Třídící znak 33 4593
- [12] ČSN EN 50133-7. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace*. Praha: Český normalizační institut. 2000. 16 s. Třídící znak 33 4593
- [13] ČSN EN 50133-2-1. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 2-1: Všeobecné požadavky na komponenty*

- Praha: Český normalizační institut. 2001. 12 s. Třídící znak 33 4593
- [14] ADI global: *global distribution* [online]. 2014 [cit. 2014-05-04]. Dostupné z: <http://www.adiglobal.cz/iiWWW/cz/produkty110.nsf/wp/domu>
- [15] GM electronic: *elektronika, kterou znáte* [online]. 2014 [cit. 2014-05-04]. Dostupné z: <http://www.gme.cz/>
- [16] ELTECOM: *Domácí telefon a příslušenství* [online]. 2009 [cit. 2014-05-04]. Dostupné z: <http://www.eltecom.eu/>
- [17] ID karta: *Identifikační systémy* [online]. 2014 [cit. 2014-04-09]. Dostupné z: <http://www.id-karta.cz/aplikace-1/pristupy-a-vstupy-5/>
- [18] ACS LINE: *Elektronický identifikační systém* [online]. 2014 [cit. 2014-05-04]. Dostupné z: <http://www.acsline.cz/cs/>
- [19] VARIANT PLUS: Komplexní řešení elektronických systémů budov [online]. 2014 [cit. 2014-05-04]. Dostupné z: <http://www.variant.cz/>
- [20] SLACH, Martin. *Integrace bezpečnostních systémů*. [Prezentace]. Odborný seminář „Integrace poplachových systémů & internet věcí – pravidla, rámce, možnosti“. Pořadatel bezpečnostní portál ORSEC, Praha, Úřad pro normalizaci, metrologii a státní zkušebnictví, 10. října 2012.
- [21] ABALARM [online]. 2014 [cit. 2014-05-04]. Dostupné z: <http://www.abalarm.cz/>
- [22] ENTRY. *Přístupové a docházkové systémy*. TSS group, 2014. Katalog výrobků, 4.listy.
- [23] ALVENO. *Biometrický a docházkový systém*. Alveno, 2014. Katalog výrobků, 1.list.
- [24] DH GATE: Fast trading marketplace [online]. 2014 [cit. 2014-05-04]. Dostupné z: <http://www.dhgate.com/>
- [25] LOXONE. *Komfort&Bezpečnost: Přístupový systém* [online]. 2014 [cit. 2014-04-09]. Dostupné z: <http://www.loxone.com/cscz/chytry-dum/komfort-bezpecnost/pristupovy-system.html>
- [26] ČSN CLC/TS 50131-7. *Poplachové systémy- Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. 44 s.
- [27] VALOUCH, Jan. *Projektování bezpečnostních systémů*. [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5. 152 s.

