

Technické způsoby integrace poplachových systémů

Techniques of Integration of Alarm Systems

Martin Kovařík

Bakalářská práce
2012



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Martin KOVAŘÍK**
Osobní číslo: **A09241**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Technické způsoby integrace poplachových systémů**

Zásady pro vypracování:

1. Analyzujte technické požadavky na poplachové systémy z hlediska jejich integrace.
2. Vymezte technické možnosti integrace poplachových a nepoplachových aplikací.
3. Analyzujte a proveďte komparaci dostupných integračních produktů.
4. Pojednejte o možnostech aplikace integrovaných poplachových systémů v obytných a průmyslových prostředích.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. LUKÁŠ, Luděk a kol., Bezpečnostní technologie, systémy a management. 1. vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.
2. UHLÁŘ, J. Technická ochrana objektů: II. díl. Elektrické zabezpečovací systémy. 1. vyd. Praha: Policejní akademie České republiky, 2005. 230 s. ISBN 80-7251-189-0.
3. KŘEČEK Stanislav. Příručka zabezpečovací techniky. Vydání 3. Blatná: Cricetus, 2006. 315 s. ISBN 80-902938-2-4.
4. Katalog produktů 2010–2011. Třebíč: Variant plus, 2010. 280 s.
5. HERMANN, Merz, THOMAS, Hansemann a CHRISTOF, Hübner. Automatizované systémy budov: Sdělovací systémy KNX/EIB, LON a BACnet. Praha: Grada, 2009. Edice Stavitel. 264 s. ISBN 978-80-247-2367-9.
6. ČSN CLC/TS 50398. Poplachové systémy– Kombinované a integrované systémy– všeobecné požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. 20 s. Třídící znak 334597.
7. VALEŠ, Miroslav. Inteligentní dům. 1. vyd. Brno: ERA, 2006. 123 s. ISBN 80-7366-062-8.
8. Inteligentní elektroinstalace Ego-n: Návrhový a instalační manuál. 5. vyd. [online]. Jablonec nad Nisou: ABB, 2011 [cit. 2012-01-10]. Dostupné z <http://www117.abb.com>.

Vedoucí bakalářské práce:

Ing. Jan Valouch, Ph.D.

Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce:

24. února 2012

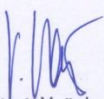
Termín odevzdání bakalářské práce:

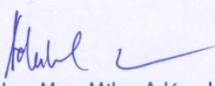
25. května 2012

Ve Zlíně dne 24. února 2012



L.S.


prof. Ing. Vladimír Vašek, CSc.
děkan


doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Bakalářská práce se v teoretické části zabývá analýzou technických požadavků na poplachové systémy z hlediska jejich integrace, vyplývajících z právních předpisů a technických norem. V této části práce je rovněž proveden popis jednotlivých technických možností, jak realizovat integraci poplachových a nepoplachových aplikací.

Součástí praktické části je analýza a komparace produktů, které se používají pro integraci a jsou v současné době dostupné na trhu. Závěrečná část představuje návrh aplikačních možností, jak využít integrované poplachové systémy v obytných a průmyslových prostředích.

Klíčová slova: požadavky, integrace, poplachový systém, nepoplachový systém, aplikace

ABSTRACT

The theoretical part of this bachelor thesis deals with analysis of technical requirements for alarm systems in terms of their integration, arising from legislation and technical standards. In this part of the work is also carried out a description of the technical possibilities, how to realize the integration of alarm and non-alarm applications.

The practical part includes an analysis and comparison of the products, which are used for integration and are currently available on the market. The final part represents the application possibilities, how to use the integrated alarm systems in residential and industrial environments.

Keywords: requirements, integration, alarm system, non-alarm system, application

Tímto bych chtěl poděkovat svému vedoucímu bakalářské práce panu Ing. Janu Valouchovi, Ph.D. za odborné vedení a pomoc při psaní této práce, připomínky a přínosné konzultace.

Zároveň bych chtěl poděkovat rodičům, sestře, celé rodině a přátelům, za podporu během studia na FAI UTB ve Zlíně a při psaní mé bakalářské práce.

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	9
I TEORETICKÁ ČÁST	10
1 TECHNICKÉ POŽADAVKY NA INTEGROVANÉ SYSTÉMY	11
1.1 POŽADAVKY PRÁVNÍCH PŘEDPISŮ	12
1.1.1 Zákon o technických požadavcích na výrobky	12
1.1.1.1 Technické požadavky na výrobek.....	13
1.1.1.2 Technické předpisy a technické dokumenty.....	13
1.1.2 Elektromagnetická kompatibilita	14
1.1.2.1 Základní požadavky.....	14
1.1.3 Elektrická zařízení nízkého napětí	15
1.1.3.1 Požadavky na bezpečnost	16
1.1.4 Rádiová a telekomunikační koncová zařízení.....	17
1.2 POŽADAVKY TECHNICKÝCH PŘEDPISŮ	18
1.2.1 Definování základních pojmů	19
1.2.2 Typy konfigurace integrovaných poplachových systémů.....	21
1.2.3 Systémové požadavky a stanovení kompatibility	23
1.2.3.1 Přístupové úrovně	24
1.2.3.2 Společné ovládací zařízení.....	24
1.2.4 Společné signalizační zařízení	24
1.2.4.1 Signalizace informace.....	24
1.2.4.2 Priority	25
1.2.4.3 Požadavky na signalizaci priorit	25
1.2.5 Napájecí zdroje.....	25
1.2.6 Centrální ovládací zařízení.....	26
1.2.6.1 Všeobecné požadavky.....	26
1.2.6.2 Požadavky na centrální ovládací zařízení třídy 2	26
1.3 DÍLČÍ ZÁVĚR	27
2 TECHNICKÉ MOŽNOSTI INTEGRACE POPLACHOVÝCH A NEPOPLACHOVÝCH APLIKACÍ	28
2.1 HW INTEGRACE	29
2.1.1 Integrace propojením vstupů a výstupů	29
2.1.1.1 Zařízení používaná pro integraci	29
2.1.1.2 Možnosti integrace propojením vstupů/výstupů.....	32
2.1.2 Integrace přes sběrnici s využitím modulů.....	35
2.1.2.1 Sběrníkový systém	37
2.1.3 Integrace pomocí systému domácí automatizace X10	40
2.1.4 Integrace v rámci systémové elektroinstalace.....	42
2.2 SW INTEGRACE	46
2.2.1 Integrace pomocí SW nastavy.....	46
2.2.1.1 Propojení jednotlivých systémů.....	47
2.2.1.2 Funkce SW nastavy	47
2.2.1.3 Bezpečnost	48
2.3 DÍLČÍ ZÁVĚR	49
II PRAKTICKÁ ČÁST	50
3 INTEGRAČNÍ PRODUKTY	51

3.1	INTEGRACE PROPOJENÍM VSTUPŮ A VÝSTUPŮ	51
3.1.1	Jablotron - Oasis.....	51
3.1.2	Jablotron – David	51
3.1.3	IP kamera AXIS 210	52
3.2	INTEGRACE PŘES SBĚRNICI S VYUŽITÍM MODULŮ	53
3.2.1	Honeywell - MB 48.....	53
3.2.2	Honeywell – Galaxy Dimension	53
3.2.3	Paradox DIGIPLEX EVO	54
3.3	INTEGRACE POMOCÍ SYSTÉMU DOMÁCÍ AUTOMATIZACE X10.....	56
3.3.1	Marmitek TotalGuard.....	56
3.4	INTEGRACE V RÁMCI SYSTÉMOVÉ ELEKTROINSTALACE.....	56
3.4.1	iNELS.....	56
3.4.2	Nikobus	57
3.4.3	ABB i-bus KNX.....	59
3.5	INTEGRACE POMOCÍ SW NÁSTAVBY	60
3.5.1	Alvis	60
3.5.2	VAR-NET INTEGRAL	62
3.5.3	TEGAL.....	64
3.5.4	Integra 3	67
3.5.5	SIMS	70
3.6	KOMPARACE PRODUKTŮ	72
3.6.1	HW integrace	72
3.6.2	SW integrace	73
3.6.2.1	Integrace pomocí SW nastavby	73
3.7	DÍLČÍ ZÁVĚR	75
4	MOŽNOSTI APLIKACE INTEGROVANÝCH POPLACHOVÝCH SYSTÉMŮ.....	76
4.1	IPS V OBYTNÉM PROSTŘEDÍ	76
4.2	IPS V PRŮMYSLOVÉM PROSTŘEDÍ.....	77
4.3	DÍLČÍ ZÁVĚR	78
	ZÁVĚR	80
	ZÁVĚR V ANGLIČTINĚ.....	82
	SEZNAM POUŽITÉ LITERATURY.....	84
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	88
	SEZNAM OBRÁZKŮ	90
	SEZNAM TABULEK.....	92

ÚVOD

S pojmem integrované poplachové systémy (dále jen „IPS“) se můžeme v dnešním světě setkávat stále častěji. Je to dáno tím, že žijeme ve 21. století, kdy se věda a technika stále více rozvíjejí. S rostoucím tempem technologií se mění i typ a množství majetku, který je třeba chránit. Díky tomu se stále zvyšují požadavky na systémy, které by nám zabezpečily nejen majetek, ale především život a zdraví. Ochranu života, zdraví a majetku můžeme zajistit třemi formami ochrany: fyzická, technická a kombinovaná. Ochranu lze definovat jako stabilní, relativně předvídatelné prostředí, ve kterém může jedinec nebo skupina sledovat své cíle bez rušení a ohrožení, bez strachu z vměšování nebo násilí. [1] Technickou ochranu dále dělíme na mechanickou, elektronickou, smíšenou a speciální. Bakalářská práce se bude zabývat především elektronickou ochranou, do které můžeme zařadit poplachové zabezpečovací systémy, elektrickou požární signalizaci, sledovací systémy pro použití v bezpečnostních aplikacích, přístupové a docházkové systémy apod. Pokud každý z těchto systémů použijeme samostatně, budeme muset ovládat a spravovat každý zvlášť. To nám zabere více času, způsobí problémy s ovládáním, a také zvýší náklady na provoz. Tyto problémy umožňuje vyřešit integrovaný poplachový systém, který dokáže všechny technologie v objektu spojit do jednoho funkčního celku. Výše jmenované formy elektronické ochrany můžeme zařadit do poplachových aplikací. Integrované systémy dokážou tyto aplikace spojit společně s automatizací, tedy nepoplachovými aplikacemi.

Výhodou integrovaných systémů je získání předpoplachové informace, úspora energie, komfortní obsluha a lepší přehled o bezpečnostní situaci.

Teoretická část bakalářské práce se bude zabývat technickými požadavky na IPS. Patří zde požadavky právních a technických předpisů. Poté budou popsány možné varianty, jak jednotlivé systémy propojit do jednoho celku.

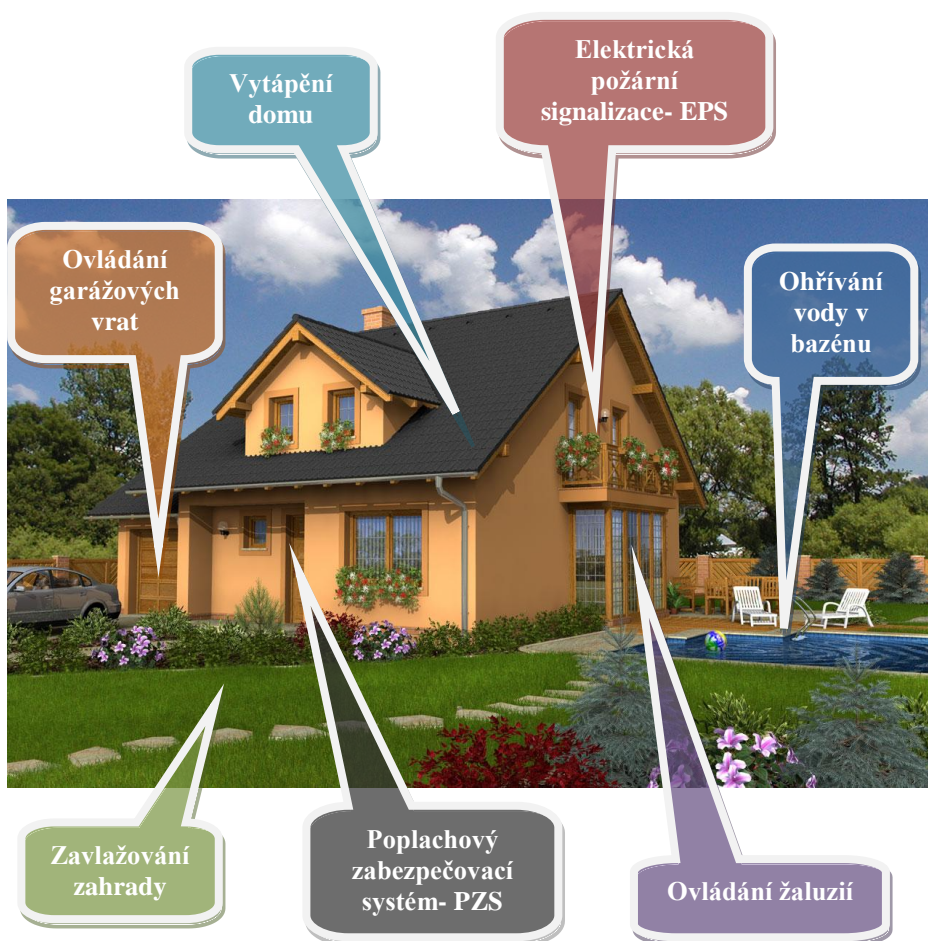
V první polovině praktické části, která se bude zabývat popisem jednotlivých produktů, které jsou dostupné na trhu, bude použita metoda analýzy. Dále budou tyto produkty porovnány pomocí komparativní metody. Poslední část práce bude obsahovat popis možností, jak aplikovat IPS do obytného a průmyslového prostředí.

Výsledky práce mohou sloužit jako podklad při návrhu IPS pro jednotlivé objekty, nebo jako materiály pro další zpracování tohoto tématu.

I. TEORETICKÁ ČÁST

1 TECHNICKÉ POŽADAVKY NA INTEGROVANÉ SYSTÉMY

Integrované systémy nám umožňují realizovat ochranu před vloupáním, požárem, přepadením, a zároveň nám dovoluje využívat služby spojené s ovládáním a správou objektu. Mezi tyto služby patří ovládání topení, osvětlení, garážových vrat, ale také nás dokážou informovat o výpadku elektrické energie, zavlažovat zahradu, simulovat naši přítomnost v domě pokud jsme na dovolené apod. Integrované systémy v sobě tedy spojují aplikace spojené se zabezpečením objektu (poplachové aplikace) a technologie, které nám usnadňují ovládání a používání prostředků v objektu (nepoplachové aplikace).



Obr. 1: Integrovaný systém rodinného domu

1.1 Požadavky právních předpisů

Jednotlivé komponenty integrovaných poplachových systémů můžeme zařadit mezi výrobky, které vzhledem k vlastní konstrukci mohou ohrozit život, zdraví a bezpečnost osob, majetek a životní prostředí. Z těchto důvodů musí tyto komponenty splňovat požadavky příslušných právních a technických předpisů. Mezi základní právní předpisy, které řeší problematiku uvádění výrobků na trh, patří zákon č. 22/1997 Sb. o technických požadavcích na výrobky. S ohledem na typ výrobku v oblasti IPS (Integrovaných Poplachových Systémů) konkretizují požadavky příslušná nařízení vlády (NV) – č. 616/2006 Sb. o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility, dále NV č. 17/2003 Sb. technické požadavky na elektrická zařízení nízkého napětí a NV č. 426/2000 Sb. technické požadavky na rádiová a na telekomunikační koncová zařízení. [2]

1.1.1 Zákon o technických požadavcích na výrobky

Zákon č. 22/1997 upravuje způsob stanovení technických požadavků na výrobky, které by mohly ohrozit zdraví nebo bezpečnost osob, majetek nebo životní prostředí. Zákon o technických požadavcích na výrobky, se také zabývá právy a povinnostmi osob, které tyto výrobky uvádějí na trh, distribuují nebo uvádějí do provozu.

Základní pojmy spojené s tímto zákonem [3]

Výrobek – výrobkem je myšlena věc, která byla vyrobena, nebo jinak získána (např. vytěžena) a je uváděna na trh jako nová, nebo již použitá.

Výrobce – za výrobce se považuje:

- osoba vyrábějící nebo navrhující výrobek,
- v případech stanovených nařízením vlády také osoba, která sestavuje, balí nebo označuje výrobek, za který odpovídá a uvádí ho na trh pod svým jménem nebo ochrannou známkou,
- osoba, jež upravila výrobek, který už byl na trhu tak, že ovlivnil jeho soulad s příslušnými technickými požadavky.

Dovozce – musí sídlit v členském státě Evropské unie (EU) a uvádí na trh výrobek z jiného než členského státu EU.

1.1.1.1 Technické požadavky na výrobek

Tyto požadavky souvisí s právními předpisy, technickými dokumenty nebo technickými normami, kde jsou stanoveny požadavky na to, jak má výrobek vypadat, jaké má mít rozměry a vlastnosti. Dále řeší název výrobku, jeho označení, zkoušení a posuzování shody s normami a předpisy. Důležité je také stanovení požadavků na výrobek v oblasti používání, zneškodnění nebo recyklace.

Technickými požadavky na výrobek se podle zákona č. 22/1997 rozumí:

1. *„technická specifikace obsažená v právním předpisu, technickém dokumentu nebo technické normě, která stanoví požadované charakteristiky výrobku, jakými jsou úroveň jakosti, užitné vlastnosti, bezpečnost a rozměry, včetně požadavků na jeho název, pod kterým je prodáván, úpravu názvosloví, symbolů, zkoušení výrobku a zkušebních metod, požadavky na balení, označování výrobku nebo opatřování štítkem, postupy posuzování shody výrobku s právními předpisy nebo s technickými normami, výrobní metody a procesy mající vliv na charakteristiky výrobků,“*[3]
2. *„jiné požadavky nezbytné z důvodů ochrany oprávněného zájmu nebo ochrany spotřebitele, které se týkají životního cyklu výrobku poté, co je uveden na trh, popřípadě do provozu, např. podmínky používání, recyklace, opětovného použití nebo zneškodnění výrobku, pokud takové podmínky mohou významně ovlivnit složení nebo povahu výrobku nebo jeho uvedení na trh, popřípadě do provozu.“*
[3]

1.1.1.2 Technické předpisy a technické dokumenty

Tyto požadavky se zaměřují na technické předpisy, ve kterých jsou stanoveny technické požadavky a pravidla pro výrobky, které jsou uváděny na trh nebo do provozu. Určují také co je to technický předpis a co má obsahovat.

1. *„Technickým předpisem pro účely tohoto zákona je právní předpis, obsahující technické požadavky na výrobky, popřípadě pravidla pro služby nebo upravující povinnosti při uvádění výrobku na trh, popřípadě do provozu, při jeho používání nebo při poskytování nebo zřizování služby nebo zakazující výrobu, dovoz, prodej či používání určitého výrobku nebo používání, poskytování nebo zřizování služby.“*[3]

2. „*Technickým dokumentem se pro účely plnění informačních povinností podle § 7 rozumí dokument, který obsahuje technické požadavky na výrobek, a není technickým předpisem ve smyslu odstavce 1 ani technickou normou, a který by mohl vytvořit technickou překážku obchodu.*”[3]

1.1.2 Elektromagnetická kompatibilita

Jednotlivé komponenty integrovaných poplachových systémů, jako převážně výrobky elektronické, musí splňovat rovněž legislativní požadavky na elektromagnetickou kompatibilitu. Těmito požadavky se zabývá a příslušné předpisy zpracovává Směrnice Evropského parlamentu a Rady 2004/108/ES ze dne 15. prosince 2004 o sblížení právních předpisů členských států, týkajících se elektromagnetické kompatibility a o zrušení směrnice 89/336/EHS. Na národní úrovni jsou uvedené požadavky stanoveny v nařízení vlády 616/2006 Sb. o technických požadavcích na výrobky, z hlediska jejich elektromagnetické kompatibility.

Nařízení řeší: [4]

- Elektromagnetickou kompatibilitu – je to schopnost nerušit jiné zařízení nebo samo sebe a zároveň odolávat elektromagnetickému rušení od ostatních přístrojů. To znamená, že zařízení může správně fungovat v elektromagnetickém prostředí.
- Elektromagnetické rušení (interferenci) – představuje elektromagnetický jev, který může zhoršit funkce zařízení. Elektromagnetickým rušením může být: elektromagnetický šum, nežádoucí signál nebo změna v samotném prostředí šíření.
- Elektromagnetickou odolnost (susceptibilitu) – jedná se o schopnost zařízení pracovat bez poruchy a zhoršení kvality i v prostředí, kde se nachází elektromagnetické rušení.

1.1.2.1 Základní požadavky

1. Požadavky na ochranu výrobku

Výrobek musí být navržen a vyroben takovým způsobem, aby:

- a) „*elektromagnetické rušení, které způsobuje, nepřesáhne úroveň, za níž rádiové a telekomunikační zařízení nebo jiné zařízení není schopné fungovat tak, jak má,*“ [4]

b) „úroveň jeho odolnosti vůči elektromagnetickému rušení předpokládanému při používání k danému účelu mu dovoluje fungovat bez nepřijatelného zhoršení určených funkcí.”[4]

2. Zvláštní požadavky pro pevné instalace a použití komponentů pro daný účel

„Pevná instalace musí být instalována s použitím správných technických postupů a při respektování údajů o použití komponentů pro daný účel, aby byly splněny požadavky na ochranu podle bodu 1. Tyto správné technické postupy musí být zdokumentovány a dokumentaci uchovává provozovatel po dobu provozování pevné instalace pro potřeby kontroly ze strany příslušných orgánů.”[4]

Výše uvedené požadavky se pokládají za splněné, v případě že je dané zařízení v souladu s: [4]

- harmonizovanými evropskými normami – v Úředním věstníku Evropské unie musí být uveden odkaz na tuto normu,
- harmonizovanými českými technickými normami – přejímající harmonizovanou evropskou normu,
- zahraničními technickými normami v členském státě EU - přejímající harmonizovanou evropskou normu. Pokud dojde k odstranění odkazu z Úředního věstníku Evropské unie, jsou tyto předpoklady neplatné.

1.1.3 Elektrická zařízení nízkého napětí

Nařízení vlády č. 17/2003 Sb. se zabývá technickými požadavky na elektrická zařízení nízkého napětí.

Elektrická zařízení nízkého napětí jsou taková, která splňují tyto kritéria:

Tabulka 1: Rozsahy napětí pro elektrické zařízení nízkého napětí [5]

Jmenovité napětí	
Střídavý proud	Stejnoseměrný proud
50 – 1000 V	75 – 1500 V

Nařízení zde stanovuje požadavky, které musí být splněny při uvedení výrobku na trh, tzn., že byl vyroben podle správné technické normy, se zásadami bezpečnosti, která je platná v Evropském společenství. Nesmí také ohrozit bezpečnost osob, zvířat a majetku při správném nainstalování, používání a údržbě.

1.1.3.1 Požadavky na bezpečnost

1. Všeobecné požadavky

Mezi všeobecné požadavky patří popis elektrického zařízení, tzn. kdo je výrobcem, jaká je značka zařízení a jak by se mělo bezpečně používat. Tyto informace musí být uvedeny na výrobku, popřípadě v průvodním dokumentu. Patří zde i požadavky na návrh a výrobu zařízení, tak aby bylo zajištěno bezpečné připojení a používání.

Pro uvedení výrobku na trh, musí být splněny požadavky podle NV č. 17/2003 Sb.