- [28] AZP Brno [online]. 2008 [cit. 2014-05-04]. Dostupné z: <http://www.azp.cz/>
- [29] TS BOHEMIA: *Váš rodinný elektromarket* [online]. 2014 [cit. 2014-05-05]. Dostupné z: <http://interlink.tsbohemia.cz/>
- [30] HEUREKA: *Nakupte s přehledem* [online]. 2000-2014 [cit. 2014-05-05]. Dostupné z: <http://sitove-kabely.heureka.cz/>
- [31] GAN: *Bezpečnostní služba* [online]. 2013 [cit. 2014-05-05]. Dostupné z: <http://www.gan.cz/>
- [32] GOOGLE: *Google maps* [online]. 2014 [cit. 2014-05-05]. Dostupné z: <https://www.google.cz/maps/preview>
- [33] PATRON PRO: *přístupové systémy pro bytové domy* [online]. 2014 [cit. 2014-05-05]. Dostupné z: <http://www.patronpro.cz/>
- [34] ROOT: *Bezkontaktní karty Mifare DESFire prolomeny.* [online]. 2011 [cit. 2014-05-05]. Dostupné z: <http://www.root.cz/zpravicky/bezkontaktni-karty-mifare-desfire-prolomeny/>
- [35] LUKÁŠ, Luděk. *Prvky poplachových zabezpečovacích systémů: Výpočet zdroje.* Zlín, 2012.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Access Control System – Systém kontroly vstupu
AES	Advanced Encryption Standard – Pokročilý šifrovací standard
APAS	Ovládací prvky a senzory místa přístupu
ASF	Alarm Status Feedback – Signálová zpětná vazba
BUS	Mezinárodní označení pro sběrnici
CCF	Central Control Facility - Centrální ovládací zařízení
CCTV	Closed Circuit Television - Uzavřený kamerový systém
CLC/TS	Technická specifikace převzatá z CEN/CENELEC
ČAP	Česká asociace pojišťoven
ČSN	Česká technická norma
EER	Equal Error Rate - Stejná míra chyb
EMC	Electromagnetics Compatibility - Elektromagnetická kompatibilita
EMI	Electromagnetics Interference - Elektromagnetická interference
EMS	Electromagnetics Susceptibility - Elektromagnetická susceptibilita
EPS	Elektrická požární signalizace
FAR	False Acceptance Rate - Falešná míra přijetí
FRR	False Rejection Rate - Chybné odmítnutí
GPRS	Global system for mobile communication - Globální systém pro mobilní komunikaci
GSM	General Packet Radio System - Hlavní datová rádiová služba
I&HAS	Intruder and Hold-up Alarm System - Poplachový zabezpečovací a tísňový systém
I/O	Input/Output – Vstup/výstup
IEEE	Institute of Electrical and Electronics Engineers - Standard pro bezdrátové sítě
IP	Internet Protocol – Protokol internetu

IPS	Integrovaný poplachový systém.
KNX	Konnex Bus – standard evropské elektroinstalační sběrnice
LAN	Local Area Network – Lokální síť
LED	Light Emmiting Diode - Světlo emitující dioda.
LTE	Long-Term Evolution - Čtvrtá generace mobilního datového přenosu
NBÚ	Národní bezpečnostní úřad
NFC	Near Field Communication - Standard pro bezdrátovou komunikaci na krátkou vzdálenost
PGM	Programmable Output – Programovatelný výstup
PIN	Personal Identification Number - Osobní identifikační číslo
PIR	Passive Infrared Detector - Pasivní infračervený detektor
PLC	Programmable Logic Controler - Programovatelný logický automat
PoE	Power Over Ethernet - Napájení přes Ethernet
RFID	Radio Frequency Identification - Rádiofrekvenční identifikační systém
SAS	Social Alarm System - Systém přivolání pomoci
SFS	Security Fog System - Bezpečnostní zamlžovací systém
SMS	Short Message Service – Krátká textová zpráva
STP	Shield Twisted Pair - Stíněná kroucená dvojlinka
TCP/IP	Transmission Control Protocol/Internet Protocol – Řídící přenosový protokol/ protokol internetu
TFT	Thin Film Transistor – Tenkovrstvý tranzistor
USB	Universal Serial Bus – Univerzální rozhraní
WIFI	Wireless Fidelity - Bezdrátová lokální síť
3G	3rd Generation - Třetí generace mobilního datového přenosu