- a) *„Základní technické charakteristiky, jejichž dodržování zajišťuje, aby elektrické zařízení bylo používáno bezpečně a v podmínkách, pro které bylo vyrobeno, musí být vyznačeny na elektrickém zařízení, anebo pokud to není možné, musí být uvedeny v průvodní dokumentaci.“ [5]*
- b) *„Jméno a příjmení fyzické osoby nebo obchodní firma nebo název právnické osoby, která je výrobcem, značka, popřípadě obchodní známka musí být zřetelně uvedeny na výrobku, a není-li to možné, na jeho obalu.“*
- c) *„Elektrické zařízení a jeho díly musí být vyrobeny tak, aby byla zajištěna bezpečná a správná montáž a připojení.“ [5]*
- d) *„Elektrické zařízení musí být navrženo a vyrobeno tak, aby u něj, za předpokladu, že je používáno pro účely, ke kterým je určeno, a že je řádně udržováno, byla zajištěna ochrana před nebezpečími uvedenými v bodech 2 a 3.“ [5]*

2. Ochrana před nebezpečím, které může způsobit elektrické zařízení

Elektrické zařízení může být nebezpečné pro lidi i zvířata, proto jsou stanoveny požadavky, které tomuto nebezpečí předcházejí. Zařízení nesmí ohrozit osoby a zvířata elektrickým proudem, vznikem nebezpečné teploty nebo záření. Izolace musí být provedena tak, aby byla účinná v předvídatelných podmínkách.

„Ve smyslu bodu 1 musí být technické provedení elektrického zařízení takové, aby bylo zajištěno, že:

- a) *osoby a domácí a hospodářská zvířata budou přiměřeně chráněny před nebezpečím zranění nebo jiného poškození, které by mohlo být způsobeno elektrickým proudem při dotyku živých nebo neživých částí,*
- b) *nevzniknou nebezpečné teploty, nebezpečné oblouky nebo nebezpečná záření,*
- c) *osoby, domácí a hospodářská zvířata a majetek budou přiměřeně chráněny před nebezpečími neelektrického charakteru, která mohou podle zkušenosti elektrická zařízení způsobovat,*
- d) *izolace musí odpovídat předvídatelným podmínkám.”[5]*

3. Ochrana před nebezpečími, která mohou vznikat působením vnějších vlivů na elektrické zařízení

Elektrické zařízení musí být také odolné proti vnějším vlivům, které na něho můžou působit. Musí zajistit bezpečnost při působení okolních podmínek, mechanickém namáhání a při předvídatelném přetížení.

„Ve smyslu bodu 1 musí být technické provedení elektrického zařízení takové, aby

- a) *odolávalo předpokládaným mechanickým namáháním tak, že osoby, domácí a hospodářská zvířata ani majetek nebudou ohroženy,*
- b) *odolávalo za předpokládaných podmínek okolního prostředí působení jiných než mechanických vlivů tak, že osoby, domácí a hospodářská zvířata ani majetek nebudou ohroženy,*
- c) *při předvídatelných přetíženích neohrozilo žádným způsobem osoby, domácí a hospodářská zvířata ani majetek.“[5]*

1.1.4 Rádiová a telekomunikační koncová zařízení

Nařízení vlády č. 426/2000 Sb., se zaměřuje na stanovení technických požadavků pro rádiová a telekomunikační koncová zařízení. **Rádiové zařízení** je výrobek nebo jeho součást, který umožňuje komunikaci pomocí vysílání a příjmu rádiových vln, v kmitočtovém spektru, které bylo přiděleno pro zemské nebo kosmické radiokomunikace. **Telekomunikační koncové zařízení** je výrobek, nebo jeho součást, pomocí kterého můžeme komunikovat a připojuje se k rozhráním veřejných telekomunikačních sítí. [6]

Základní požadavky:

- a) Výrobky musí zajistit ochranu zdraví a bezpečnost uživatele, popř. jiných osob, podle Nařízení vlády č.17/2003 Sb., bez ohledu na to, jaká je hodnota napětí.
- b) Dalším požadavkem je zajistit ochranu spojenou s elektromagnetickou kompatibilitou, podle Nařízení vlády č. 616/2006Sb.
- c) Konstrukce rádiových zařízení musí být taková, aby co nejlépe využívala kmitočtové spektrum pro zemskou nebo kosmickou radiokomunikaci. [6]

Telekomunikační zařízení a přístroje musí být konstruovány tak, aby:

- a) umožňovaly spolupráci s jinými přístroji a zařízeními, prostřednictvím veřejné telekomunikační sítě. Musí být připojitelné k rozhraní veřejné telekomunikační sítě na území České republiky a na území členského státu Evropské unie,
- b) - nepříznivě neovlivňovaly veřejnou telekomunikační síť,
 - nezpůsobovaly nepřijatelné zhoršení jakosti služeb,
 - nezneužívaly kapacity a možnosti veřejné telekomunikační sítě,
- c) zabezpečovaly ochranu osobních dat a soukromí uživatele a účastníka, pomocí zabezpečovacích prvků,
- d) podporovaly:
 - funkce zabraňující podvodům,
 - funkce umožňující přístup k tísňovým službám,
 - funkce usnadňující jejich používání zdravotně postiženým uživatelům.

Přístroje a zařízení v určitých třídách nebo přístroje a zařízení určitých typů musí být Úřadem zveřejněna v Telekomunikačním věstníku formou sdělení. [6]

1.2 Požadavky technických předpisů

Technickým předpisem je právní předpis, který obsahuje:

- technické požadavky na výrobky,
- pravidla pro služby.

V průmyslu komerční bezpečnosti (v technické části), se využívají především tyto řady norem:

- ČSN EN 50131 - Poplachové zabezpečovací a tísňové systémy
- ČSN EN 50132 - Poplachové systémy – CCTV (Closed circuit television) sledovací systémy pro použití v bezpečnostních aplikacích
- ČSN EN 50133 - Systémy kontroly vstupu
- ČSN EN 50134 - Systémy přivolání pomoci
- ČSN EN 54 - Elektrická požární signalizace
- ČSN EN 50136 - Poplachové systémy – Poplachové přenosové systémy a zařízení

Problematiku IPS řeší v rámci technických předpisů platných v ČR norma ČSN CLC/TS 50398. Tato technická norma se zabývá všeobecnými požadavky a příklady struktur integrovaných poplachových systémů. Cílem normy je zajištění integrace aplikací do jednoho integrovaného systému. Může se jednat o jednu nebo více aplikací. V normě jsou uvedeny informace o návrhu, plánování, instalaci, předávání, provozu a údržbě kombinovaného a integrovaného systému. V normě jsou dále specifikovány požadavky na poplachové systémy, které jsou integrovány s jinými systémy. Tyto systémy mohou být poplachové a nepoplachové. Nyní budou popsány jednotlivé části této normy.

1.2.1 Definování základních pojmů

Norma ČSN CLC/TS 50398 používá především tyto základní pojmy: [7]

Poplach - informace o výskytu nebezpečí, které ohrožuje život osob, majetek nebo životní prostředí.

Poplachová aplikace – jedná se o aplikaci, která má za úkol ochranu života, majetku a prostředí:

- PZTS – Poplachové a zabezpečovací tísňové systémy
- ACS – Systém kontroly vstupu
- SAS – Systém přivolání pomoci
- CCTV – Kamerové systémy
- EPS – Elektrická požární signalizace

Poplachové přijímací centrum (PPC) – je centrum, které je neustále pod dohledem obsluhy. Předávají se zde informace o stavu poplachových systémů.

Poplachový stav – stav poplachového systému nebo jeho komponentů, který je výsledkem odezvy systému na přítomnost nebezpečí.

Poplachový systém – elektrické zařízení, které reaguje na detekci přítomnosti nebezpečí. Tato detekce může být vyvolána manuálním podnětem nebo automatickou detekcí.

Poplachové přenosové zařízení – zařízení, které se používá k přenosu poplachu z rozhraní poplachového systému, do rozhraní vyhodnocovacího zařízení PPC. Lze ho také použít pro přenesení informací a povelů z centra do poplachových systémů.

Poplachový přenosový systém (ATS) – síť a zařízení, používané k přenosu informací mezi poplachovými systémy nebo poplachovými přijímacími centry.

Ústřední ovládací zařízení (CCF) – používá se pro řízení nebo signalizaci v konfiguraci typu 1, který je připojen k jednoúčelovým systémům. Toto zařízení je obsluhováno provozním personálem.

Společné zařízení – jedná se o zařízení, které je sdíleno jednou nebo více aplikacemi. Může být společné pro 2 nebo více aplikací.

Společná přenosová trasa – je trasa, kterou využívají dvě nebo více aplikace.

Zařízení – hardwarové nebo softwarové vybavení, které umožňuje systému plnit určité funkce.

Poruchový stav – tento stav neumožňuje systému plnění funkcí, které byly pro tento systém navrženy.

Poruchový signál – jedná se o zprávu, která je vygenerována v důsledku poruchy.

Integrovaný poplachový systém – systém, který má společně jedno nebo více zařízení. Aby se jednalo o integrovaný poplachový systém, musí být alespoň jedno zařízení poplachovou aplikací.

Integrita – schopnost aplikace, při které plní funkce, pro něž byla konstruována a odolává vlivům ovlivňující její správnou činnost.

Nepoplachové systémy – jsou to systémy, které se používají pro ovládání a jejich hlavní funkce nespočívá v ochraně života, majetku nebo životního prostředí.

Sabotážní stav – stav poplachového systému, v němž byla detekována sabotáž.

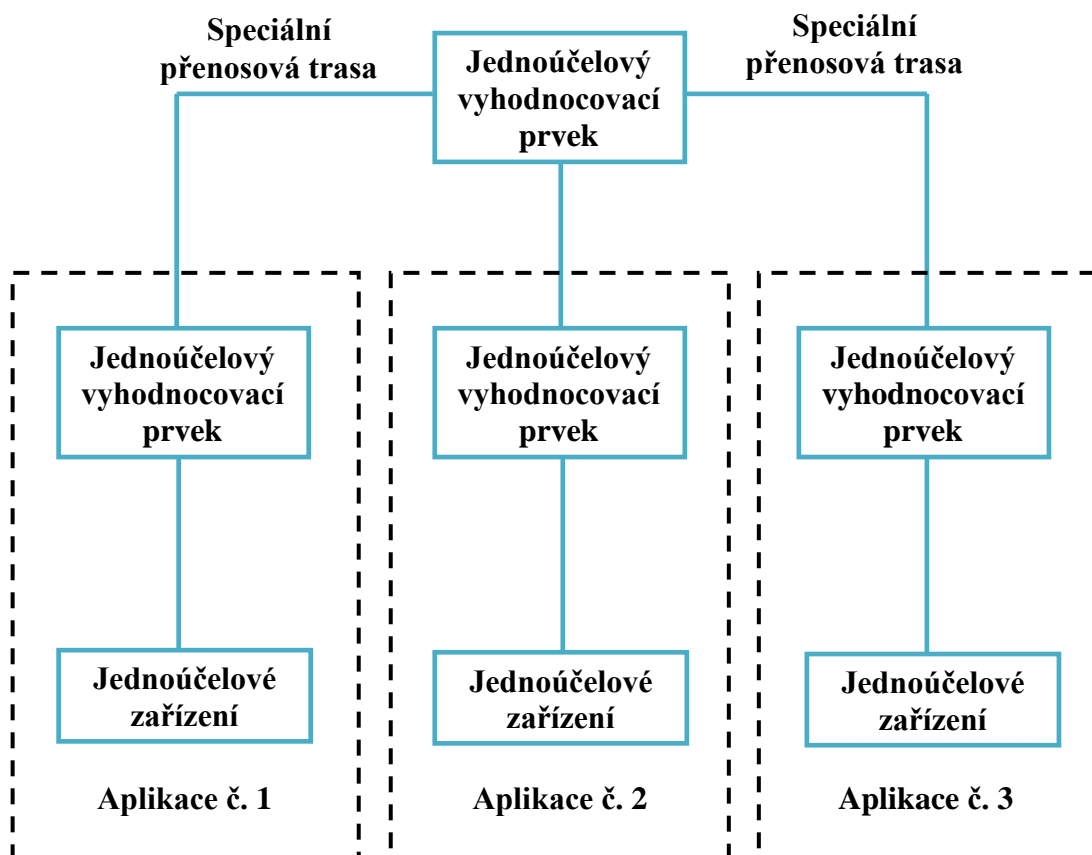
Přenosová cesta – je to komunikační cesta, která se využívá pro přenos informace v integrovaném poplachovém systému.

1.2.2 Typy konfigurace integrovaných poplachových systémů

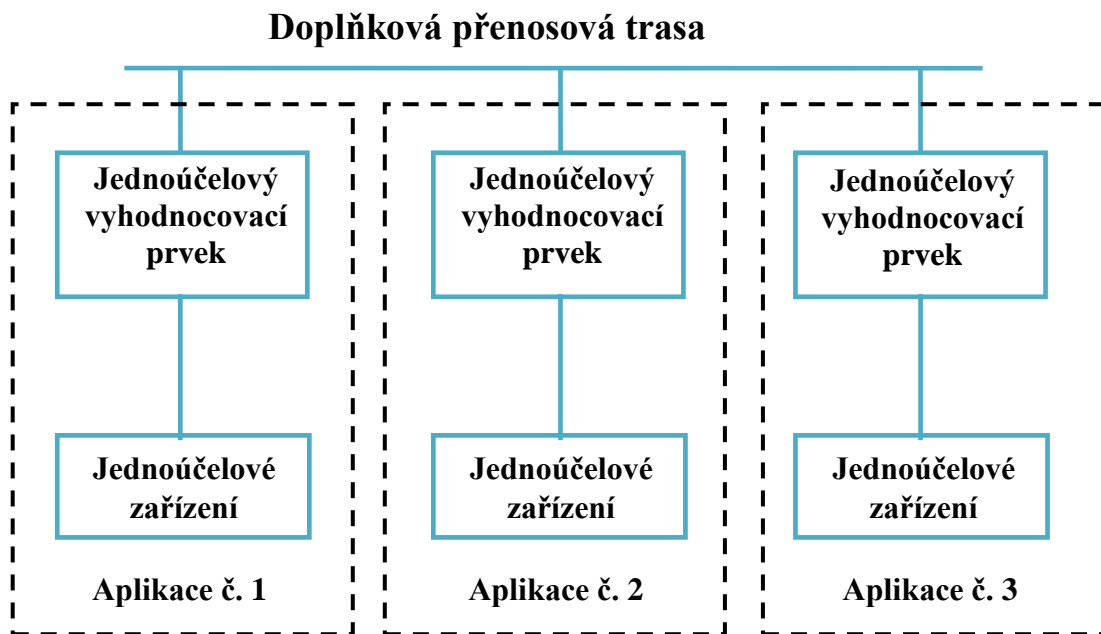
Existují dva typy konfigurace poplachových systémů. Druhý typ se dále rozděluje na dvě varianty.

Typ 1:

Využívá se pro integraci a kombinaci jednoúčelových poplachových a nepoplachových systémů. Propojení těchto jednoúčelových systémů je řešeno připojením ke společnému doplňkovému zařízení. Pro toto připojení se používá společná přenosová trasa. Platí zde, že zařízení v konfiguraci typu 1 nesmí být v žádném provozním stavu negativně ovlivněno jakýmkoli jednoúčelovým systémem, nebo doplňkovým zařízením. [7]



Obr. 2: První varianta konfigurace typu 1 [7], upravil Kovařík, 2012

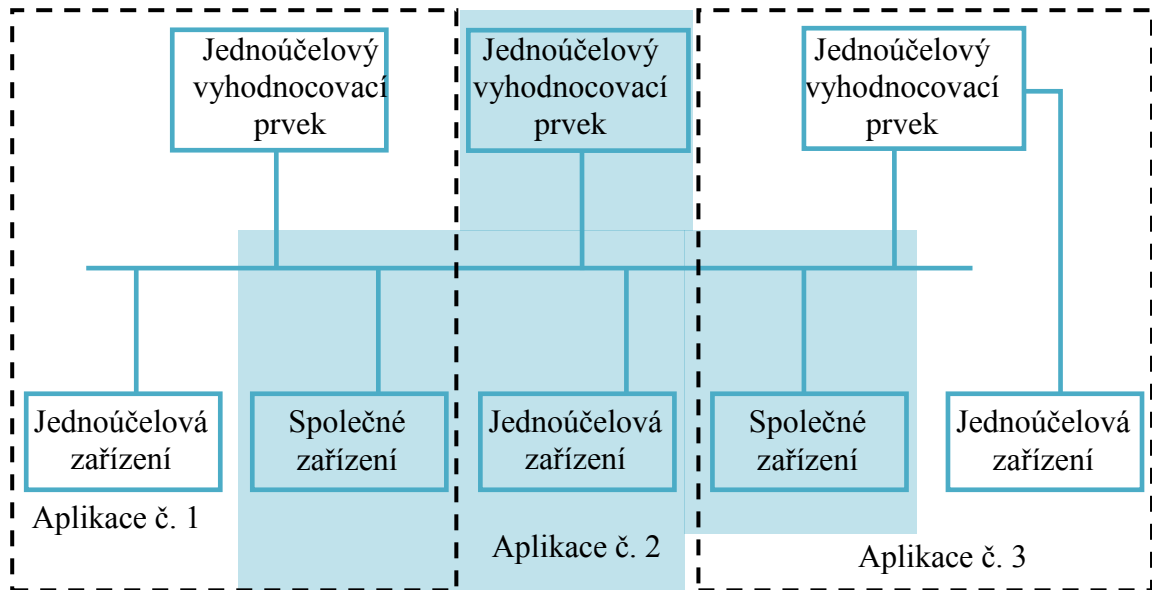


Obr. 3: Druhá varianta konfigurace typu 1 [7], *upravil Kovařík, 2012*

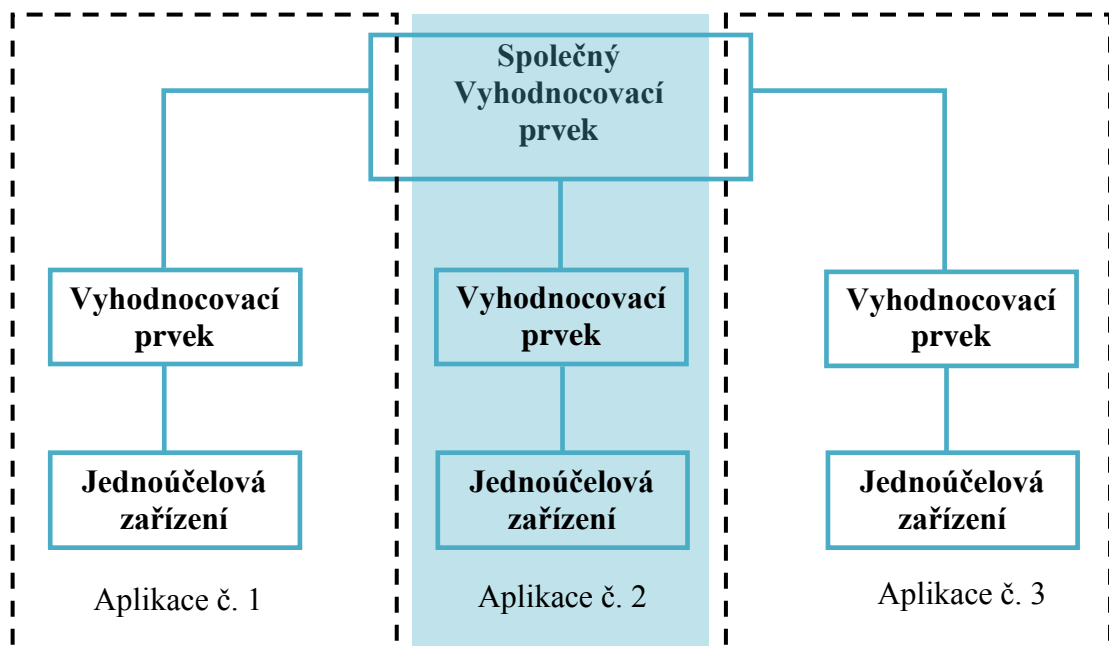
Typ 2:

Stejně jako u předchozího typu se jedná o kombinaci dvou nebo více jednoúčelových systémů. Od typu 1 se liší tím, že normou vyžadované zařízení je společné minimálně pro jednu aplikaci. [7]

- **Typ 2A** – Je aplikovaný pro kombinaci a integraci poplachových a nepoplachových systémů, které používají společné přenosové trasy, zařízení a vybavení. Jestliže dojde k poruše v jakékoli aplikaci, nemá to žádný negativní dopad na jinou poplachovou aplikaci. Tím pádem není integrita, kteréhokoli normou vyžadovaného zařízení, nepříznivě ovlivněna. [7]
- **Typ 2B** - Je aplikovaný pro kombinaci a integraci poplachových a nepoplachových systémů, které používají společné přenosové trasy, zařízení a vybavení. Pokud by došlo k poruše v jedné aplikaci, může mít tato porucha negativní vliv na jinou poplachovou aplikaci. Z toho vyplývá, že integrita může být nepříznivě ovlivněna jedinou poruchou. [7]



Obr. 4: První varianta konfigurace typu 2 [7], upravil Kovařík, 2012



Obr. 5: Druhá varianta konfigurace typu 2 [7], upravil Kovařík, 2012

1.2.3 Systémové požadavky a stanovení kompatibility

Při používání integrovaného poplachového systému může docházet ke snížení bezpečnosti a zabezpečení vlivem nesprávného použití. Aby k takovým situacím nedocházelo, je vhodné postupovat následovně: [7]

- při navrhování systému by měly být k dispozici všechny informace o provozních podmínkách pro celý integrovaný systém, od všech zúčastněných stran. Především podmínky pro povelové zařízení, které bude zřejmě požadováno,
- pokud by měla nesprávná činnost povelového zařízení vážný vliv na zabezpečení nebo na bezpečnost, musí být tento problém vyřešen. Řešení může spočívat ve vyřazení tohoto zařízení z činnosti, nebo se tato činnost musí předefinovat tak, aby tato situace nemohla nastat,
- zařízení, které budeme aplikovat, by mělo být zvoleno tak, aby umožňovalo jen žádoucí povelové funkce.

1.2.3.1 Přístupové úrovně

Jednotlivé aplikace musí mít přístupové úrovně v souladu s normou pro každou aplikaci. Nesmí umožnit neoprávněný přístup ke kterékoli jiné aplikaci. [7]

1.2.3.2 Společné ovládací zařízení

Jestliže manuálně ovládáme jakoukoli aplikaci, musí být ovládání jasné a jednoznačné. Pokud toto ovládání ovlivňuje více aplikací, musí být tyto aplikace jasně indikovány. [7]

1.2.4 Společné signalizační zařízení

Požadavky na spolehlivost:

Společné signalizační zařízení můžeme použít jako: [7]

- doplňkové zařízení – platí zde požadavek, kdy signalizace musí být úměrná jejímu významu,
- normou vyžadované – požadavky na signalizační zařízení jsou definovány v příslušných normách.

1.2.4.1 Signalizace informace

K signalizaci informace se využívají jednotlivé barvy. Tyto barvy musí být použity tak, aby jejich viditelnost umožňovala signalizaci nejvíce závažné informace, při předpokládané úrovni osvětlení. Musí se dodržovat příslušné normy pro barvy různých informací.

V případě akustické signalizace musíme brát ohled na okolní podmínky. [7]

1.2.4.2 Priority

Signalizace informací se provádí podle předem stanovených priorit. Tyto priority určují pořadí, kdy se bude signalizovat určitá informace. Z všeobecného hlediska by měly být použity tyto priority: [7]

- Priorita 1 – Jde o poplachové signály, které se vztahují k ochraně života osob, při požárním poplachu nebo při napadení.
- Priorita 2 – Poplachové signály pro ochranu majetku nebo ochranu proti nedovolenému vniknutí do objektu.
- Priorita 3 – Poplachové signály z ostatních poplachových systémů.
- Priorita 4 – Signály o poruše ze systému ochrany života a majetku.
- Priorita 5 – Signály o poruše z ostatních poplachových systémů.
- Priorita 6 – Informace z nepoplachových systémů.

Může se stát, že u některých aplikací bude toto pořadí nevyhovující a bude třeba jednotlivé priority přehodit. Z toho vyplývá, že se nejedná o pořadí, které se musí dodržovat, ale bude záležet na stanovené situaci. [7]

1.2.4.3 Požadavky na signalizaci priorit

- při požádání o doplňkové informace musí být zachována viditelnost prioritních informací,
- pokud již byl zobrazen opakovaný poplachový signál, nesmí být znovu signalizován,
- jestliže se vyskytují poplachy ve více aplikacích, musí být tato skutečnost signalizována,
- indikace poplachu nesmí být omezena jakoukoli činností aplikace,
- pokud existuje více poplachů, než je signalizační zařízení schopno zobrazit, je třeba tento stav signalizovat. [7]

1.2.5 Napájecí zdroje

Požadavky na napájení nesmí být ohroženy speciálními nebo společnými zařízeními. Také nesmí snižovat dobu pohotovostního stavu. [7]

1.2.6 Centrální ovládací zařízení

Jsou definovány 2 třídy: [7]

Třída 1 – Informace musí být zobrazeny pouze v prostorech, kde je systém pod dohledem provozní obsluhy. Signalizační zařízení, které je vyžadováno normou, např. signalizační panely nebo poplachový zabezpečovací systém, musí být umístěny ve stejném prostoru. Výhodou je zaregistrování poplachu z ústředny provozní obsluhou i v případě, že došlo k poruše centrálního ovládacího zařízení.

Třída 2 – Stejně jako u třídy 1 platí, že na systém dohlíží provozní obsluha a centrální ovládací zařízení se používá pouze k zobrazování informací, ovšem jedná se o jediný informační displej v daném prostoru. Pokud centrální ovládací zařízení umožňuje také natavení stavu střežení/klid, ovládání zón a ukládání parametrů systému, musí být v souladu s normami. Jedná se o druhý typ integrovaného systému.

1.2.6.1 Všeobecné požadavky

Pro centrální ovládací zařízení musí platit:

Tabulka 2: Všeobecné požadavky na CCF

Jednoznačná identifikace podle odpovídající třídy
Umístění v prostoru specifikovaného výrobcem
Vyhrazení pouze integrovanému poplachovému systému

1.2.6.2 Požadavky na centrální ovládací zařízení třídy 2

Monitorování provozu – Běžný provoz musí být neustále monitorován a signalizován v místě, kde je nainstalován. Poruchu v určité aplikaci je třeba opticky a akusticky signalizovat. Napájecí napětí musí být také monitorováno. [7]

Provoz při poruše – Při poruše musí být k dispozici postup, ve kterém bude uvedeno, kde jsou jednotlivé ústředny poplachového zabezpečovacího systému umístěny a popis jejich ovládání. [7]

Záložní napájení – Záložní zdroj musí být obsažen v centrálním ovládacím zařízení, pro zajištění napájení alespoň po dobu nutnou ke splnění nezbytných postupů při poruše. [7]

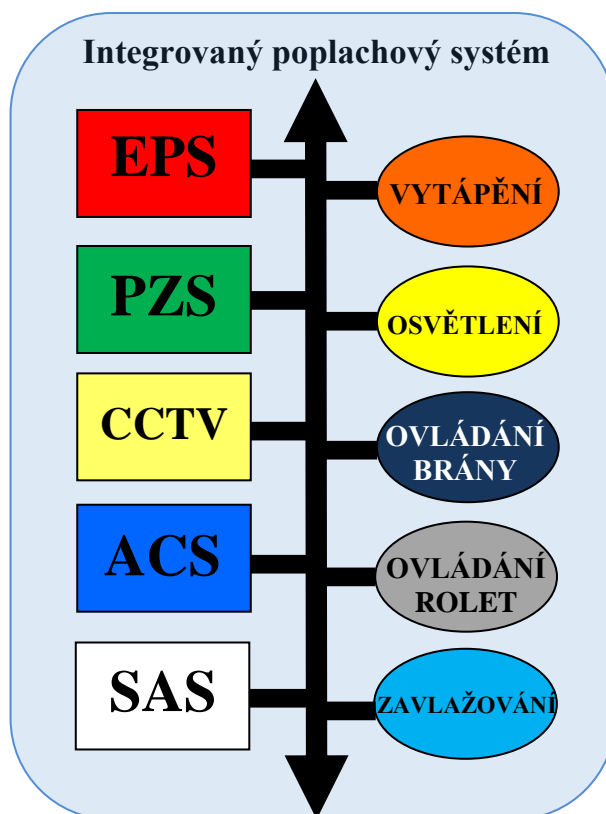
1.3 Dílčí závěr

Jelikož se IPS skládají z velkého počtu komponent, které by mohly ohrozit život a zdraví osob, jejich majetek a životní prostředí, jsou v první kapitole této práce uvedeny požadavky, které by měly zabránit výše uvedeným rizikům. Jedná se o požadavky spojené s vlastnostmi výrobku, jeho používáním, zkoušením a posuzováním shody. Dále také požadavky, které musí výrobek splňovat při uvádění na trh. Aby nedocházelo k ovlivňování ostatních zařízení, jsou zde uvedeny také požadavky spojené s elektromagnetickou kompatibilitou, rádiovými a telekomunikačními zařízeními. Komponenty IPS jsou vlastně elektrická zařízení nízkého napětí, a proto se na ně vztahují požadavky spojené s ochranou před nebezpečím, které by mohly způsobit.

Druhou část první kapitoly tvoří požadavky technických předpisů. Jsou specifikovány dva typy konfigurace IPS - typ 1 a typ 2. Druhý typ konfigurace se od prvního liší tím, že normou vyžadované zařízení, je společně minimálně pro jednu aplikaci. Konfigurace typu 2 se dále dělí na typ 2A a 2B. Tyto dva typy jsou rozdílné v oblasti ovlivňování integrity normou vyžadovaného zařízení, při poruše v kterékoliv aplikaci. Důležitým faktorem pro IPS jsou požadavky na přístupové úrovně, společné signalizační zařízení, signalizaci informace, priority pro signalizaci informací a především požadavky na centrální ovládací zařízení.

2 TECHNICKÉ MOŽNOSTI INTEGRACE POPLACHOVÝCH A NEPOPLACHOVÝCH APLIKACÍ

Pojem integrace pochází z latinského slova *integratio*= scelení. U poplachových a nepoplachových aplikací, chceme pomocí integrace dosáhnout začlenění určitých aplikací do jednotlivého celku, tzn., že naším úkolem je zajistit, aby si aplikace různého charakteru, ať už jsou spojeny se zabezpečovací nebo automatizační technikou, předávaly potřebné informace v rámci jednoho systému. Tento systém nám poté poskytuje plnohodnotné využití všech funkcí jednotlivých aplikací a umožňuje jednodušší používání a obsluhu. Existuje několik způsobů, jak můžeme tyto aplikace integrovat. V následující části bakalářské práce se budu zabývat hardwarovou (HW) a softwarovou (SW) integrací.



Obr. 6: Integrovaný poplachový systém

2.1 HW Integrace

Jedná se o způsob integrace, který využívá různé HW prvky, rozhraní, sběrnice, systémovou elektroinstalaci nebo pomocné moduly. Zvolení určité možnosti integrace záleží na velikosti objektu, možnostech stavebních úprav, dostupných finančních prostředcích a především na systémech, které chceme integrovat.

2.1.1 Integrace propojením vstupů a výstupů

Tento typ integrace využívá propojení vstupů a výstupů jednotlivých prvků systémů tak, aby mezi sebou mohly bez problémů komunikovat. Využívá se zejména pro propojení PZS, ACS, EPS, CCTV a různých nepoplachových aplikací, jako jsou například vytápění, osvětlení objektu, ovládání garážových vrat, rolet, ale také zavlažovacího systému nebo klimatizace. Integrace propojením vstupů a výstupů je nejjednodušším způsobem, jak jednotlivé systémy spojit. U tohoto způsobu integrace, se využívají zejména: [8]

- pomocná relé,
- bezdrátové vysílače,
- bezdrátové přijímače,
- GSM ovladače,
- PGM – programovatelné výstupy ústředěn,
- alarmové vstupy/výstupy.

2.1.1.1 Zařízení používaná pro integraci

Pomocná relé – jsou to elektromagnetické součástky, pomocí kterých můžeme ovládat různá zařízení nebo elektrické okruhy.



Obr. 7: Pomocné relé [8]

Relé se skládá z cívky, jádra a překlápěcí kotvy. Po přivedení proudu do cívky vznikne elektromagnetické pole, které přitáhne překlápěcí kotvu a ta sepne dva kontakty. Po vypnutí elektrického proudu dojde k odtažení kotvy a rozepnutí kontaktů. Ovládací proud bývá obvykle velmi malý. V dnešní době se používají spínací, přepínací a rozpínací pomocná relé.

Bezdrátové vysílače – Jedná se o zařízení, pomocí kterých můžeme dálkově ovládat ústředny, spotřebiče, vyvolat tísňový poplach, ale také detekovat pohyb nebo otevření dveří. Tyto funkce jsou zajištěny vysíláním radiového signálu, který je přijat buď ústřednou, nebo přijímačem. Do vysílačů můžeme zařadit bezdrátové ovladače, detektory, nástěnné tlačítka a snímače.



Obr. 8: Bezdrátový magnetický snímač [8]

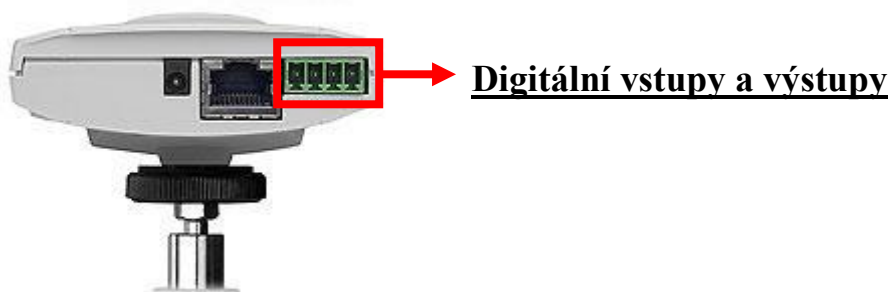
Bezdrátové přijímače – Tyto zařízení přijímají signály od ústředen, termostatů, ovladačů, snímačů a detektorů. Obsahují určitý počet nezávisle, bezdrátově ovládaných relé, díky kterým můžeme dálkově ovládat spotřebiče, osvětlení, ventilace apod.



Obr. 9: Bezdrátový modul silových relé [8]

GSM ovladače – jsou určeny pro ovládání příslušného výrobku nebo spotřebiče prostřednictvím GSM sítě. Tyto ovladače obsahují SIM kartu. Díky tomu můžeme příslušné zařízení ovládat na dálku, pouhým prozvoněním nebo odesláním textové zprávy. Ovladače mohou také odesílat textové zprávy a volat na mobilní telefony. Hlavní součástí GSM ovladače jsou výstupní kontakty silových relé a vstupní svorky, které mohou hlásit sepnutí a rozepnutí kontaktů (např. detektor zaplavení, magnetický kontakt apod.).

Alarmové vstupy a výstupy (I/O) komponent poplachových a nepoplachových aplikací - Pro integraci můžeme využít i produkty, které obsahují digitální a analogové vstupy/výstupy. Většinou se jedná o síťové kamery, do kterých lze připojit vnější zařízení. Vnějšími zařízeními může být cokoli od detektorů až po relé. Díky vstupům můžeme snímat určitou scénu jenom tehdy, pokud došlo k pohybu nebo jiné nastavené události. Tím odstraníme zbytečné přenosy záběrů, na kterých se nic neděje. V případě, že dojde k aktivování vstupu (např. detektor detekuje pohyb), můžeme nastavit různé akce pro výstup, které budou následovat: ukládání snímané scény, upozornění majitele odesláním SMS nebo emailu, popřípadě může dojít k aktivaci sirény nebo zamknutí dveří. [9]



Obr. 10: Síťová kamera s I/O konektory [9], upravil Kovařík, 2012

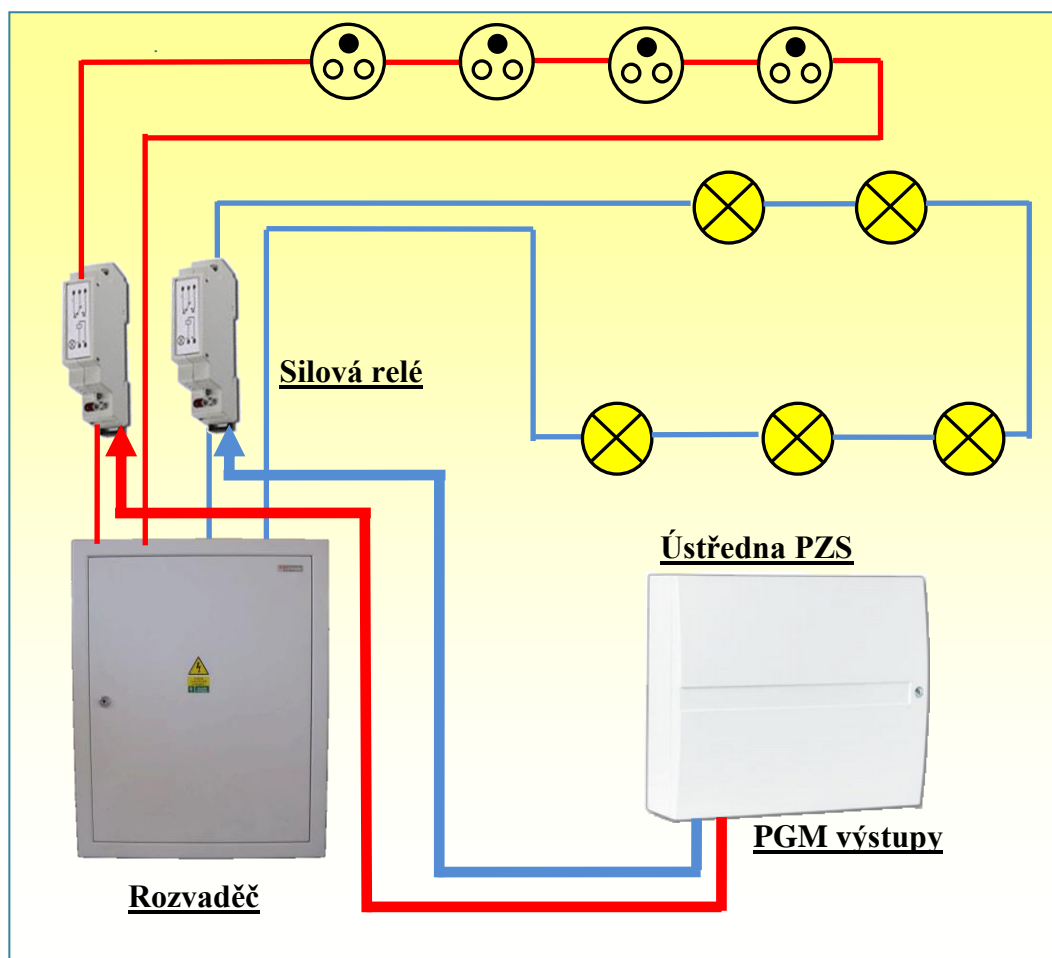
Digitální vstupy – na digitální vstupy můžeme připojit jakékoliv zařízení, které umí přepínat mezi otevřeným a uzavřeným okruhem. Patří sem tedy většina detektorů. Například: magnetické detektory otevření dveří, PIR (Passive Infrared detector) detektory, nášlapné koberce, poplachové fólie, apod. [9]

Digitální výstupy – umožňují nám pomocí kamery aktivovat vnější připojené zařízení, které následně provede požadovanou akci. Může se jednat o relé kontakty, sirény, GSM komunikátory apod. [9]

2.1.1.2 Možnosti integrace propojením vstupů/výstupů

Využití silových relé a PGM výstupů v oblasti ovládání osvětlení a zásuvek

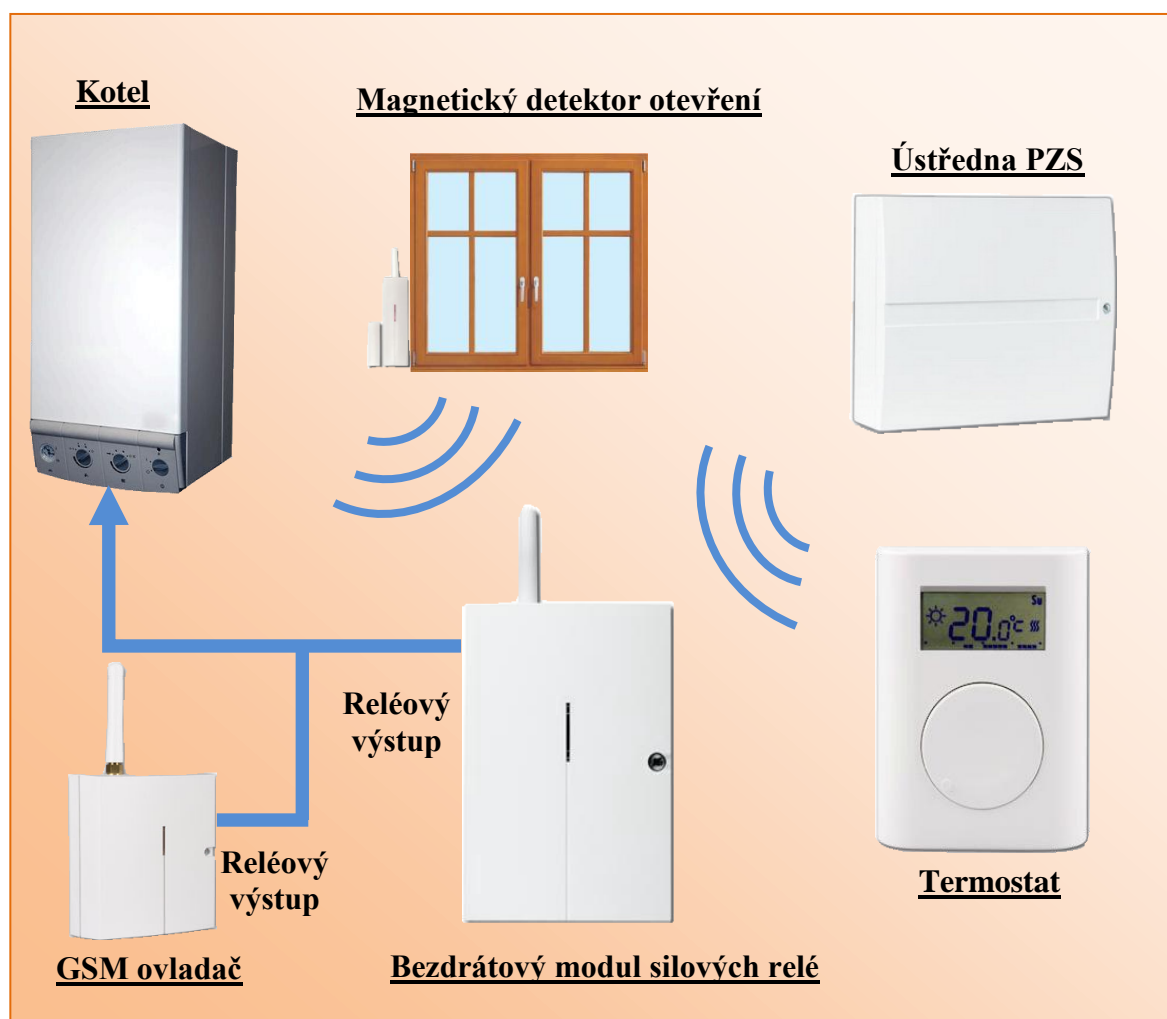
Ovládání jednotlivých prvků osvětlení je možno realizovat pomocí ústředny PZS (Poplachového Zabezpečovacího Systému), při odchodu z objektu. Pro propojení ústředny a elektrického okruhu, se využívají pomocná relé, která se buď spínají, nebo rozpínají. Na vstup relé jsou přivedeny vodiče od rozvaděče a signály od ústředny PZS. Výstupy jsou zapojeny do stanoveného elektrického okruhu, který chceme ovládat. Na *Obr. 11* se jedná o okruhy s osvětlením a elektrickými zásuvkami. Pokud odcházíme z objektu, nechceme, aby nám světla zbytečně svítla. Ústřednu si tedy naprogramujeme tak, že při zastřežení vyšle signál na vstup relé. Tím dojde k jeho rozepnutí a zároveň k přerušení elektrického obvodu pro osvětlení. Stejným způsobem dojde k vypnutí všech elektrických zásuvek. Díky tomuto řešení získáme ochranu před vznikem požáru, v důsledku nevypnutého elektrického spotřebiče. Vypnutím osvětlení ušetříme náklady za elektrickou energii.



Obr. 11: Příklad propojení ústředny PZS a elektrického okruhu

Aplikace bezdrátových vysílačů a přijímačů pro ovládání vytápění

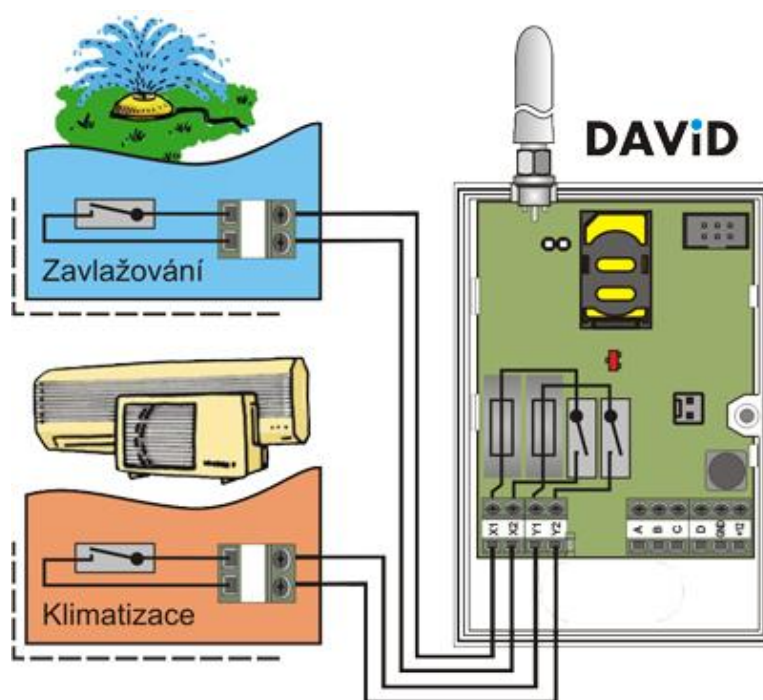
Teplotu v objektu můžeme ovládat pomocí bezdrátových vysílačů a bezdrátového modulu silových relé. Tento modul obsahuje relé, které sepne, pokud dostane signál od termostatu nebo ústředny. Modul je připojený ke svorkám kotle. Pokud tedy dojde k sepnutí relé, začne kotel topit. Na termostatu může být nastavena hodnota teploty, která se má dosáhnout. Po dosažení této teploty vyšle termostat rádiový signál a relé se rozezne. Topení můžeme také zapínat a vypínat pomocí programovatelných výstupů zabezpečovací ústředny. Jako bezdrátový vysílač můžeme použít také magnetický detektor otevření. Pokud ho umístíme na okno, bude nám zajišťovat, že se nebude topit v případě, když bude okno otevřené. Při použití GSM ovladače, můžeme topení ovládat pomocí telefonního hovoru, textové zprávy (SMS) nebo z internetu.