SEZNAM OBRÁZKŮ

<i>Obr. 1. Integrovaný poplachový systém [2]</i>	12
<i>Obr. 2. Poplachové aplikace</i>	13
<i>Obr. 3. Nepoplachové aplikace</i>	15
<i>Obr. 4. Nejčastější požadavky klientů</i>	16
<i>Obr. 5. Nevýhody IPS</i>	18
<i>Obr. 6. Schematické znázornění elektromagnetické kompatibility</i>	19
<i>Obr. 7. Schéma aktivačních a reakčních událostí</i>	20
<i>Obr. 8. Modelové schéma softwarové integrace</i>	21
<i>Obr. 9. Funkce softwarových produktů</i>	22
<i>Obr. 10. Způsoby hardwarové integrace</i>	23
<i>Obr. 11. Integrace IN/OUT</i>	24
<i>Obr. 12. I&HAS jako integrační prvek</i>	24
<i>Obr. 13. Automatizační systém jako integrační prvek</i>	25
<i>Obr. 14. Poplachová aplikace jako integrační prvek</i>	25
<i>Obr. 15. Příklad konfigurace 1 s CCF třídy 1 [6], upravil Pavlínek, 2014</i>	28
<i>Obr. 16. Konfigurace typu 2 [6], upravil Pavlínek, 2014</i>	29
<i>Obr. 17. LED přehledové tablo Honeywell [7]</i>	30
<i>Obr. 18. Provozní kniha Eurosat [8]</i>	32
<i>Obr. 19. RFID karta [9]</i>	33
<i>Obr. 20. Přístupový a docházkový terminál [10]</i>	34
<i>Obr. 21. Kryt se skrytým kabelovým průchodem [14]</i>	38
<i>Obr. 22. Záložní napájecí zdroj [15]</i>	39
<i>Obr. 23. Popis USB/RS 485 převodníku [16]</i>	39
<i>Obr. 24. Globální struktura přístupového systému [18]</i>	43
<i>Obr. 25. Integrace přístupového systému s poplachovými aplikacemi</i>	43
<i>Obr. 26. Softwarové řešení integrace VAR-NET INTEGRAL [19]</i>	44
<i>Obr. 27. Schéma integrace přístupového systému s I&HAS</i>	45
<i>Obr. 28. Integrace přístupového systému s IAS [20]</i>	46
<i>Obr. 29. Zamlžovací systémy [21]</i>	47
<i>Obr. 30. Integrovaný přístupový systém se zamlžovacím systémem</i>	47
<i>Obr. 31. Přístupový systém s neadresnými hlásiči</i>	48
<i>Obr. 32. Bezdrátový přístupový systém GDS [19]</i>	49

<i>Obr. 33. Přístupový systém s adresnými hlásiči požáru</i>	50
<i>Obr. 34. Integrace přístupové systému pomocí kamery AXIS</i>	51
<i>Obr. 35. Integrace pomocí digitálního videorekordéru Siemens.....</i>	52
<i>Obr. 36. Siemens SiPass Entro s využitím LAN.....</i>	53
<i>Obr. 37. Přístupový systém s funkcí rozpoznávání obličeje [22], upraveno Pavlínek, 2014.....</i>	54
<i>Obr. 38. Použití Axis kamery s videoanalytickými aplikacemi</i>	55
<i>Obr. 39. Integrace přístupového systému</i>	56
<i>Obr. 40. Integrovaný docházkový systém s přístupovým systémem.....</i>	57
<i>Obr. 41. Docházkový systém s externí čtečkou otisku prstů Alveno [23]</i>	58
<i>Obr. 42. Ovládání výtahů na základě přístupového systému [22].....</i>	59
<i>Obr. 43. Schéma zapojení čtečky otisku prstů [24]</i>	60
<i>Obr. 44. Domácí automatizace s použitím I/O</i>	61
<i>Obr. 45. Systém domácí automatizace Loxone [25]</i>	62
<i>Obr. 46. Realizace přístupového systému Loxone</i>	62
<i>Obr. 47. Celkový půdorys objektu</i>	65
<i>Obr. 48. První nadzemní podlaží (Administrativní část)</i>	74
<i>Obr. 49. První nadzemní podlaží (výrobní část).....</i>	75
<i>Obr. 50. Druhé nadzemní podlaží (Administrativní část).....</i>	76
<i>Obr. 51. SCR100[19]</i>	77
<i>Obr. 52. Přívěšek Sebury 125 kHz[19]</i>	77
<i>Obr. 53. Odchodové tlačítko[19]</i>	78
<i>Obr. 54. Docházkový terminál TAC 07[19]</i>	78
<i>Obr. 55. Turniket TRM 01[28]</i>	79
<i>Obr. 56. Set s ústřednou EVO 192[19]</i>	79
<i>Obr. 57. AKKU SMART 12V/18Ah[19]</i>	81
<i>Obr. 58. Integrační modul PRT3[19]</i>	81
<i>Obr. 59. Doplnkový BUS zdroj[19]</i>	82
<i>Obr. 60. Relé PU2 [19]</i>	82
<i>Obr. 61. PC S250[19]</i>	83
<i>Obr. 62. PIR DM 50[19]</i>	83
<i>Obr. 63. Stropní PIR DG467[19]</i>	84
<i>Obr. 64. Glasstrek 457[19].....</i>	84
<i>Obr. 65. Magnetický kontakt ZC1[19]</i>	85