Obr. 13: Ovládání topení pomocí termostatu, ústředny a GSM ovladače

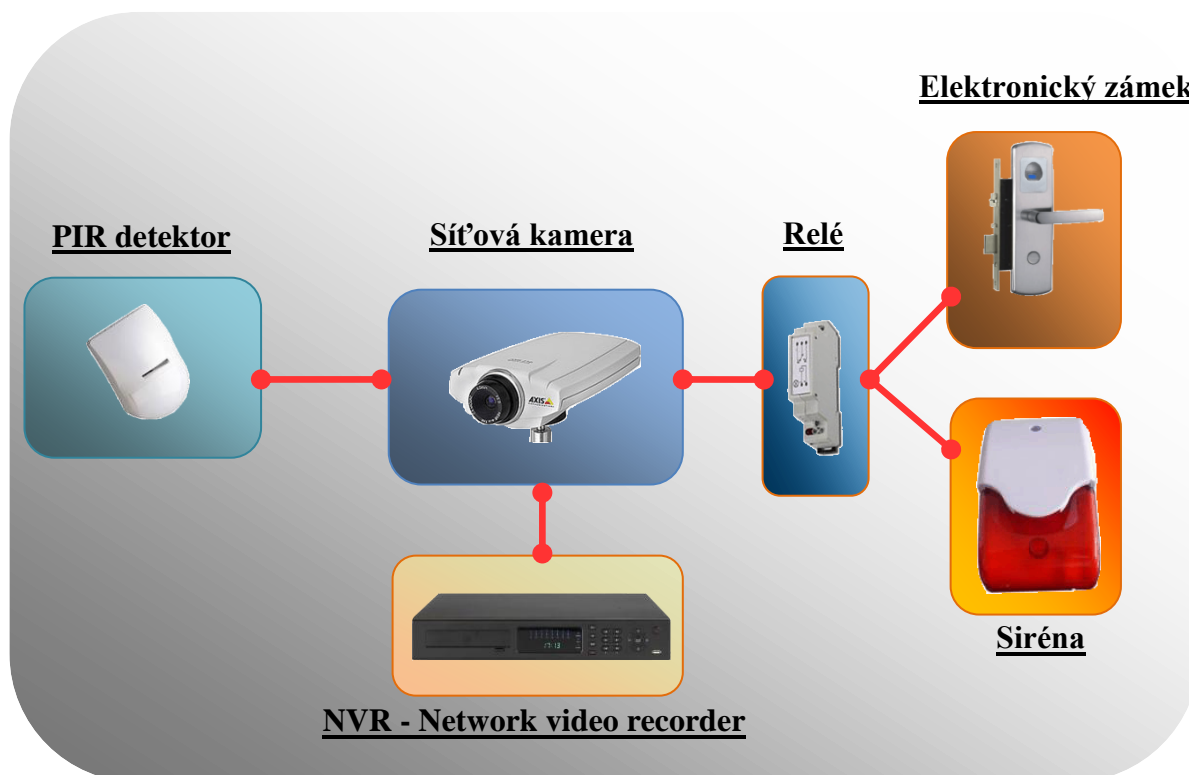
GSM ovladače

GSM ovladače jsou vlastně relé, které můžeme ovládat pomocí mobilního telefonu. Obsahují určitý počet výstupních kontaktů, které můžeme použít pro vypínání nebo zapínání námi požadovaného zařízení, pomocí SMS nebo pouhým prozvoněním. Prozvonění je zdarma, a proto se nejvíce využívá pro otevírání bran, závor a garážových vrat. GSM ovladač nám může sloužit také jako časový spínač, který lze ovládat mobilním telefonem. Díky vstupním svorkám můžeme být formou SMS informováni např. o výpadku napájení pro čerpadlo. Na Obr. 14 je znázorněno zapojení GSM ovladače DAVID od firmy Jablotron, pro ovládání zavlažování a klimatizace. Na jeden výstupní kontakt je připojeno spínání zavlažovacího systému a na druhý spínání klimatizace. Pokud na GSM ovladač odešleme SMS s přednastaveným textem, dojde k sepnutí nebo rozepnutí výstupního kontaktu a tím se zapne/vypne klimatizace či zavlažování. [10]



Obr. 14: Zapojení GSM ovladače pro ovládání zavlažování a klimatizace [10]

Další možností je zapojení, ve kterém budou nastaveny vazby mezi vstupy a výstupy. Příkladem je připojení detektoru zaplavení na vstupní kontakty a připojení čerpadla na výstupní kontakty. Pokud tedy dojde k sepnutí kontaktu detektoru zaplavení, sepne se zároveň i výstup, který ovládá čerpadlo.

Integrace pomocí síťové kamery s digitálními I/O

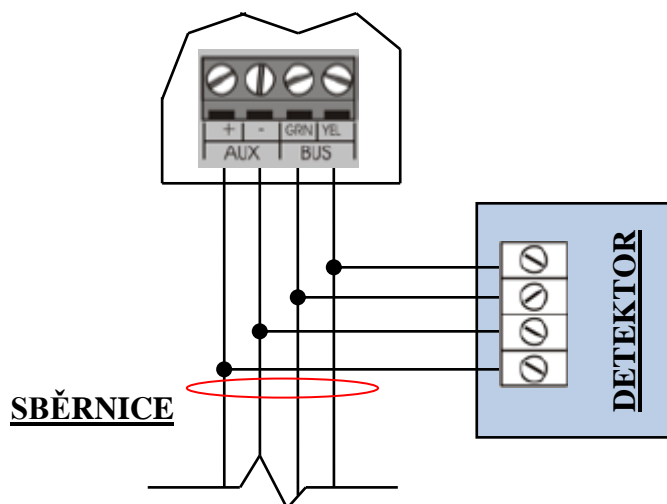
Obr. 15: Síťová kamera s digitálními I/O

Využití alarmových vstupů je velmi výhodné pro propojení CCTV a detektorů tak, aby kamera zbytečně nepoživovala záznam, na kterém se nic neděje. Podle Obr. 15 je vhodné použít PIR detektor, který detekuje pohyb. V případě detekce pohybu vyšle PIR detektor signál na digitální vstup kamery. Kamera poté pomocí digitálního výstupu zapne nahrávání na síťový videorekordér a začne pořizovat záznam. Digitální výstup z kamery může být dále připojen k pomocnému relé, které je schopno provést námi požadované akce, jako např. zapnout sirénu nebo uzamknout elektronický zámek.

2.1.2 Integrace přes sběrnici s využitím modulů

Druhým způsobem, jak integrovat jednotlivé aplikace, je využití sběrnice a modulů. Sběrnice (BUS) se obecně označuje jako soustava vodičů, pomocí kterých jsou propojena jednotlivá zařízení. Využívá se k propojení dvou a více stanovených aplikací, mezi kterými dochází k výměně informací. Pro propojení ústředny a jednotlivých modulů se nejčastěji používá 2 vodičová a 4 vodičová sběrnice.

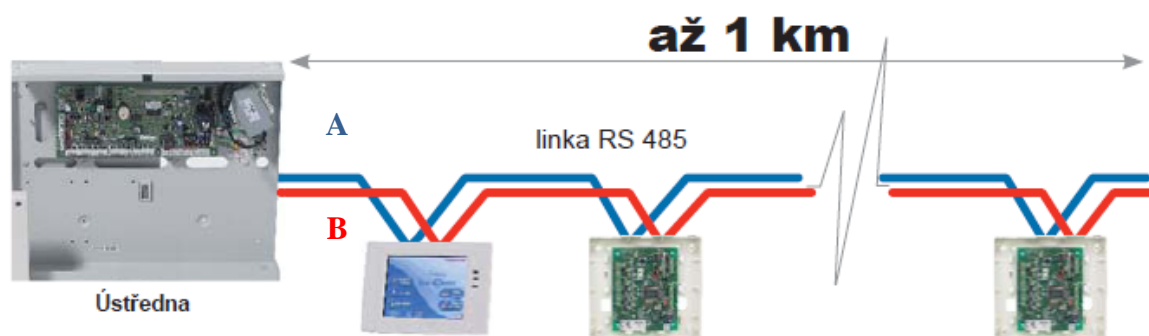
Čtyř vodičová sběrnice nám umožňuje vytvářet větve s dosahem stovek metrů. Dva vodiče slouží pro napájení a další dva pro přenos signálů. Ve vnitřním prostředí můžeme použít klasický, stíněný sdělovací kabel. Vnější prostředí vyžaduje kabel, který bude odolný proti vnějším vlivům. V oblasti integrace jsou sběrnice vybaveny konektory, na které můžeme připojit potřebné moduly.



Obr. 16: Připojení detektoru na sběrnici

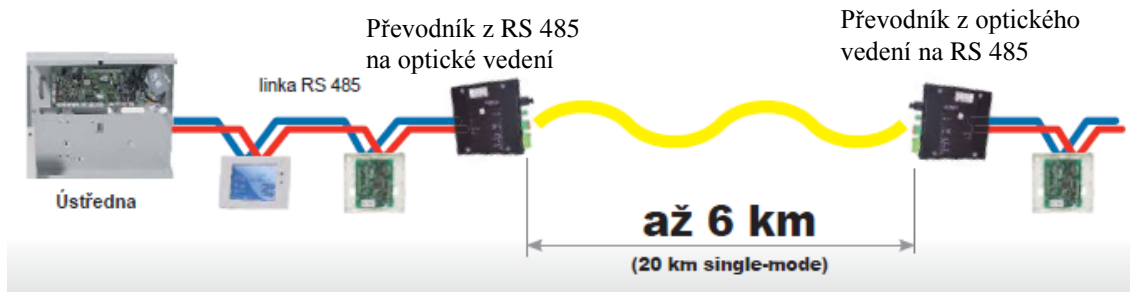
Sběrnici můžeme větvit a jednotlivé prvky řadit sériově, paralelně, do hvězdy a také vytvářet uzly a páteřní vedení. Maximální délka sběrnice se pohybuje okolo 900 metrů. Je ovšem důležité dodržet potřebné napájecí napětí pro všechny moduly. [11]

Dvou vodičová sběrnice se skládá pouze ze dvou vodičů, které slouží pro komunikaci a pro napájení modulů. Vodiče se obvykle označují A a B. Moduly se ke sběrnici připojují paralelně. Platí, že svorka A předchozího modulu se připojuje na svorku A následujícího modulu. Stejný postup se dodržuje i pro svorku B. Zapojení do hvězdičky a větvení není dovoleno. RS 485 je komunikační standard, který se používá především v průmyslovém prostředí (Obr. 17). [12]



Obr. 17: Zapojení modulů na sběrnici RS 485 [12]

Pro tuto sběrnici je vhodné použít datový kabel stíněný hliníkovou fólií. Na Obr. 17 je vidět, že maximální délka sběrnice se pohybuje okolo 1 kilometru. Tuto délku můžeme prodloužit pomocí optických převodníků a optického vlákna až na 6 kilometrů.



Obr. 18: Využití převodníků [12]

2.1.2.1 Sběrníkový systém

Základem většiny sběrníkových systémů je ústředna. Jednotlivé ústředny se od sebe odlišují především těmito vlastnostmi:

- počtem - zón, podsystémů, programovatelných výstupů PGM, uživatelských kódů,
- podporou určitého počtu rozšiřujících sběrníkových modulů,
- pamětí událostí,
- délkou sběrnice.

Ústředny tedy slouží k programování a komunikaci s jednotlivými prvky v systému a hlavně pro vyhodnocování příslušných signálů. Některé ústředny mají v sobě již integrovanou nadstavbu přístupu ACS. Ke sběrníkovému systému můžeme připojit:

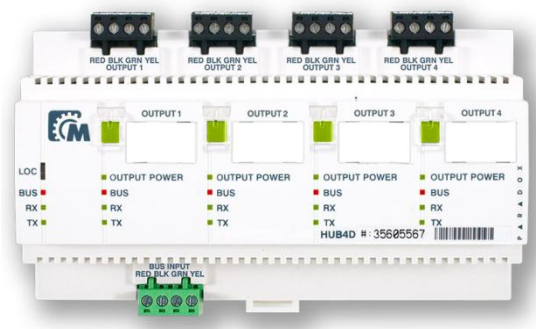
Klávesnice – jsou určeny k programování ústředny, ovládání systému a poskytují nám přehled o tom, v jakém stavu se nachází celý systém nebo podsystém. Dokážou nám signalizovat poruchy, narušené zóny nebo paměť poplachů. Využívají se dva typy zobrazování:

- klávesnice s LED diodami
- klávesnice s LCD displejem [11]

Sběrníkové detektory – tyto detektory se připojují přímo na sběrnici, pomocí které obousměrně komunikují s ústřednou. Tím je zabezpečena maximální rychlost přenosu informace. Nastavení vlastností detektorů a jejich naprogramování je umožněno pomocí LCD klávesnice, nebo vzdáleně přes programovací software. [11]

Moduly – díky modulům můžeme výhodně rozšířit možnosti použití sběrnice systému. Kromě modulů, které nám pomohou vylepšit zabezpečení, existují i moduly pro ovládání dalších technologií a zařízení. Každý modul má vlastní adresu, díky které může komunikovat s ústřednou. Mezi nejčastěji používané moduly patří: [11]

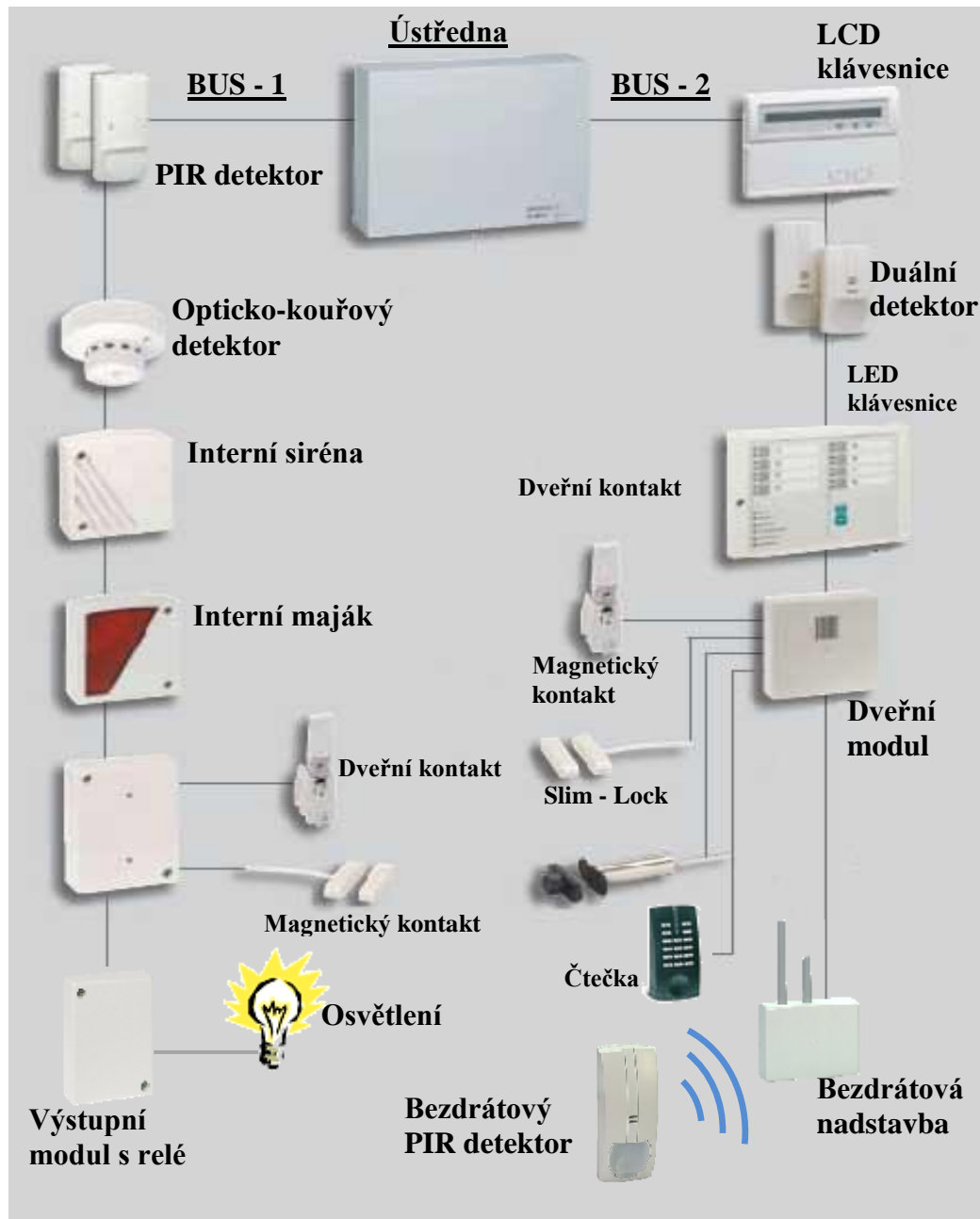
- Expandér zón – jedná se především o drátové expandéry, které nám umožňují rozšíření adresných zón.
- Modul PGM výstupů - tento modul nám slouží k rozšíření programovatelných výstupů.
- Dveřní moduly – slouží pro rozšíření sběrnice systému o kontrolu přístupu a umožňuje připojení čtečky, dveřního kontaktu, magnetického kontaktu nebo také dveřního zámku.
- Moduly bezdrátové nadstavby – jsou to rádiové přijímače/vysílače, díky kterým můžeme do systému připojit různé bezdrátové prvky, jako jsou např. PIR detektory, magnetické kontakty, ovládací klíčenky apod.
- Posilovače sběrnice – tyto moduly posilují a oddělují sběrnice. Většinou obsahují jeden vstup, na který přivedeme sběrnici od ústředny a 4 nezávislé výstupy. Každý z těchto výstupů musí být zvlášť napájený pomocí externího zdroje.



Obr. 19: Posilovač sběrnice [11]

- Modul pro tiskárnu – příklad modulu, pomocí kterého se nevylepší zabezpečení, ale umožňuje ovládání jiných zařízení, v tomto případě tiskárny.
- Moduly přístupu – používají se pro otevírání dveří, omezení přístupu a ovládání zabezpečovacího systému pomocí karet.

- Doplňkové zdroje – slouží pro udržení správného napětí na modulech.
- Převodníky – převádí sběrnici na optické vedení a zpět, čehož se využívá pro zvýšení dosahu sběrnice. Optické vedení je také odolné proti elektromagnetickému rušení.



Obr. 20: Struktura sběrnicevého systému [13] *upravil Kovařík, 2012*

2.1.3 Integrace pomocí systému domácí automatizace X10

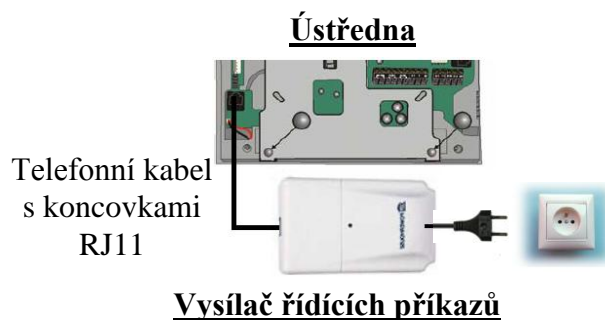
System domáci automatizace X10 predstavuje jednoduchý prostriedek, jak ovládat domáci spotřebiče a zabezpečení. Tento systém je založen na přenosu řídicích signálů po stávající rozvodné síti v domě – 230V/50Hz. Velkou výhodou je možnost nainstalování systému do již postavených domů, bez nutných stavebních úprav a velkých finančních a časových nákladů. Systém X10 můžeme využít všude tam, kde je přiveden rozvod 230V. Základním prvkem je vysílač řídicích příkazů. Na tyto příkazy reagují přijímací moduly, které mohou být zapojené přímo do sítě, nebo zasunuty do klasické zásuvky. Existují také moduly na DIN lištu, které můžeme umístit přímo do rozvaděče. Moduly jsou napájeny přímo ze sítě a nevyžadují žádný servis ani údržbu. Díky tomuto systému můžeme ovládat osvětlení, zavlažování, topení, klimatizaci, garážová vrata, rolety, domáci spotřebiče, zabezpečení apod. Aby se zabránilo šíření řídicích signálů mimo budovy, umísťují se na vstup sítě 230V fázové filtry. Tyto filtry slouží také jako ochrana před rušivými signály a zajišťují, že se řídicí signály dostanou do všech fází. [14]

Integrace s ústřednou PZTS se realizuje připojením vysílače řídicích příkazů k ústředně. Ústředna je poté zdrojem řídicích signálů, které jsou vysílačem převedeny z úrovně TTL do sítě 230V.

Identifikace jednotlivých modulů – aby nedocházelo k záměně jednotlivých budov a modulů, nastavují se dva identifikační parametry: [14]

- House code (kód domu) – tento kód se nastavuje na řídicím modulu, tedy na ústředně a na všech přijímacích modulech, které bude ústředna ovládat. Tím dojde k rozlišení a oddělení jednotlivých budov používajících X10. Vysílač tedy může ovládat pouze takové moduly, které mají stejný kód domu jako on.
- Unit code (číslo modulu) – přijímací moduly se ještě dále rozlišují pomocí čísla modulu. Toto číslo se přiřazuje také určité události na vysílači. Pokud tedy vznikne přednastavená událost, budou reagovat pouze ty přijímací moduly, jejichž číslo odpovídá číslu na výstupu X10, které je přiřazeno dané události.

Připojení ústředny do sítě 230V – ústředna se do sítě připojuje pomocí vysílače, který je zakončen vidlicí do zásuvky. Propojení vysílače a ústředny je realizováno telefonním kabelem s koncovkami RJ11. [14]



Obr. 21: Propojení ústředny se sítí 230V [14] *upravil Kovařík, 2012*

Provedení spínacích modulů [14]

Zásuvkový spínací modul – dálkově ovládaný spínač, který pracuje se stavy ZAPNUTO/VYPNUTO. Používá se pro spínání elektrických spotřebičů, které se připojují do zásuvky na přední straně modulu.

Spínací modul s vývody – má stejné vlastnosti, jako předchozí modul. Rozdíl je pouze v provedení. Umisťuje se do falešných stropů nebo přímo do ovládaných spotřebičů.

Univerzální modul – obsahuje výstupní relé, které můžeme použít pro spínání topení, klimatizace, alarmu, zavlažování zahrady, ale také pro připojení reproduktorů k audio zesilovači.

Spínací modul do objímky – tento modul se využívá ke spínání osvětlení. Jeho velkou výhodou je snadná montáž, kdy stačí tento modul našroubovat do objímky spínaného světla.

Spínací modul na DIN lištu – zařízení, které je připojeno k tomuto modulu, můžeme ovládat třemi způsoby. Prvním způsobem je ruční přepínač, který je umístěn na přední straně modulu. Druhý způsob je pulzní ovládání z tlačítka, které můžeme připojit ke svorkám tohoto modulu. Poslední možností je nucené ovládání z vypínače, kterým můžeme modul zapnout nebo vypnout. Vypínač je připojený ke svorce modulu.



Obr. 22: Zásuvkový spínací modul, spínací modul do objímky, spínací modul na DIN lištu [14]



Obr. 23: Struktura systému domácí automatizace X10 [14]

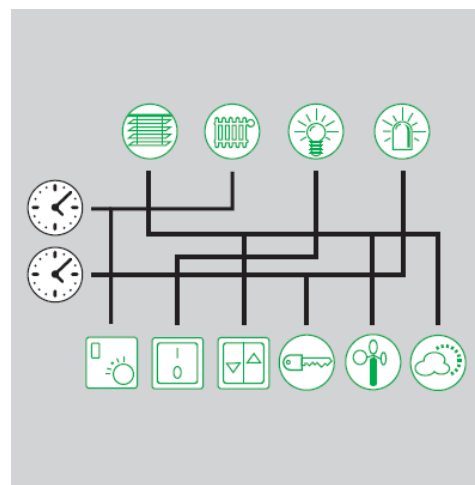
2.1.4 Integrace v rámci systémové elektroinstalace

Dalším způsobem, jak integrovat poplachové a nepoplachové aplikace pomocí HW, je využití inteligentní nebo také systémové elektroinstalace. Hlavní výhodou této elektroinstalace je to, že dokáže spojit jednotlivé technologie do jednoho funkčního celku. Umožňuje nám tedy ovládat a řídit jednotlivé technologie a procesy v budovách. Použití inteligentní elektroinstalace má velký vliv na přehlednost, komfort, bezpečnost a automatizaci. Dokáže také snížit náklady na energie. Nyní budou popsány základní rozdíly mezi klasickou a systémovou elektroinstalací.

Klasická elektroinstalace

U klasické elektroinstalace platí, že se skládá z několika okruhů - např. okruh pro osvětlení nebo okruh pro zásuvky. Velkou nevýhodou je, že každý spínací příkaz, každé měření, zpráva, ovladač nebo regulátor vyžaduje mnoho samostatných vodičů a kabelů. Z toho vyplývá, že všechny systémy používané v budově, potřebují svoje samostatné vedení a každý řídicí systém komunikační síť.

Všechny tyto aspekty vedou k nepřehlednosti instalace. Pokud bychom chtěli v této elektroinstalaci provést změny, budou vyžadovat značné stavební úpravy, a také finanční a časové náklady. U klasické elektroinstalace se neposílají žádné informace, ale dochází přímo k sepnutí obvodu pro stanovený spotřebič. [15]



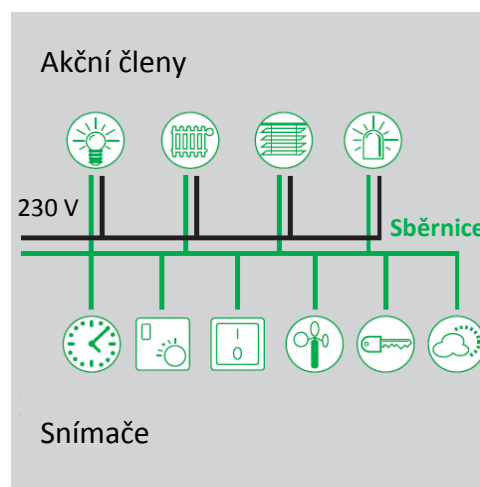
Obr. 24: Klasická elektroinstalace [16]

Inteligentní elektroinstalace (IE)

Základem inteligentní elektroinstalace je silové vedení 230V a sběrnice. Sběrnice umožňuje propojení jednotlivých aplikací. Sběrnice je dvou vodičová, jednoduchá, přehledná a dovoluje nám snadné rozšíření o další prvky. [15]

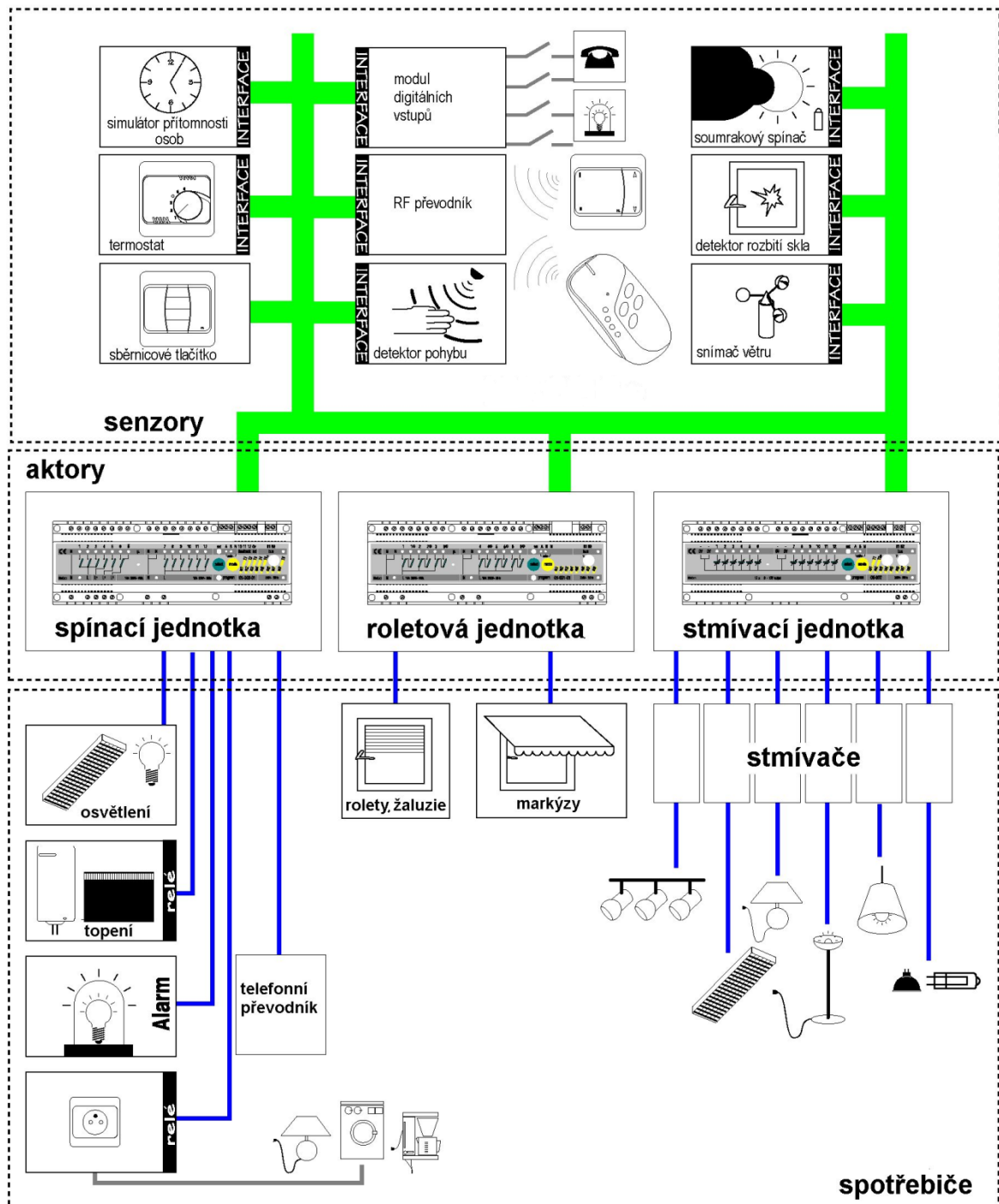
Do sběrnice můžeme připojit tyto zařízení: [15]

- systemové přístroje – řadíme zde napájecí zdroje, datové sběrnice, komunikační rozhraní, svorkovnice,
- snímače (senzory) – jsou to zařízení, které do systému přináší požadavky: tlačítkové ovladače, snímače počasí (vítr, déšť, světlo, teplo...), termostaty, detektory pohybu, hlásiče požáru, detektory rozbití skla, dveřní a okenní kontakty, binární vstupy,
- akční členy (aktory) – prvky, které vykonávají daný povel - akční členy pro spínání, stmívání, dále pro řízení žaluzií, tepla, alarmu apod.,



Obr. 25: Inteligentní elektroinstalace [16]

- řídící prvky (kontroléry) – jsou to logické členy nebo logické moduly, pomocí kterých se vzájemně logicky propojují snímače a akční členy. Tím je zajištěn vyšší počet komplexních funkcí.



Obr. 26: Struktura inteligentní elektroinstalace [17]

Popis funkce – Na sběrnici, která je napájena bezpečným napětím SELV, se připojují snímače, akční členy, systémové přístroje a řídící prvky. Snímače slouží k převádění akce,

kteřou získají např. od termostatu, tlačítka, snímače pohybu nebo uživatele, na datovou informaci. Tato informace je odeslána po sběrnici. Akční člen, kterému je daná informace směřována, ji vyhodnotí a provede vyžadovanou činnost, např. řízení žaluzií, stmívání, topení, spínání apod. Aby nemohlo dojít k záměně jednotlivých členů, má každý prvek v IE svoji jedinečnou adresu, díky které je umožněna snadná komunikace. Princip je tedy takový, že snímač odešle do sběrnice adresu. Akční členy „naslouchají“ a pokud má některý z nich nastavenou stejnou adresu, jako je adresa vyslaná, provede naprogramovanou akci. [18]

Bezpečnost v rámci IE – do systému IE můžeme integrovat různé bezpečnostní prvky:

- detektory pohybu,
- detektory rozbití skla,
- dveřní a okenní magnetické kontakty,
- hlásiče požáru,
- optickou a akustickou signalizaci,
- klávesnice,
- čtečky karet,
- elektronické zámky.

Tyto prvky můžeme připojit na sběrnici pomocí binárních vstupů, nebo bezdrátově, pomocí radiofrekvenčního RF modulu.

Příkladem použití může být detektor pohybu, který detekuje pohyb v objektu. Vyšle signál na spínací jednotku (aktor), která může provést naprogramované akce. Touto akcí může být zapnutí výstražného zařízení a osvětlení, zamknutí elektronického zámku dveří, nebo informování uživatele, popřípadě poplachového přijímacího centra o vniknutí pachatele do střeženého objektu.

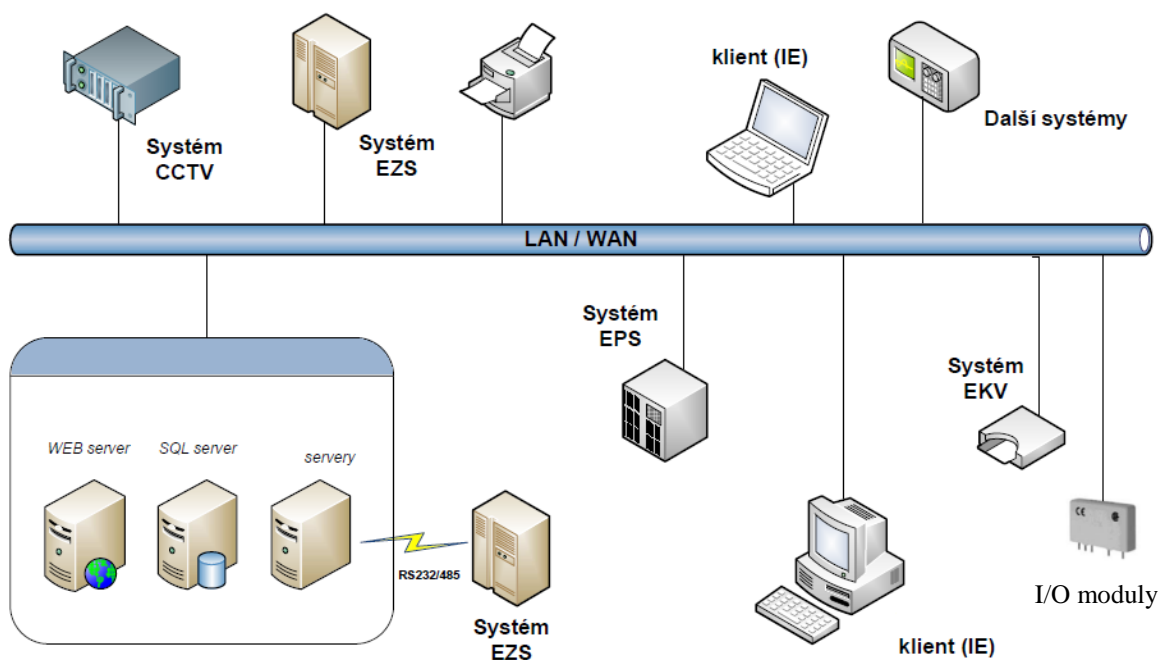
V případě, že požární hlásič vyhlásí požár, může roletová jednotka stáhnout rolety, aby zamezila dalšímu šíření ohně. Spínací jednotka dále může odemknout zámky dveří pro snadné opuštění objektu.

2.2 SW integrace

Integrace pomocí softwaru, dále jen SW, je jedním z dalších způsobů, jak propojit poplachové a nepoplachové systémy do kompaktního celku. Je vhodná pro použití v takových objektech, kde vzhledem na požadavky obsluhy nebo složitost objektu, není možné bez počítačové nadstavby dosáhnout přehledného monitorování a řízení objektu. Při této integraci se jednotlivé systémy nijak neovlivňují a nejsou na sobě závislé. Pro správnou činnost je potřeba využívat komunikační protokol, který bude podporován všemi připojenými aplikacemi. [19]

2.2.1 Integrace pomocí SW nástavby

Pod pojmem SW nástavba si můžeme představit univerzální program (grafické prostředí), díky kterému jsme schopni vytvářet aplikace monitorovacích a řídicích systémů. Uspadňuje nám správu a údržbu celého objektu, umožňuje zvýšení bezpečnosti a automatizaci některých činností. SW nástavby jsou založeny na architektuře klient/server, která umožňuje rozdělit monitorovací a výstražný systém mezi více počítačů. Tyto počítače se vzájemně propojují, za pomoci počítačových sítí – LAN, WAN, INTERNET. V architektuře klient/server je klientem vizualizační program, který slouží k zobrazování stavů a událostí sledovaného systému. Ke sledování tohoto stavu využívá data, která jsou posílána od ústředen, nebo jiných zařízení na servery. [20]

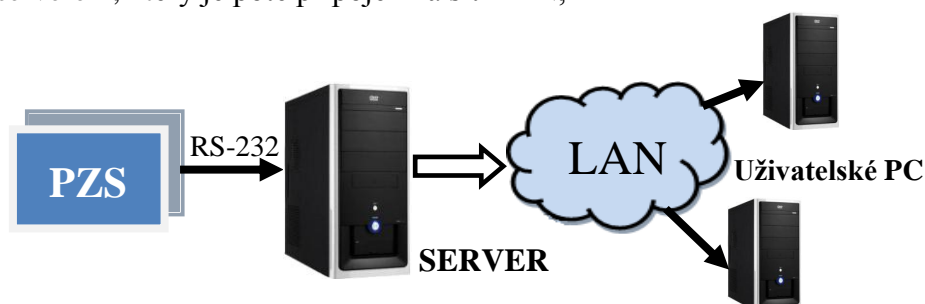


Obr. 27: SW nástavba [21]

2.2.1.1 Propojení jednotlivých systémů

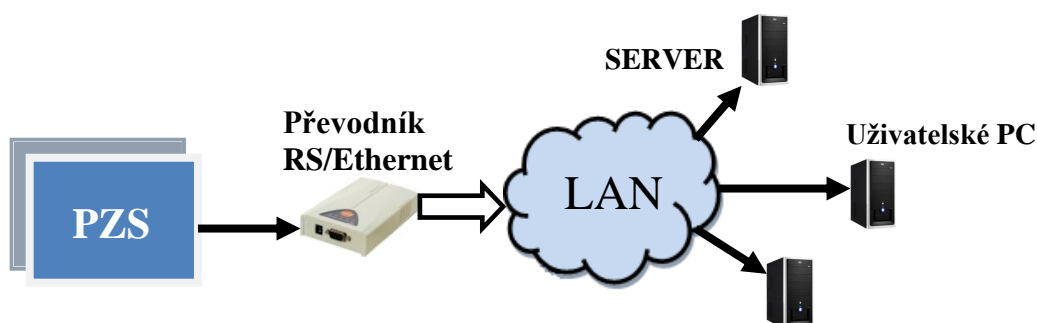
Většina zařízení, které chceme integrovat, obsahují porty RS-232 (komunikační rozhraní osobních počítačů), RS-422 (rozhraní pro vysokorychlostní komunikaci na větší vzdálenosti) nebo RS-485 (komunikační standard, který se používá především v průmyslovém prostředí). Díky těmto portům můžeme tyto systémy jednoduše propojit. Existují dvě varianty řešení: [22]

- a) přímé propojení se serverem – ústředna, popřípadě jiné zařízení se propojí přímo se serverem, který je poté připojen na síť LAN,



Obr. 28: První varianta propojení

- b) propojení přes převodník RS-232/Ethernet – potřebné zařízení se připojí na převodník RS/Ethernet, který je poté připojen do sítě LAN, WAN, Internet.



Obr. 29: Druhá varianta propojení

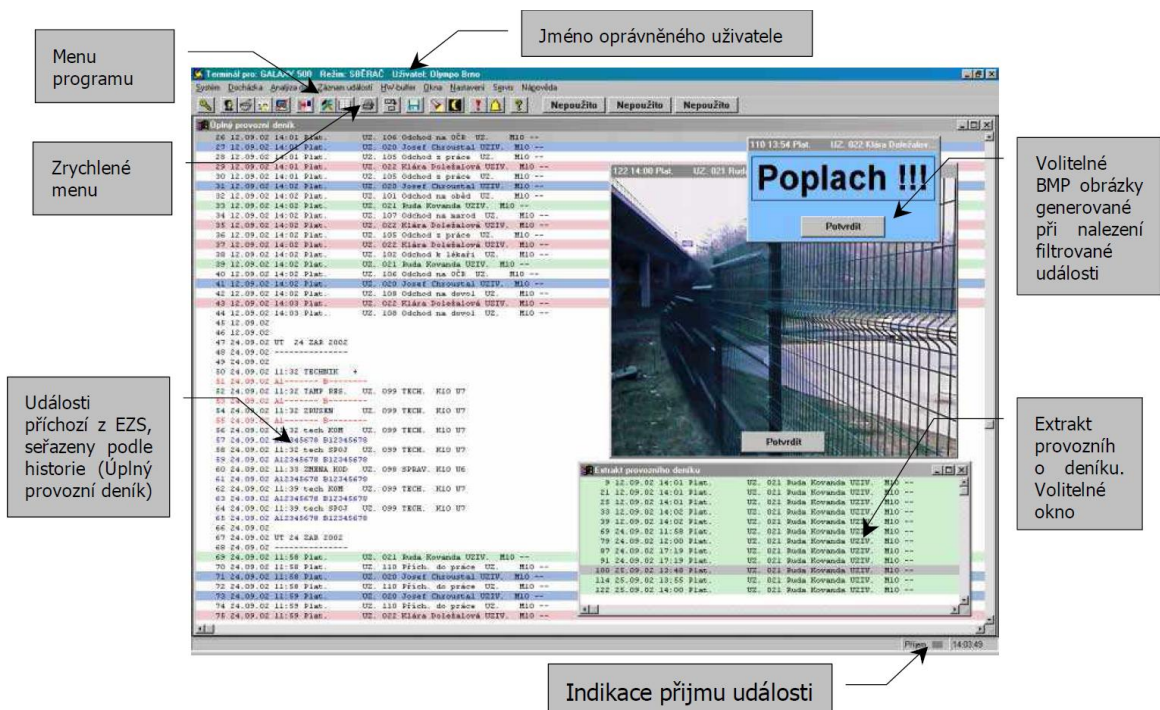
2.2.1.2 Funkce SW nástavby

Sběr a zpracování dat z jednotlivých systémů – mezi tyto systémy můžeme zařadit PZS, EPS, ACS, CCTV, ale i zařízení, která obsahují vstupně/výstupní moduly (jako jsou např. garážová vrata). Data obsahují informace o stavu zařízení, tzn., zda je zařízení zapnuté, jestli se někde nevyskytuje porucha, ale především hlášení poplachů a přenášení obrazů z kamer.

Vytváření výstupních informací – tyto informace jsou zpracovány pro uživatele tak, aby byly jednoznačné a srozumitelné. Využívá k tomu plány objektu a jednotlivé značky zařízení. Podklady si může uživatel zvolit sám. Díky plánům a označení zařízení, může aplikace vyznačit místo, kde vznikl poplach a zároveň ukázat obraz z kamery. Dále lze zobrazovat informace o tom, která zóna je zastřežena nebo odstřežena. Uživatel tedy získá ucelené informace o vzniklé události. Informace můžeme sledovat z jakéhokoliv počítače, připojeného k Internetu, pomocí webového prohlížeče.

Vytváření záznamů událostí – systém dokáže ukládat veškeré informace o dění v daném objektu. Díky této funkci kdykoliv zjistíme, k jaké situaci došlo, přesný čas události, zda bylo zastřeženo/odstřeženo. Máme také možnost sledovat pohyb osob po objektu. Tím odpadá potřeba jakékoliv administrativy a organizace.

Vzdálené ovládání bezpečnostních a ostatních technologií – uživatel může pomocí tohoto systému zastřežovat/odstřežovat celý objekt, nebo jeho určitou část. SW nastavba umožňuje také ovládat ostatní technologie pomocí I/O modulů (klimatizace, zavlažování, garážová vrata apod.). [23]



Obr. 30: Prostředí programu [24]

2.2.1.3 Bezpečnost

Díky tomu, že se do systému můžeme připojit odkudkoliv, je potřeba, aby byl dostatečně zabezpečen. Před nepovoleným přístupem je systém zabezpečen použitím firewallu,

omezením IP adres cílových stanic nebo využitím zabezpečeného HTTPS (HyperText Transfer Protokol Secure) protokolu. Ochrana před samotnými uživateli je řešena přidělením přístupových práv uživatelům, kteří mají svoje vlastní uživatelské jméno a heslo. Každý přístup do systému je navíc evidován do databáze. [21]

2.3 Dílčí závěr

První možnost HW integrace popisovaná v této práci – propojení vstupů a výstupů, je vhodná především pro rodinné domy a malé objekty. V případě použití u rozsáhlých objektů by tato možnost byla velmi náročná na návrh a instalaci systému. Naopak druhá možnost je vhodná zejména pro střední a velké objekty. Je to dáno tím, že se tento systém skládá ze sběrnice a modulů, pomocí kterých lze sběrnici rozšířit. Jak již vyplývá z názvu třetí možnosti integrace – domácí automatizace, je určena především pro použití v rodinných domech. Integrace v rámci inteligentní elektroinstalace patří mezi nejkompexnější způsoby integrace. Lze ji použít jak v malých objektech, kde je ovšem problémem vyšší cena, tak i ve velmi rozsáhlých prostorech.

SW integrace je vhodná pro použití ve všech různých typech objektů. Nejedná se ale o plnohodnotnou integraci, jde spíše o vizualizaci a ovládání připojených technologií.

II. PRAKTICKÁ ČÁST

3 INTEGRAČNÍ PRODUKTY

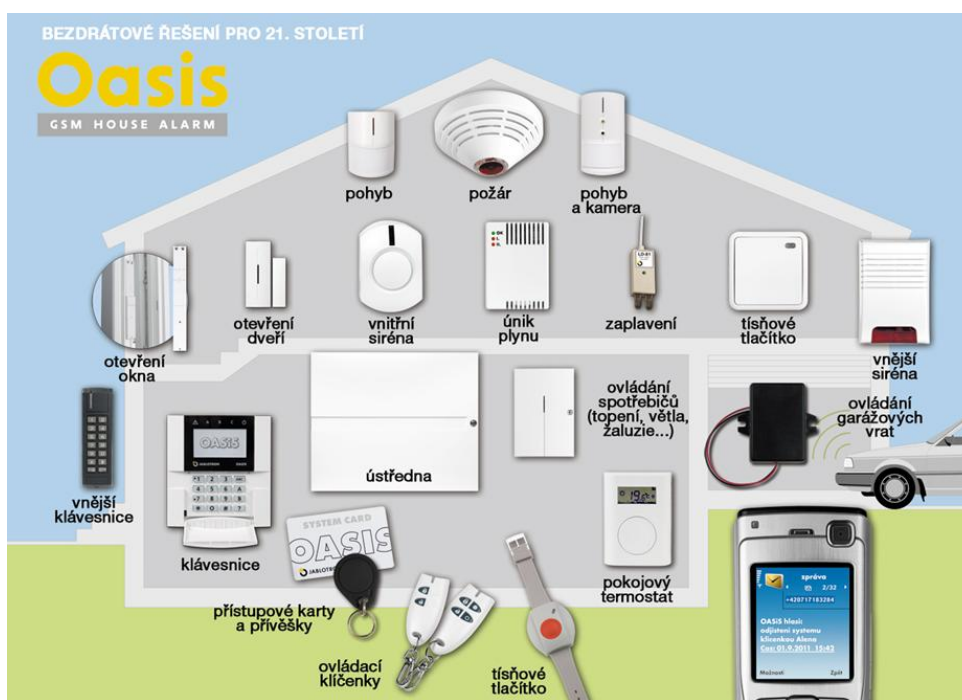
Třetí kapitola bakalářské práce se bude zabývat popisem a komparací produktů, které odpovídají klasifikaci technických možností integrace poplachových a nepoplachových aplikací, uvedené v předcházející kapitole.

3.1 Integrace propojením vstupů a výstupů

3.1.1 Jablotron - Oasis

Jedná se o bezdrátový zabezpečovací systém od české firmy Jablotron Alarms a.s. Systém lze ovládat pomocí klávesnice a dálkového ovladače, ale také přes mobilní telefon a internet.