<i>Obr. 66. Siréna BELL [19]</i>	<i>85</i>
<i>Obr. 67. Tísňové tlačítko – Panic Emergency[19]</i>	<i>85</i>
<i>Obr. 68. FDR-26-S [19]</i>	<i>86</i>
<i>Obr. 69. I&HAS kabeláž [19]</i>	<i>86</i>
<i>Obr. 70. Dome kamera ACTi E82[19]</i>	<i>87</i>
<i>Obr. 71. PoE switch 8/8[19]</i>	<i>87</i>
<i>Obr. 72. Záznamový systém VS-2008 PRO[19]</i>	<i>88</i>
<i>Obr. 73. WD RE 4 [29]</i>	<i>88</i>
<i>Obr. 74. STP kabel LYNX [30]</i>	<i>89</i>
<i>Obr. 75. Schematické znázornění zapojení IPS</i>	<i>89</i>
<i>Obr. 76. Vzdálenost DPPC od chráněného objektu[32]</i>	<i>96</i>
<i>Obr. 77. Logo společnosti GAN a.s. [31]</i>	<i>97</i>
<i>Obr. 78. Typy nastavbových softwarů IPS.....</i>	<i>100</i>
<i>Obr. 79. Loxone APPS[25]</i>	<i>101</i>
<i>Obr. 80. NFC technologie u přístupových systémů [33]</i>	<i>102</i>
<i>Obr. 81. Externí modul pro počítání osob[14]</i>	<i>103</i>
<i>Obr. 82. Bezdrátový přístupový systém GSD[19].....</i>	<i>104</i>

SEZNAM TABULEK

<i>Tab. 1. Tabulka úrovně střežení [27], upraveno Pavlínek, 2014</i>	<i>73</i>
<i>Tab. 2. Rozdělení objektu na podsystémy</i>	<i>91</i>
<i>Tab. 3. Podsystém 1 – zóny</i>	<i>92</i>
<i>Tab. 4. Podsystém 2 - zóny</i>	<i>92</i>
<i>Tab. 5. Podsystém 3 - zóny</i>	<i>93</i>
<i>Tab. 6. Podsystém 4 – zóny</i>	<i>93</i>
<i>Tab. 7. Cenová kalkulace za software</i>	<i>94</i>
<i>Tab. 8. Cenová kalkulace za hardware.....</i>	<i>95</i>

SEZNAM PŘÍLOH

Příloha P I: Certifikát VAR-NET INTEGRAL společnosti VARIANT PLUS, s.r.o

PŘÍLOHA P I: CERTIFIKÁT VAR-NET INTEGRAL

SN: V+HSB31052012

VARIANT plus, spol. s r.o. vydává

CERTIFIKÁT

ODBORNÉ ZPŮSOBILOSTI
pro návrh a implementaci software

 **VAR-NET[®]**
INTEGRAL[®]

Potvrzujeme, jako výhradní distributor že společnost:

Název společnosti

se zúčastnila námi pořádaného školení na integrační software VAR-NET INTEGRAL. Školení bylo zaměřeno na teoretickou znalost software, návrh, implementaci a školení uživatelů. Účastníci jsou tak plně kvalifikováni k návrhu a implementaci integračního software VAR-NET INTEGRAL.

Školení v Praze, dne 31.05.2012 se účastnili:

Jméno a příjmení

Vydáno v Třebíči, dne 04.06. 2012


Bc. Petr Zelníček

 **VARIANT[®]**
plus

Certifikát společnosti **VARIANT plus, spol. s r.o.** 005587

Scitní tiskárna cenín, s.p.