Integraci umožňují dva PGM výstupy ústředny (PGX a PGY) a bezdrátové reléové moduly a termostaty. Příkladem využití může být např. vypnutí všech světel po zastřežení objektu, zatáhnutí žaluzií, zapnutí topení nebo zavlažování trávníku.

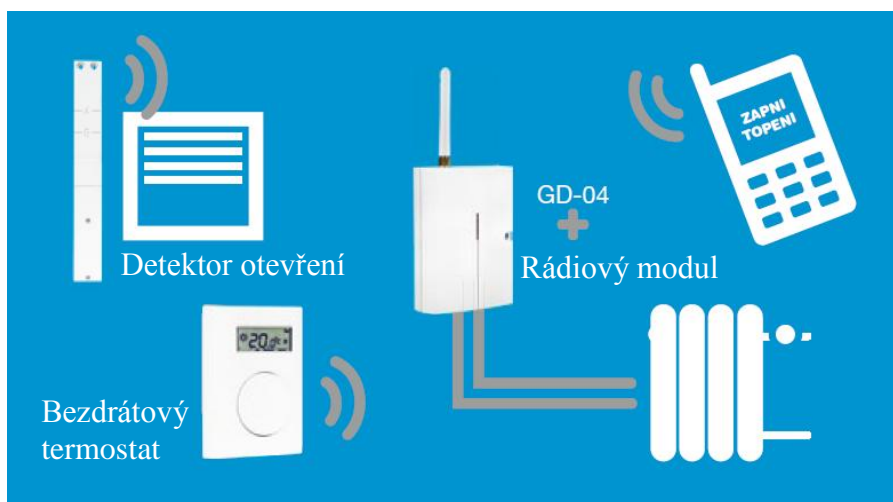


Obr. 31: Jablotron Oasis [25]

3.1.2 Jablotron – David

David, který je také označován jako GD-04 je univerzální GSM ovladač a hlásič. Obsahuje 2 výstupní relé a 4 vstupní svorky. Umožňuje zapínání a vypínání spotřebičů

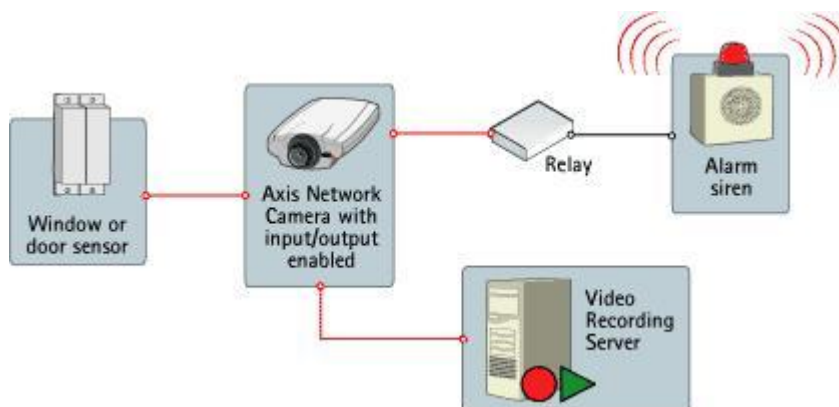
a střežení stavů. Ovládá se pomocí mobilního telefonu, na který jsou také odesílány zprávy o vzniklé situaci. Zapojením rádiového modulu do GD-04 je umožněna komunikace s prvky systému Oasis, tzn. detektory pohybu, magnetickými detektory, požárními hlásiči apod. [26]



Obr. 32: Příklad použití GSM ovladače David [26]

3.1.3 IP kamera AXIS 210

IP kamera AXIS 210 je vhodná pro zabezpečení vnitřních prostor objektu. Obsahuje vestavěnou detekci pohybu a digitální vstupy a výstupy, ke kterým lze připojit detektory, světla a alarmová relé. Mezi těmito vstupy a výstupy lze vytvořit vzájemné vazby. Příklad použití je uveden na Obr. 33, kde je na vstup připojený magnetický kontakt a na výstup videorekordér a výstražné zařízení. V případě sepnutí magnetického kontaktu dojde k nahrávání vzniklé situace a zároveň k signalizaci narušení. Tyto vstupy a výstupy lze spravovat přes síť, ze vzdáleného počítače nebo automatizovaně díky vestavěné logice v kameře. [9]

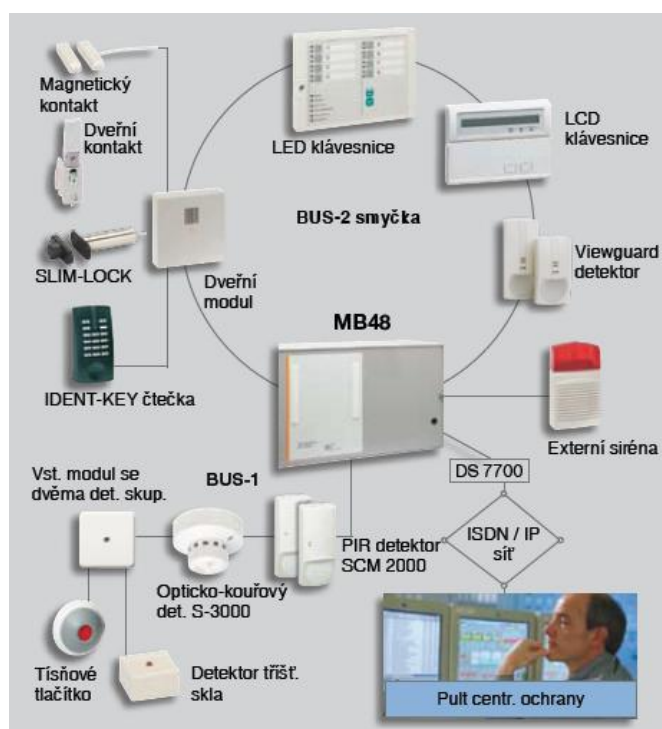


Obr. 33: Příklad použití IP kamery AXIS 210 [9]

3.2 Integrace přes sběrnici s využitím modulů

3.2.1 Honeywell - MB 48

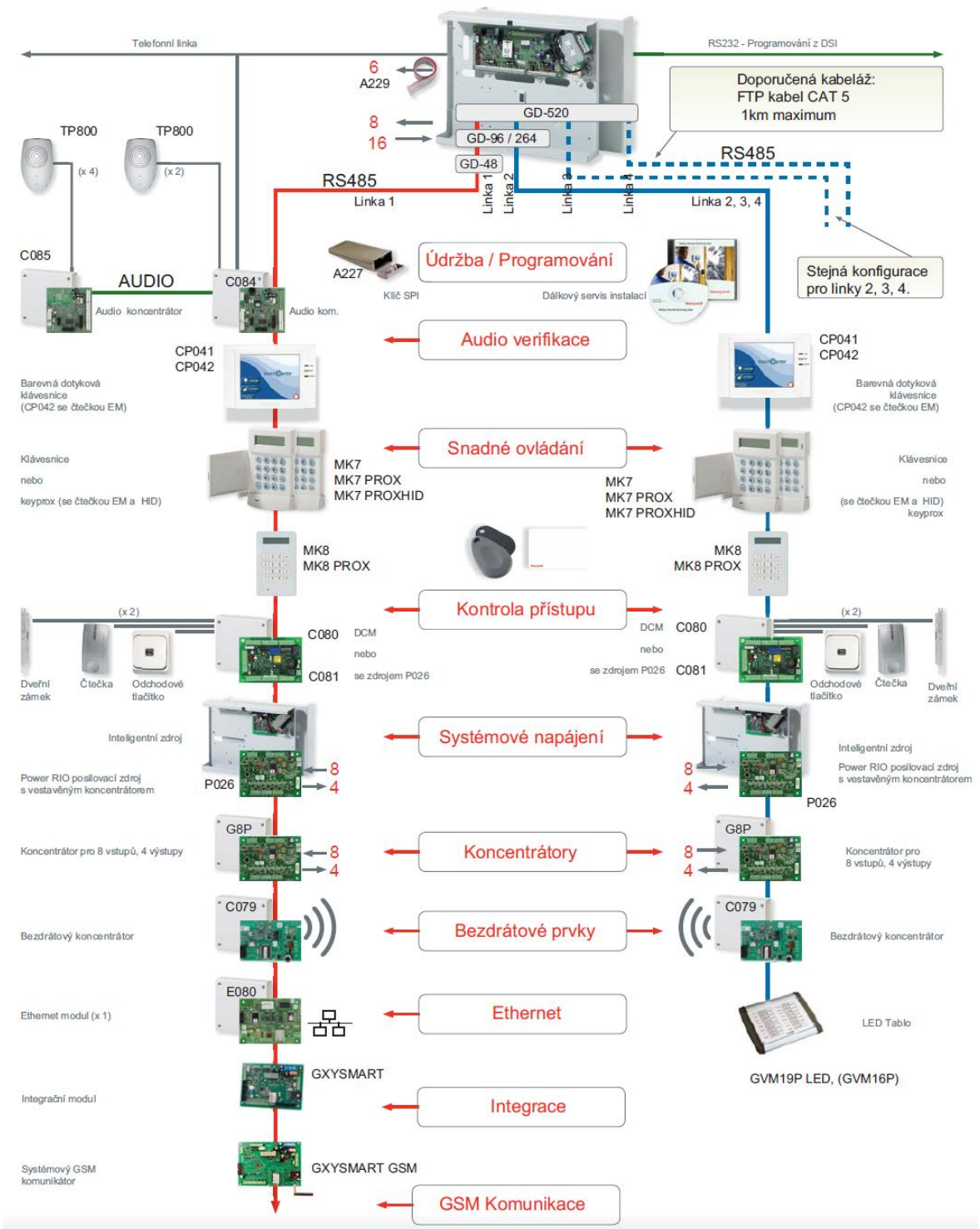
Základem systému je ústředna MB 48 a datové sběrnice BUS-1 a BUS-2. Jedná se o adresný systém, kde pro BUS-1 je 63 a pro BUS-2 64 připojitelných prvků v základu. Integraci umožňuje modulárnost systému, díky které můžeme ke sběrnici připojit jednotlivé moduly a zařízení. Pro integraci MB-48 s přístupovým systémem lze využít dveřní moduly IDENT-KEY. Mezi další dostupné moduly patří modul tiskárny, komunikační modul TCP/IP a také bezdrátová nadstavba pro připojení bezdrátových prvků. Pro rozšíření adres ústředny slouží moduly BUS-1 a BUS-2. [13]



Obr. 34: Struktura Honeywell – MB 48 [13]

3.2.2 Honeywell – Galaxy Dimension

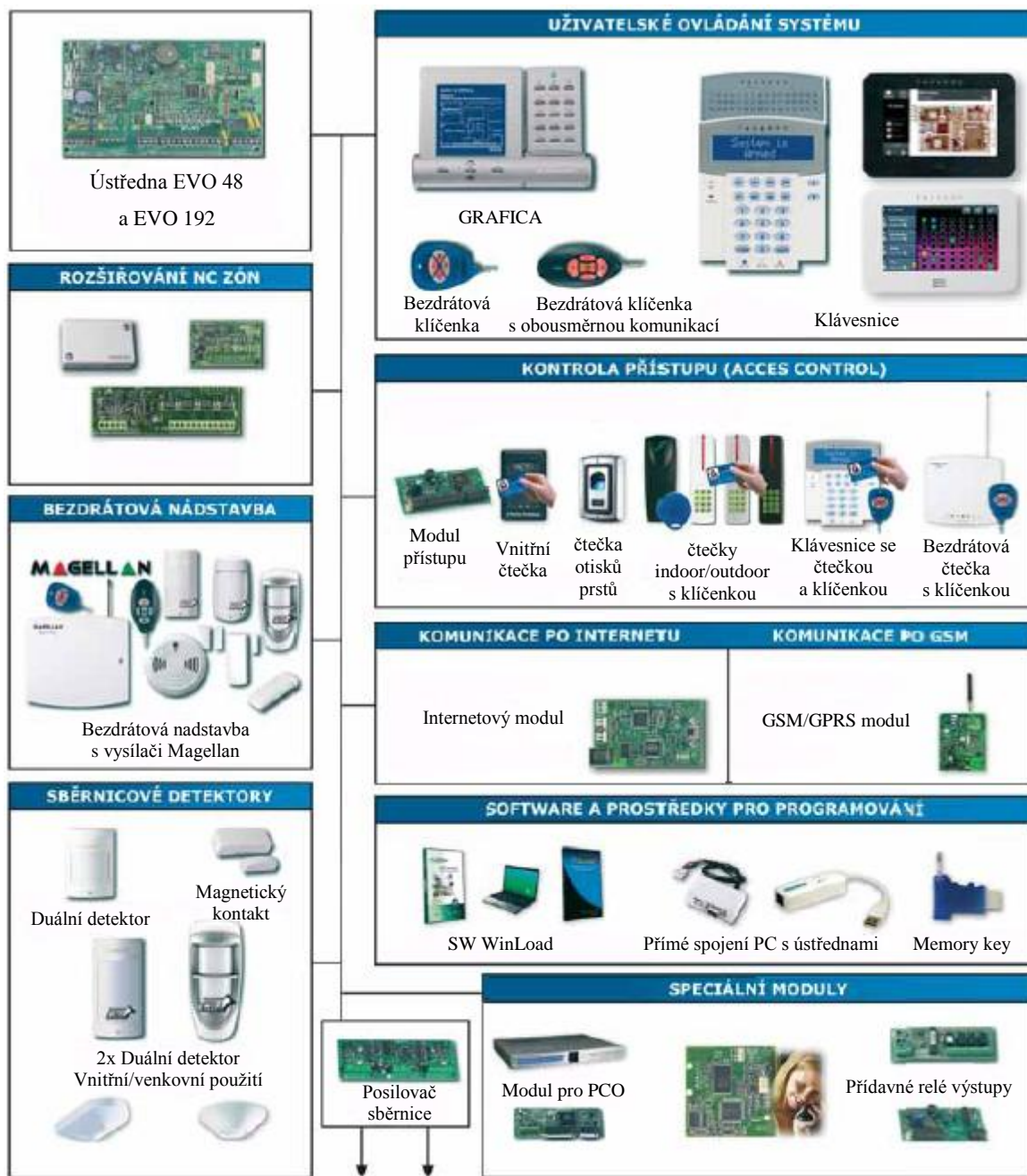
Jedná se o systém pro komplexní řešení zabezpečení a kontroly vstupu do objektu. K ústředně GD-520 lze připojit až 4 sběrnice, na které pak můžeme připojit potřebné moduly. Komunikace mezi ústřednou a těmito moduly probíhá po komunikační sběrnici RS 485. Moduly se ke sběrnici připojují paralelně. Integrace PZS a ACS je realizována pomocí dveřních modulů, ke kterým lze připojit dveřní zámek, odchodové tlačítko nebo čtečku. [12]



Obr. 35: Topologie ústředny Galaxy Dimension [12]

3.2.3 Paradox DIGIPLEX EVO

Základem systému je ústředna EVO 192 a sběrnice se čtyřmi vodiči. Maximální součet délky vodičů je 900 m. Dosah sběrnice lze rozšířit modulem pro posílení sběrnice. Počet modulů, které můžeme připojit na sběrnici je omezen na 256. Sběrnici můžeme větvit a jednotlivé prvky řadit sériově, paralelně nebo do hvězdy a vytvářet uzly a páteřní vedení.



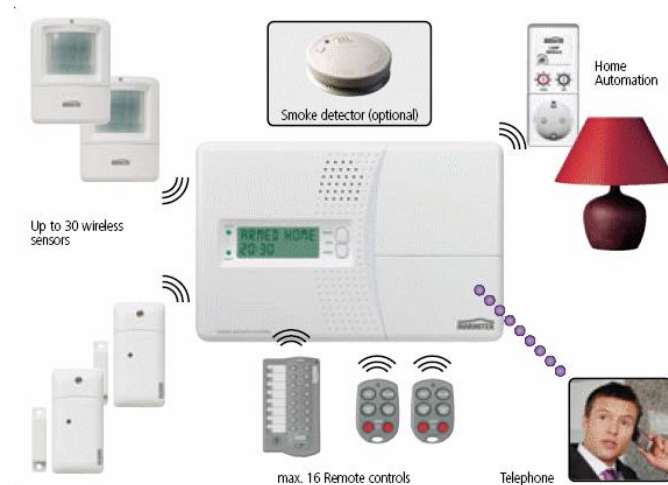
Obr. 36: Topologie systému Galaxy DIGIPLEX EVO [11], upravit Kovařík 2012

Mezi moduly, které lze připojit k ústředně, patří např. modul dálkové správy pomocí mobilního telefonu, modul LAN/INTERNET a modul pro vnitřní i vnější komunikaci. Pro integraci se využívají PGM výstupy ústředny nebo PGM moduly. Integraci s ACS umožňuje modul přístupu, který slouží k vytvoření 1 přístupového bodu – 1 čtečka, 2 detektory (magnetický kontakt, PIR detektor) a relé výstup pro otevření dveřního zámku. [11]

3.3 Integrace pomocí systému domácí automatizace X10

3.3.1 Marmitek TotalGuard

Jedná se o bezdrátový zabezpečovací systém, který v sobě integruje ovládání modulů domovní automatizace X10 přes klávesnici, dálkovým ovladačem nebo telefonem. Umožňuje naprogramovat simulaci přítomnosti osob, nebo v případě narušení prostoru zapnout světla či jiné spotřebiče v objektu. Pro ovládání X10 obsahuje 16 adres. K ústředně lze připojit 30 bezdrátových detektorů (detektor otevření dveří a oken, PIR detektor apod.) a 2 detektory po vodičích. [27]



Obr. 37: Topologie systému TotalGuard [27]

3.4 Integrace v rámci systémové elektroinstalace

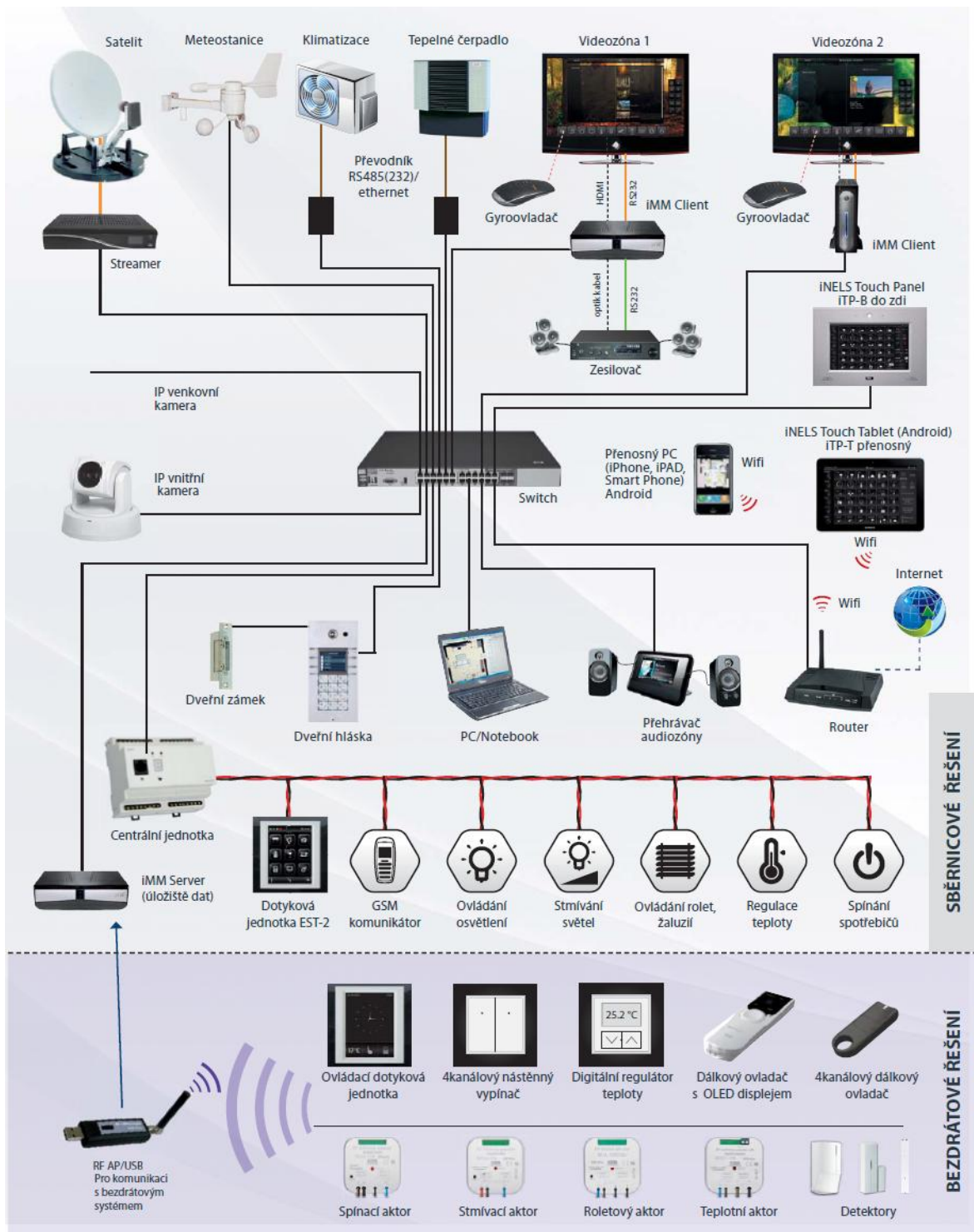
3.4.1 iNELS

iNels Smart Home Solutions je systém inteligentní elektroinstalace, který dokáže řídit celý dům, regulovat vytápění a klimatizaci, ovládat osvětlení, rolety, spotřebiče a také se starat o zabezpečení domu.

Základem je centrální jednotka CU2-01M, ke které lze připojit dvě sběrnice CIB (Common Installation Bus). Součástí centrální jednotky jsou i 4 bezpotenciálové vstupy, které umožňují připojení tlačítek, vypínačů, senzorů, detektorů apod.

Prvky PZS lze do systému připojit dvěma způsoby. Prvním je připojení přes jednotky binárních vstupů IM2-20B a IM2-40B.

Druhou možností je využití bezdrátového řešení, které je znázorněno na Obr. 38 [28]

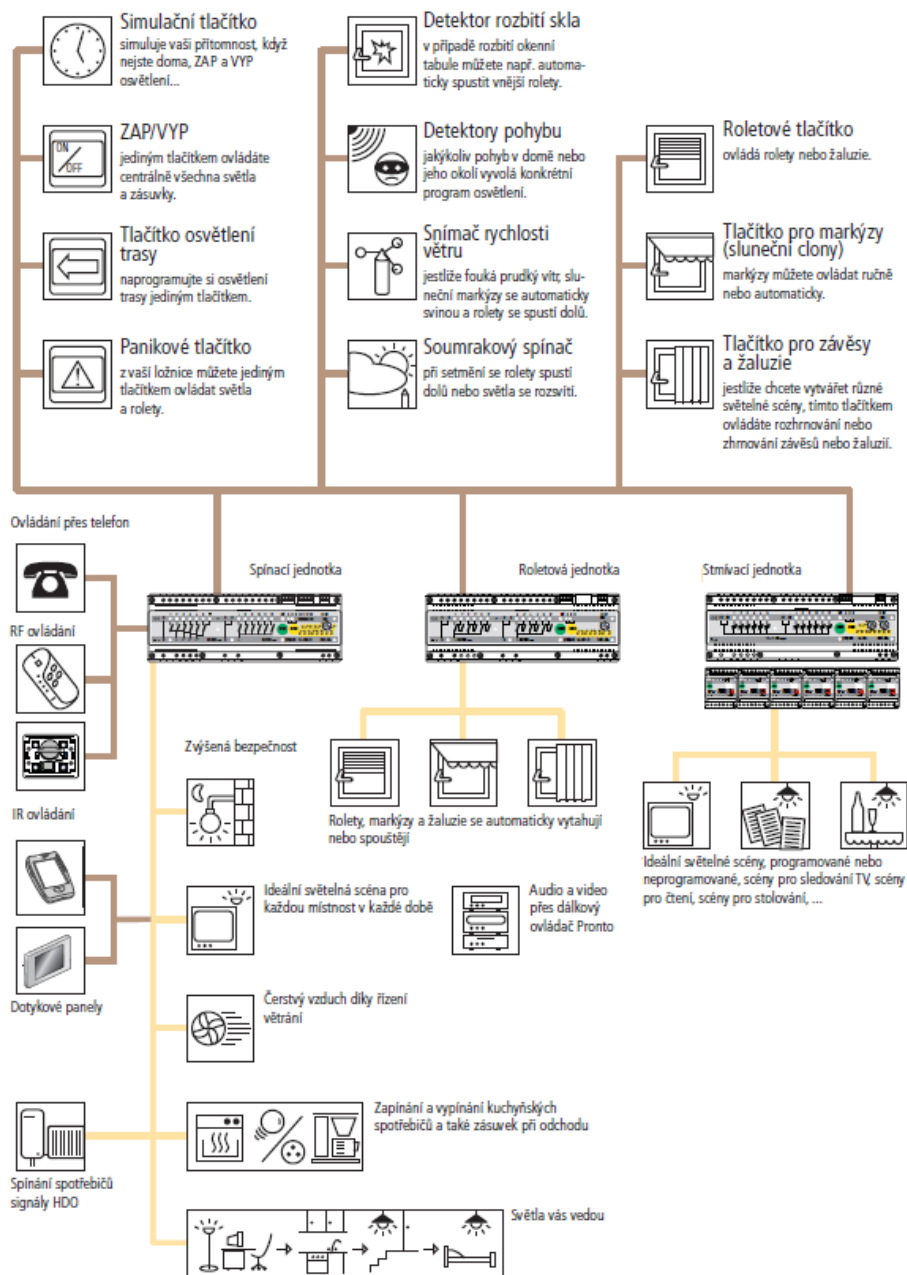


Obr. 38: Topologie inteligentní elektroinstalace iNELS [28]

3.4.2 Nikobus

System inteligentní elektroinstalace Nikobus je vhodný pro obytné budovy, rodinné domy, byty a malé podniky, kanceláře, hotely, obchodní centra apod. Umožňuje ovládat osvětlení,

rolety a žaluzie, příjezdové brány, garážová vrata, elektrické spotřebiče a to individuálně, nebo i centrálně ve skupinách. [29]



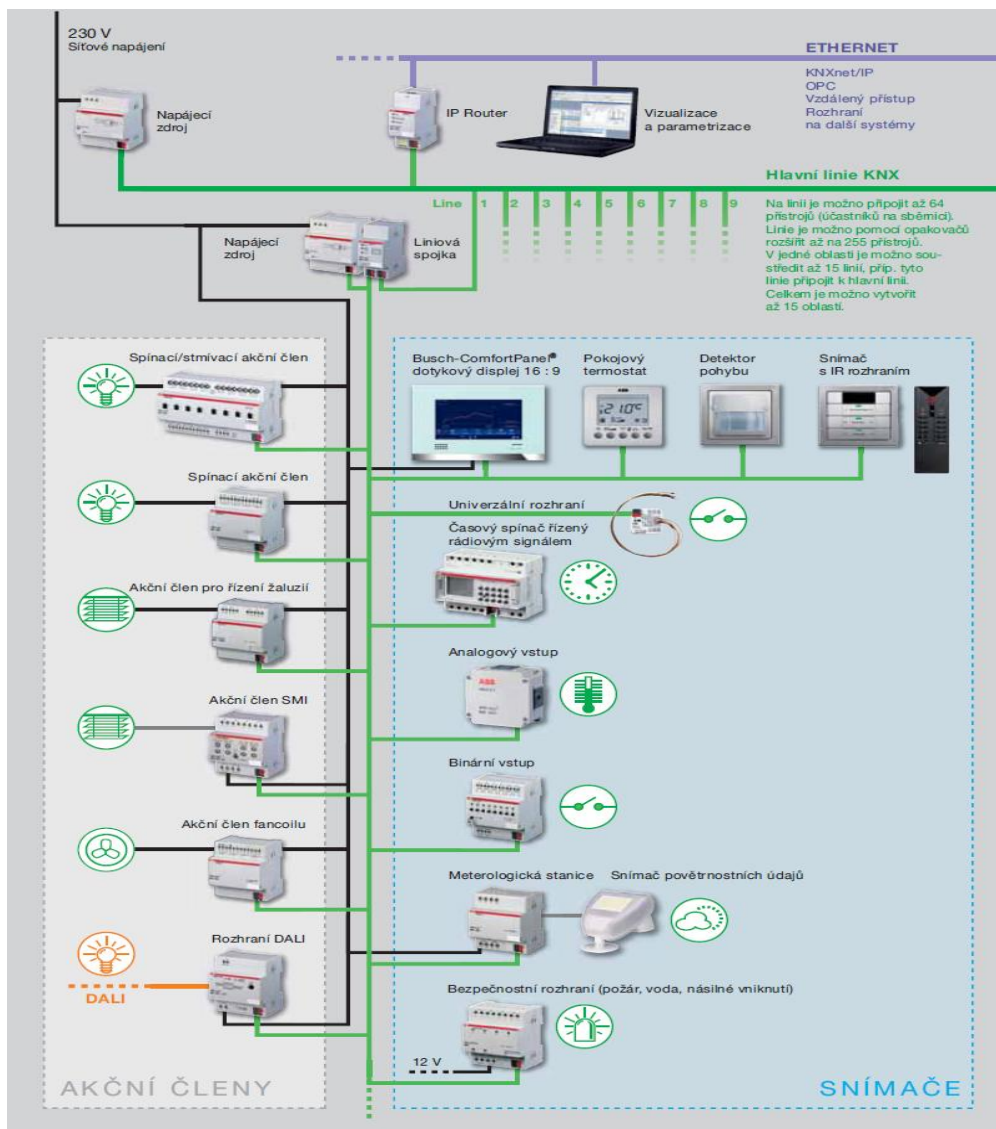
Obr. 39: Topologie systému Nikobus [29]

Sběrnice Nikobus se skládá ze 4 vodičů, 2 slouží pro napájení a 2 pro přenos dat. Prvky bezpečnostních technologií se do systému připojují pomocí modulů binárních a logických vstupů. Ty umožňují připojení bezpotenciálových kontaktů a snímačů, které mohou být v systému logicky vyhodnoceny - kontakty povětrnostní automatiky, senzor vlhkosti, tříštivé detektory, okenní kontakty, detektory kouře nebo zaplavení, PZS, EPS apod. [29]

3.4.3 ABB i-bus KNX

ABB i-bus KNX je systém inteligentní elektroinstalace, který je určen zejména pro komerční, velké a luxusní projekty. Systém se používá v oblastech osvětlení, řízení klimatu a spotřeby, zabezpečení objektů, automatizace, komunikace a vizualizace. Umožňuje tedy jedním systémem vyřešit kompletní elektroinstalaci a ovládání technologií v budově. Systém využívá dvoužilovou sběrnici KNX.

Bezpečnostní technologie můžeme do systému inteligentní elektroinstalace integrovat díky bezpečnostním terminálům, které lze použít samostatně, v kombinaci se zabezpečovací ústřednou nebo jako rozhraní mezi zabezpečovacím systémem a systémem ABB i-bus KNX. Obsahují vstupy pro připojení detektorů pohybu, magnetických kontaktů, snímačů otřesů skla apod. [16]



Obr. 40: Topologie systému ABB i-bus KNX [16]

3.5 Integrace pomocí SW nástavby

3.5.1 Alvis

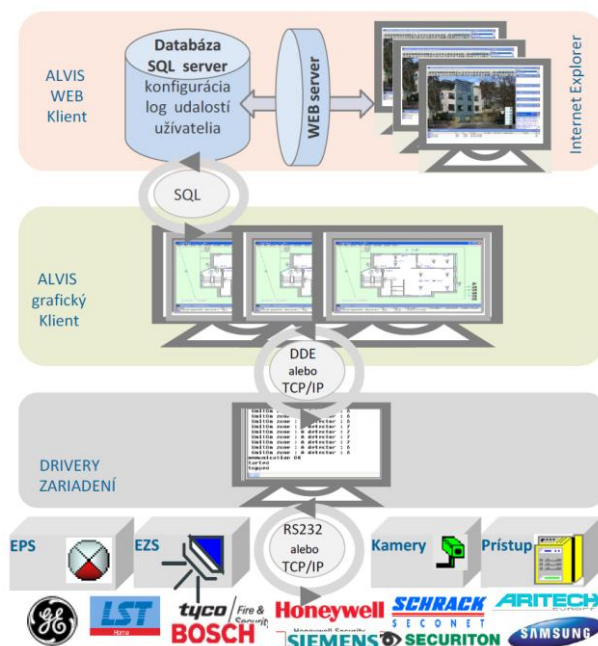
Grafický systém ALVIS (Alarm Visualization System) je produktem slovenské společnosti SPIRIT – informační systémy, a. s., která se zabývá návrhem a vývojem informačních systémů a poskytováním vlastních programů a služeb. Grafický systém ALVIS patří do kategorie systémů pro integrování, monitorování a řízení technologických zařízení objektů. Jedná se o nejrozšířenější produkt na českém a slovenském trhu. Umožňuje integrovat PZS, EPS, ACS, CCTV, měření, regulaci a ostatní systémy. [30]

Vlastnosti systému

Jedná se o systém, který je modulární a umožňuje kombinaci architektury klient/server respektive WEB server. Díky modulárnosti lze systém složit od jednoduché, jednouživatelské instalace, až po rozsáhlé distribuované síťové instalace klient/server respektive serverové instalace, které jsou vybaveny databázovým a WEB serverem. Díky WEB klientu můžeme do systému přistupovat přes klasický prohlížeč Internet Explorer. Grafický klient ALVIS v sobě kombinuje funkce:

- vývojového prostředí,
- "backend" RunTime komunikačního procesoru, což je funkce pro zpracování dat,
- grafického uživatelského prostředí.

Činnost grafického klienta vyžaduje ovladače zařízení, díky kterým dokážou komunikovat s ostatním připojenými zařízeními. Komunikace ovladače/serveru s grafickým prostředím respektive databázovým rozhraním, je řešena síťovým protokolem TCP/IP (Transmission Control Protocol/Internet Protocol), respektive s využitím DDE (Dynamic Data Exchange) protokolu. Počet ovladačů/serverů v síti není omezen. [30]



Obr. 41: Struktura systému ALVIS [30]

Režimy systému

ALVIS pracuje ve dvou režimech. První režim je nazván "Vývoj" a slouží pro navrhování monitorovacího a výstražného systému. Při práci v tomto režimu můžeme vkládat jednotlivé plány objektů a symboly pro hlásiče a zařízení. Druhý režim "Monitorování" je určený pro sledování a zobrazování všech událostí a vysílání příkazů pro připojená zařízení. [30]

Monitorování zařízení

Všechny prostory monitorovaného objektu jsou zobrazeny pomocí plánů, na kterých jsou umístěny symboly všech monitorovaných zařízení (detektor pohybu, hlásič požáru, kamery atd.). Pro každý z těchto symbolů lze nastavit chybové hlášení a stavy závislé na naměřených hodnotách signálů od zařízení. Každý stav může mít nastavené příslušné atributy: [30]

- chování symbolu – v případě, že nastal daný stav, lze nastavit blikání nebo zvukový signál symbolu,
- poplach – při poplachu můžeme nastavit:
 - prioritu poplachu,
 - oprávněnost potvrzení poplachu,
 - automatické zobrazení plánu, na kterém nastal poplach,
 - automatické potvrzení poplachu,

- poplachové zprávy - krátká zpráva, která se zobrazuje v přehledovém okně poplachů a 2 druhy podrobných zpráv s instrukcemi pro obsluhu,
- automatický tisk plánu a podrobných informací o poplachu,
- výstupy – povely vyslané na příslušné zařízení, automaticky nebo manuálně,
- protokoly – všechny události jsou zapisovány v protokolu událostí, společně s datem a časem události.

Zabezpečení systému

Systém je chráněn pomocí hesel a přístupových práv. Je vytvořen seznam uživatelů s hesly a po přihlášení může uživatel vykonávat jen ty úlohy, které má povoleny v přístupových právech. Tím je zajištěna ochrana proti neoprávněné manipulaci. [30]

Technické požadavky - Procesor: PC Pentium, Operační paměť: 512 MB RAM, Pevný disk: 120 GB, Operační systém: MS Windows 2000/XP/Win7/server 2003/2008

Cena: 64 464,-Kč

3.5.2 VAR-NET INTEGRAL

VAR-NET INTEGRAL je software pro integraci, správu a kontrolu bezpečnostních systémů (PZS, EPS, CCTV, ACS) a přídatných modulů. Tento softwarový produkt nabízí firma VARIANT plus, spol. s r.o., která byla založena roku 1992, sídlí v Třebíči a specializuje se na elektronické systémy budov.

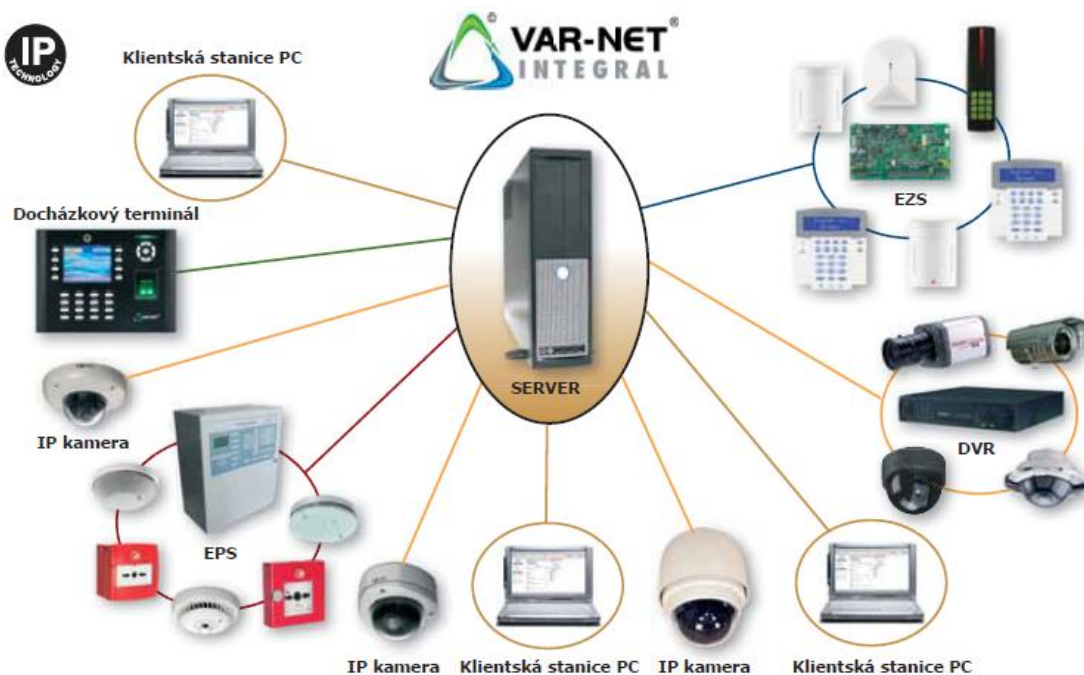
Popis systému

Základní funkcí systému je možnost sledovat události v objektu, popřípadě je aktivně řídit. Jedná se o modulární software, díky kterému může zákazník využívat pouze ty funkce, které bude potřebovat. Skládá se z jednotlivých modulů, které jsou vzájemně provázány, avšak mohou pracovat také samostatně. Do programu jsou zařazeny následující produkty jednotlivých systémů: [11]

Tabulka 3: Produkty jednotlivých systémů

PZS - ústředny	DIGIplex EVO, v budoucnu IMPERIAL
CCTV	IP kamery ACTi, DVR Micro Digital
EPS	JOB detectomat
ACS	Terminály VAR-NET

Je zde také možnost zajistit integraci technologií i s jinými výrobci (ústředny GALAXY, kamery AXIS, EPS SIEMENS apod.) Software tedy slouží pro sledování, správu a vyhodnocování těchto systémů v objektu. VAR-NET INTEGRAL je postaven na architektuře typu server – klient. Díky tomu můžeme pro ovládání využít jakýkoli počítač, u něhož je nainstalován prohlížeč Windows Internet Explorer. Protože systém podporuje protokol TCP/IP, není instalace softwaru omezena lokální sítí. [11]



Obr. 42: Okruhy systému VAR-NET INTEGRAL [11]

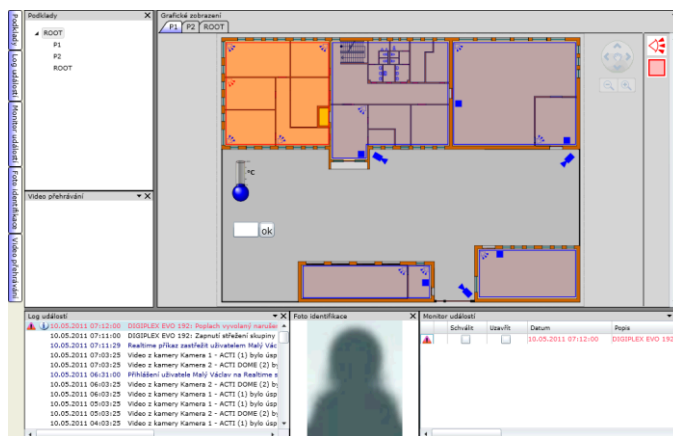
Řešení tohoto systému umožňuje současně obsluhovat 6 okruhů. Obvyklé využití je následující: 1 okruh= ústředna PZS, 1 okruh= ústředna EPS, 1 okruh= CCTV kamery (maximálně 16), 1 okruh= docházka. Technologie se do systému připojují pomocí protokolu TCP/IP, komunikačního portu RS-232 nebo technologie GPRS (General Packet Radio Service). [11]

Základní funkce a vlastnosti

Bezpečnost – důležitým požadavkem na tyto programy je vzdálený dohled a ovládání ústředny a požárních senzorů, kontroly vstupu, kamerových a bezpečnostních systémů. Vizualizace a sjednocení ovládání nám zpřehledňuje a zjednodušuje ovládání všech bezpečnostních prvků. Systém pořizuje záznamy o činnosti operátorů systémů a umožňuje nastavit automatizované vazby mezi připojenými technologiemi. Řízení a logování probíhá podle zadaných pravidel.

Management lidí a prostředků – jde o oblast, která je v programu nejobsáhlejší. Umožňuje mnoho možností nastavení a změn.

Správa a vyhodnocení – bezpečnost a snadná orientace je zajištěna centralizací a přidělením práv jednotlivým osobám. Díky architektuře programu můžeme snadno systém využívat a konfigurovat, při splnění požadavků na pohodlí a ekonomickou stránku. [11]



Obr. 43: Prostředí systému VAR-NET INTEGRAL [31]

Modularita a flexibilita – jelikož se jedná o stavebnicový systém, může být vybaven jen těmi moduly, které si zákazník přeje. Také rozšíření o ostatní moduly je velmi jednoduché.

Otevřenost – systém není závislý na HW prvcích a jeho vývoj následuje nejnovější požadavky.

Jednoduchost a nenáročnost – ovládání je podobné jako u operačních systémů MS Windows, tzn. rozhraní je intuitivní a uživatelsky příjemné.

Technické požadavky - Procesor: 2 jádrový s frekvencí 2Ghz, Operační paměť: 2 GB, Pevný disk: 100 GB, Operační systém: Windows 2003/2008 server. [11]

Cena: 47 000,-Kč

3.5.3 TEGAL

Tegal je grafický monitorovací a terminálový program s vyhodnocením docházky. Tento program pochází od firmy Honeywell, spol. s r.o. – Security Products, se sídlem v Brně. Tato firma se zabývá distribucí a integrací zabezpečovacích technologií.

Popis programu

Tegal je program vhodný pro monitorování, sběr a záznam událostí z ústředí PZS a EPS. Tento program využijí zejména:

- správci systému PZS,
- pracovníci ostražky a bezpečnostní technici,
- řídicí pracovníci.

V programu můžeme vytvářet vazby mezi jednotlivými událostmi a objekty díky tomu, že se jednotlivé události zobrazují v řádcích. Tyto vazby mohou být zobrazeny pomocí grafických nebo audio prvků. V případě, že dojde k přednastavené události, zobrazí se mapa a fotografie objektu, dále také fotografie a informace o uživateli. Je zde také možnost upozornění pomocí zvuku, SMS nebo e-mailu.

Správu databáze obstarává 32-bitový Borland Database Engine, který zajišťuje její konzistenci a neporušenost.

Zabezpečení proti neoprávněné manipulaci je řešeno stejným způsobem, jako u předchozích programů, tzn. uživatelským jménem, heslem a přidělením přístupových práv jednotlivých uživatelů, k jednotlivým funkcím. [24]

Kompatibilita s jednotlivými technologiemi: [24]

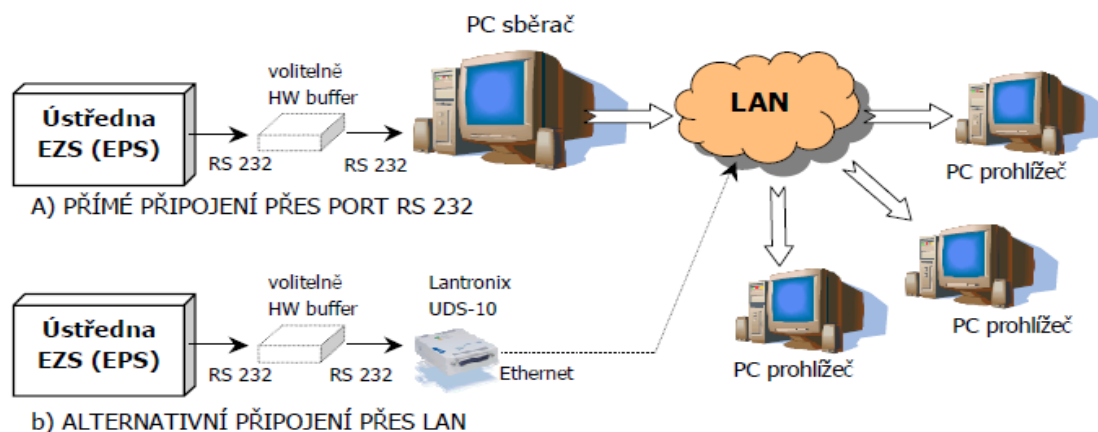
Tabulka 4: Kompatibilita technologií s programem

<u>PZS</u>	Ademco-Microtech(GALAXY 18 až 512)
	Rokonet (OrbitPro)
	DSC
	Europlex (Aplex), Inner Range (Concept)
<u>EPS</u>	LitesMHU 109
	Zettler LOOP 500, Expert
	ESSER

Struktura programu – program pracuje ve 2 pracovních režimech – sběrač a prohlížeč. V režimu sběrač je počítač s programem TEGAL propojen s monitorovanou ústřednou, pomocí komunikačního portu RS-232 nebo pomocí protokolu TCP/IP. Jak již vyplývá z názvu, slouží pro sběr dat a vytváření databáze událostí. Používají se dva typy databáze – společná a privátní. Společná databáze je taková, která sdílí tabulky pro režim sběrač

i prohlížeč. Tabulky v privátní databázi mohou být rozdílné pro každou připojenou stanicí (např. filtry pro jednotlivé události).

Pro režim prohlížeč platí stejné podmínky jako pro režim sběrač. Rozdíl mezi těmito režimy spočívá ve způsobu, jakým režim získává data. Aby režim prohlížeč získal data, musí nahlédnout do společné databáze vytvořené režimem sběrač. [24]



Obr. 44: Možnosti propojení [24]

Nejčastějším způsobem je použití jednoho počítače ve funkci sběrač a ostatních počítačů, připojených do sítě, ve funkci prohlížeč. Počet počítačů prohlížeč je omezen licenci.

Vlastnosti programu

Jako zdroj dat si můžeme definovat vlastní ústřednu. Je zde také možnost připojení jiných zařízení, podporujících výstup dat pomocí RS-232. Program také podporuje HW buffer, který slouží pro ukládání dat.

Všechny události jsou ukládány do databáze nazvané ÚDP (Úplný Provozní Deník). Počet uložených událostí je omezen pouze velikostí disku. Události můžeme exportovat do textového souboru, nebo vytisknout přímo na tiskárně.

Archivace dat se provádí manuálně nebo automaticky, první den kalendářního měsíce.

Docházka – docházku lze sledovat díky ústřednám PZS. Monitorovat docházku a přítomnost osob můžeme ve třech režimech:

- sledování pohybu osob po objektu za pomoci čteček,
- režim dvě čtečky – příchodová a odchodová čtečka + sledování pohybu osob po objektu,
- režim docházkový terminál – připojení docházkového terminálu k ústředně PZS.

Data o docházce můžeme exportovat do libovolného docházkového programu ve formě textového souboru. [24]

Technické požadavky - Procesor: Intel Pentium II s frekvencí 300 Mhz, Operační paměť: min. (minimálně) 64 MB, Pevný disk: 15 MB pro instalaci + min. 50 MB pro databázi událostí, Operační systém: Windows 95/98/2000/NT/XP, Sériový port.

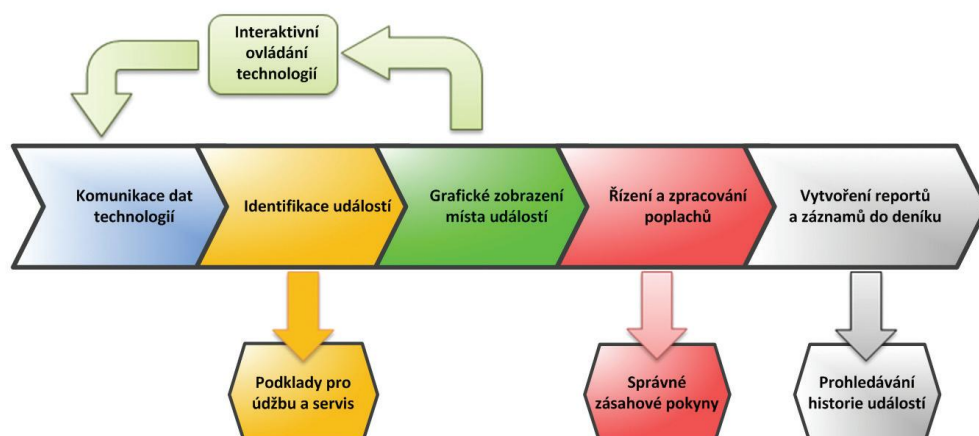
3.5.4 Integra 3

System Integra 3 je nástroj pro správu bezpečnosti a provozu budov, podniků a rozsáhlých areálů. Tento produkt nabízí česká firma INTEGEOO, s.r.o. Firma má sídlo v Dobřichovicích a pobočku v Praze. Hlavní oblasti, ve kterých se firma prosazuje, jsou kamerové systémy (CCTV), integrace bezpečnostních technologií a jádra bezpečnostních řešení.

Popis systému

System Integra 3 patří mezi technologicky nejpokročilejší integrační nástroje. Umožňuje vzájemně propojit zabezpečovací, protipožární, kamerové a vstupní systémy, dále také zařízení s I/O moduly. Mezi základní úkoly systému patří získávání a zpracování informací z připojených technologií, tyto informace srozumitelně zobrazovat na plánu objektu a tím pomáhat personálu v řešení vzniklé situace. Mezi tyto úkoly můžeme zařadit také schopnost vzdáleně ovládat jednotlivé technologie, tzn. měnit režimy střežení apod. Neméně důležité je také automatické vytváření deníku událostí, poskytování podkladů pro vyšetřování události a podpora údržby zařízení jednotlivých technologií.

Výsledkem všech výše zmíněných činností je zvýšení bezpečnosti objektu a snížení nákladů na provoz objektu. [32]



Obr. 45: Procesní schéma systému Integra 3 [33]

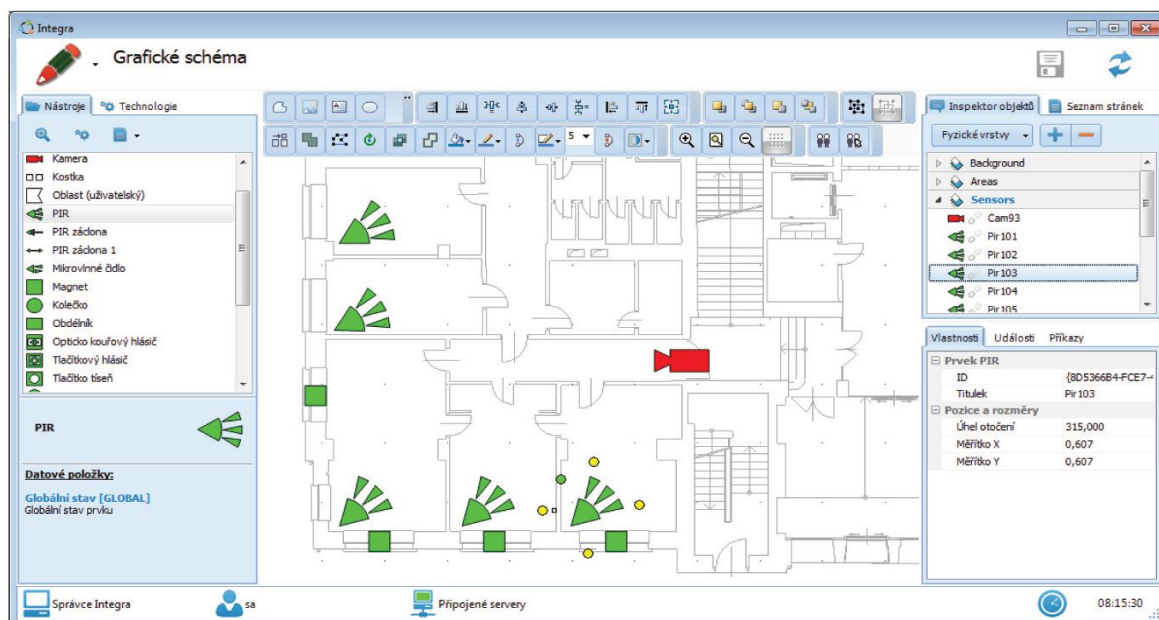
Architektura – systém je postaven na architektuře klient – server. Integra 3 umožňuje také komunikace mezi vzdálenými lokalitami. Tato komunikace je šifrovaná. Velký důraz je kladen na dostupnost. Ta je dosažena aplikací Watchdog, která spouští a sleduje SW služby. [33]



Obr. 46: Architektura systému [23]

Funkce systému

Integra 3 je vhodný nástroj pro manažery, pracovníky ostrahy i správce informačních technologií. Jedná se o prostředí, ve kterém lze vytvořit řešení, které bude přesně odpovídat potřebám, procesům, rozloze, zdrojům a použitým technologiím. [33]



Obr. 47: Prostředí programu [33]

Administrátor systému může snadno vytvářet uživatelské skupiny, kterým přiřazuje uživatelská práva. Další pravomocí administrátora je definování režimů – zapnuto/vypnuto, zastřeženo/odstřeženo. Systém umožňuje snadné přidávání nových prvků (senzory, kamery, čtečky kontroly vstupu, měřící zařízení apod.). Administrátor připravuje pro pracovníka ostrahu uživatelské prostředí. Bezpečnostní pracovník má díky grafickému zobrazení celkový přehled o používaných zařízeních. Nejdůležitější informací pro ostrahu je poplach. Ten je okamžitě vyznačen na mapovém podkladu, společně s instrukcemi jak situaci řešit. Vedoucí pracovníci mají okamžité informace o stavu systému, o tom kde a kdy došlo k dané situaci a jaká byla reakce ostrahu. [33]

Podporovaná zařízení

<p>Elektronické zabezpečovací systémy (EZS)</p> <ul style="list-style-type: none"> • Galaxy 144-514, přes SmartModul RS232 i TCP/IP • Siemens Sintony 4XX, přes RS232 • EffEff MB100, MB10, MB 48 – přes Winmag a OPC server • Caddx NX8, přes RS 232 nebo TCP/IP • Domminus Millenium, přes RS 232 nebo TCP/IP 	<p>Požární signalizace (EPS)</p> <ul style="list-style-type: none"> • Esser 8000 a IQ8, přes SEI modul • Siemens Synova 330, přes RS232 • Siemens FC700, přes RS232 • Zettler Expert , přes RS232
<p>Kamerové systémy (CCTV)</p> <ul style="list-style-type: none"> • Bosch Divar, přes TCP/IP • Bosch Dibos, přes TCP/IP • Verint Nextiva • Genetec Omnicast • PTZ Pelco-D server • Pelco Matrix, přes RS485 	<p>I/O moduly a ostatní</p> <ul style="list-style-type: none"> • I/O moduly Papouch • I/O moduly HW Server • OPC rozhraní obecně, přes TCP/IP • Detekce RZ/SPZ
<p>Perimetrické radarové systémy</p> <p>Produkty ICX Technologies</p>	<p>Přístupové a docházkové systémy (EKV)</p> <ul style="list-style-type: none"> • Techfass APS 400, přes TCP/IP • Honeywell Winpak, přes SDK

Obr. 48: Kompatibilita zařízení [32]

Technické požadavky

- Operační systém: Windows Vista, Windows 7, Windows Server 2003 a 2008

3.5.5 SIMS

Informační a monitorovací software SIMS (Safety Informational Monitory Software) nabízí firma SW SIMS HRACHOVINA, s. r. o., která se věnuje vývoji a údržbě informačních a monitorovacích programů pro pracoviště poplachových přijímacích center.

SIMS se zabývá informační soustavou pro subjekty zabývající se ochranou majetku a osob prostřednictvím elektronických systémů a PPC (Poplachových Přijímacích Center). Je koncipován tak, aby zajišťoval maximální flexibilitu, efektivnost vedení, zpracování a vyhodnocování informací potřebných pro provoz pracoviště PPC, respektive pracoviště stálé služby. [34]

Popis programu

SW SIMS je určen pro operační systém Windows, pro databázi využívá SQL server, který vyžaduje operační systém min. Windows 2000 (server).

Pro komunikaci se využívají telefonní, radiové, SMS, GPRS a IP komunikátory.

Program má k dispozici ovladače pro bezpečnostní zařízení, zejména pro PPC těchto firem: [34]

Tabulka 5: Podporovaní výrobci PPC

SG DR	HaSaM
Jablotron	FBII
RHMS	FEI
Matilda	NAM
Radom	ORZO Security

Program umožňuje současně propojit informace ze všech PPC, pro které má ovladače, do jednoho systému. Komunikace mezi počítačem a PCO probíhá na úrovni služeb.

Funkce systému

Program slouží především pro operátory, kterým usnadňuje práci tím, že všechny zprávy, které jsou pouze informativní, ukládá automaticky do souboru zpráv, kdežto pro poplachové informace vyžaduje obsluhu. Vytváří přehledné databáze pro všechny zprávy a objekty, společně s informacemi o bezpečnostních zařízeních. Ke všem objektům lze přiřadit mapy, fotografie, IP kamery apod. Program sleduje činnosti obsluhy a sestavuje zprávy, které obsahují informace o době reakce na poplachovou informaci, čas příjezdu

zásahové skupiny apod. Tyto informace umožňuje vytisknout pro potřebu zákazníka. V případě, že bude probíhat servisní zásah v objektu, umožňuje blokaci poplachových informací z daného objektu.

Díky tomuto SW můžeme přijímat a posílat SMS zprávy, a to buď manuálně, nebo automaticky v souvislosti s událostí doručenou na PPC. Zákazníkům je umožněna on-line kontrola adres objektů, kontaktních osob a zpráv ze zabezpečovacích ústředěn jejich objektů.

SIMS pracuje převážně v sítích, proto je před zneužitím chráněn přístupovými právy. [34]

Pro program SIMS jsou nabízeny také 2 nadstavby:

Fakturace – program využívající data ze SIMS pro vytváření faktur.

SISMWEB – program pro přístup k datům o objektu prostřednictvím internetu.

Technické požadavky - operační systém Windows 2000(server) a vyšší. [34]

Cena: 32 890,-Kč

The screenshot shows the SIMS 2.3.0.30 software interface. The main window displays a list of events and messages. The interface includes a menu bar with options like 'Zpracování', 'Číselníky', and 'Parametry'. Below the menu bar, there are several tabs: 'Objekty', 'Zprávy', 'Adresy', 'SMS', 'Email', 'WWW a SMS zprávy', 'SMS události zprávy', and 'Restart služby'. The main area contains a table with columns for 'Datum', 'Čas', 'Číslo objektu', 'Grupa', 'Název objektu', 'Název', 'Čas', 'Objekt', 'Datum', 'Datum zakočení', and 'Datum'. The table lists various events, including 'Paradox', 'TEST PCS 100', and 'Pouška komunikace'. The status of each event is indicated by a small icon in the 'Číslo objektu' column.

Id	Datum	Čas	Číslo objektu	Grupa	Název poc	Název objektu	Název abytu	Název číselného kódu	Událost	Číselný
209	18.3.2009	16:13:50	3333	0	Paradox	TEST PCS 100	Pouška komunikace		E354	0
210	18.3.2009	16:13:54	3333	1	Paradox	TEST PCS 100 Objekt generovaný při Zavřeno			R401	1
211	18.3.2009	16:13:57	3333	1	Paradox	TEST PCS 100 Objekt generovaný při Zavřeno bez kláves			R407	0
212	18.3.2009	16:14:01	3333	0	Paradox	TEST PCS 100	Pouška komunikace		E354	0
213	18.3.2009	16:14:04	3333	1	Paradox	TEST PCS 100 Objekt generovaný při Obnova	Poplach vzloupání	Odpor na desce	E130	2
214	18.3.2009	16:14:08	3333	0	Paradox	TEST PCS 100	Pouška komunikace		E354	0
215	18.3.2009	16:14:12	3333	1	Paradox	TEST PCS 100 Objekt generovaný při Obnova		Odpor na desce	R130	2
216	18.3.2009	16:14:16	3333	1	Paradox	TEST PCS 100 Objekt generovaný při Diveno - zasteno			E406	1
217	18.3.2009	16:14:20	3333	1	Paradox	TEST PCS 100 Objekt generovaný při Diveno užívatelem			E401	1
218	18.3.2009	16:14:23	3333	0	Paradox	TEST PCS 100	Pouška komunikace		E354	0
219	18.3.2009	16:14:47	3333	1	Paradox	TEST PCS 100 Objekt generovaný při Zavřeno			R401	1
220	18.3.2009	16:14:51	3333	1	Paradox	TEST PCS 100 Objekt generovaný při Zavřeno bez kláves			R407	0
221	18.3.2009	16:14:55	3333	0	Paradox	TEST PCS 100	Pouška komunikace		E354	0
222	18.3.2009	16:14:58	3333	0	Paradox	TEST PCS 100	Konec dálkového programování		E628	0
223	18.3.2009	16:15:28	1111	1	Paradox	Test IP 100 Objekt generovaný progr. Periodický test UL			TX	0
224	18.3.2009	16:18:06	3333	1	Paradox	TEST PCS 100 Objekt generovaný při Zavřeno			R401	1
225	18.3.2009	16:19:27	3333	1	Paradox	TEST PCS 100 Objekt generovaný při Diveno užívatelem			E401	1
226	18.3.2009	16:28:21	1111	1	Paradox	Test IP 100 Objekt generovaný progr. Ukončení dálkového programování			RS	0
227	18.3.2009	16:28:44	3333	1	Paradox	TEST PCS 100 Objekt generovaný při Zavřeno			R401	1
228	18.3.2009	16:29:04	1111	1	Paradox	Test IP 100 Objekt generovaný progr. Zavrženo kódem			CL	1
229	18.3.2009	16:29:08	1111	1	Paradox	Test IP 100 Objekt generovaný progr. Periodický test UL			TX	0

Obr. 49: Prostředí SW SIMS [35]

3.6 Komparace produktů

V této části práce budu porovnávat jednotlivé produkty pro integraci, v souvislosti s rozdělením ve druhé kapitole, tzn. produkty pro hardwarovou a softwarovou integraci.

3.6.1 HW integrace

V této části práce provedu komparaci jednotlivých možností HW integrace. Patří zde tedy integrace: propojením vstupů a výstupů, přes sběrnici s využitím modulů, pomocí systému domácí automatizace a integrace v rámci systémové elektroinstalace.

Komparace je provedena podle různých kritérií. V tabulce používám čísla od 1 do 5, kde číslo 1 znamená, že uvedený způsob integrace naplňuje stanovené kritérium nejlépe a naopak číslo 5 nejhůře.

Tabulka 6: Komparace HW produktů pro integraci

	Vhodnost použití v rodinných domech	Vhodnost použití v rozsáhlých objektech	Cena	Možnost rozšíření	Uživatelský komfort	Technická náročnost na projekt a instalaci	Spolehlivost
Integrace propojením vstupů a výstupů	1	4	2	2	2	3	2
Integrace přes sběrnici s využitím modulů	3	1	3	1	3	3	4
Integrace pomocí systému domácí automatizace	1	5	2	1	2	1	3
Integrace v rámci systémové elektroinstalace.	2	1	4	2	2	3	3

Nejvhodnější způsob integrace pro použití v rodinném domě představuje integrace propojením vstupů a výstupů a systém domácí automatizace. Pro rozsáhlé objekty je nejvíce vhodná inteligentní elektroinstalace a integrace přes sběrnici s využitím modulů.

3.6.2 SW integrace

3.6.2.1 Integrace pomocí SW nastavy

V poslední kategorii, kterou popisují v této práci, se nachází 5 produktů. Čtyři softwarové programy nabízí české firmy a jedna firma ze Slovenska. Mezi nejpoužívanější patří grafický systém pro integraci ALVIS, informační systém INTEGRA 3 a systém pro integraci, správu a kontrolu elektronických systémů VAR-NET INTEGRAL.

Nyní následuje komparace všech 5 dostupných produktů, podle různých kritérií.

Vhodnost použití

Prvním kritériem, podle kterého budu programy porovnávat, je vhodnost použití v jednotlivých prostorech. Prostory jsem rozdělil na domácnost, malý, střední a velký podnik. Za malý podnik se považuje firma, která zaměstnává méně než 100 zaměstnanců. Střední podnik má zaměstnanců do 500 a velký podnik více než 500.

V následující tabulce porovnám jednotlivé programy podle vhodnosti použití, ve výše uvedeném rozdělení.

Tabulka 7: Komparace podle vhodnosti použití

	Domácnost	Malé podniky	Střední podniky	Velké podniky	Městský bezpečnostní systém
ALVIS	3	1	1	2	2
VAR-NET INTEGRAL	3	1	1	3	3
TEGAL	3	1	2	3	3
INTEGRA 3	3	2	1	2	2
SIMS	3	2	2	2	1

V tabulce 7 používám čísla od 1 do 4, kde číslo 1 znamená vhodné, 2 – méně vhodné, 3 – nevhodné, 4 – nepoužitelné pro daný objekt.

Podpora bezpečnostních technologií

Druhým kritériem pro komparaci je podpora bezpečnostních technologií – PZS, EPS, CCTV a ACS.

Tabulka 8: Podpora bezpečnostních technologií

	PZS	EPS	CCTV	ACS	I/O moduly
ALVIS	+	+	+	+	+
VAR-NET INTEGRAL	+	+	+	+	-
TEGAL	+	+	+	+	-
INTEGRA 3	+	+	+	+	+
SIMS	+	+	+	-	-

V tabulce 8 používám znaky + a -. Znak + znamená, že produkt podporuje danou bezpečnostní technologii. Naopak – znamená, že tuto bezpečnostní technologii nepodporuje.

Cena systému

Poslední tabulka uvádí ceny jednotlivých systémů.

Tabulka 9: Ceny produktů

	ALVIS	VAR-NET INTEGRAL	TEGAL	INTEGRA 3	SIMS
Cena	64 464,-Kč	47 000,-Kč	nezjištěno	nezjištěno	32 890,-Kč

Cena uvedená u programu ALVIS zahrnuje neomezený počet adres, umožňuje připojit 5 ústředěn a neobsahuje DDE server. Cena produktu VAR – NET INTEGRAL obsahuje základní jádro, okruhy PZS, EPS, CCTV, ACS a mapové rozhraní. Cena programu SIMS platí pro 0 – 150 připojených zařízení. Cenu programů TEGAL a INTEGRA 3 se mi nepodařilo zjistit.

3.7 Dílčí závěr

V této kapitole byla provedena analýza a komparace dostupných produktů integrace. Nejdříve jsou popsány HW produkty, kde jsou uvedeny řešení pro integraci propojením vstupů a výstupů – Jablotron Oasis, David, IP kamera Axis. Integrace přes sběrnici a moduly - Honeywell MB 48, Honeywell Galaxy Dimension, Paradox Digiplex EVO. Systém domácí automatizace Marmitek TotalGuard. Inteligentní elektroinstalace Inels, Nikobus, ABB i-bus KNX.

SW integrace má zastoupení v programech ALVIS, VAR-NET INTEGRAL, TEGAL, INTEGRA 3 a SIMS.

Komparace HW řešení byla provedena podle stanovených kritérií v tabulce č. 6. Nejvhodnější způsob integrace pro použití v rodinném domě představuje integrace propojením vstupů a výstupů a systém domácí automatizace. Pro rozsáhlé objekty je nejvíce vhodná inteligentní elektroinstalace a integrace přes sběrnici s využitím modulů. Z hlediska možností pro rozšíření, jsou na tom všechny způsoby integrace podobně. To platí i pro uživatelský komfort, který nabízejí. Porovnání podle technické náročnosti na projekt a realizaci vyšlo nejlépe pro domácí automatizaci. Zde je ovšem potřeba brát ohled na rozsah a typ instalace. Posledním kritériem v tabulce je spolehlivost. Nejlepší známku dostala integrace propojením vstupů a výstupů díky tomu, že v případě poruchy není ohrožen chod celého systému, ale jen postižené části.

Z tabulky č. 6 je patrné, že každý způsob integrace je vhodný pro různé typy objektů a nabízí různé možnosti. Nelze tedy přesně říci, která možnost je nejlepší. Záleží na jednotlivých řešeních.

SW produkty jsou v tabulce č. 7 porovnávány podle vhodnosti použití. Nejlepším programem jsem podle výsledků analýzy zvolil SW ALVIS. Také zde musíme brát ohled na typ objektu a potřeby zákazníka. Tabulka č. 8 ukazuje kompatibilitu programů s jednotlivými bezpečnostními technologiemi.

4 MOŽNOSTI APLIKACE INTEGROVANÝCH POPLACHOVÝCH SYSTÉMŮ

IPS můžeme používat v obytném a stejně tak v průmyslovém prostředí. Pro každé z těchto dvou jmenovaných prostředí vznikají odlišné potřeby, které souvisí s používáním IPS. Tato kapitola se bude zabývat jednotlivými funkcemi pro dané prostory.

4.1 IPS v obytném prostředí

U integrovaných systémů v obytném prostředí, je kladen důraz především na komfort, úspory a bezpečnost.

Komfort – zvýšené pohodlí umožňují především funkce pro ovládání osvětlení, žaluzií a rolet, garážových vrat, nebo také vytápění, zavlažování, klimatizace a vyhřívání bazénu. Osvětlení v celém domě i na zahradě lze řídit z jednoho místa. Svítidla můžeme stmívat a vytvářet tak jednotlivé světelné scény, které lze naprogramovat a poté jednoduše vyvolat. Tyto světelné scény lze volit podle aktuální situace v domě, např. rodinná oslava, čtení knížky, sledování televize apod. Žaluzie nebo rolety se mohou vytahovat a zatahovat v závislosti na počasí, např. při východu a západu slunce nebo při deštivém a větrném počasí. Jednotlivé pokoje mohou být vytápěny na předem stanovenou teplotu. To stejné platí i pro bazén. Vytápění lze ovládat i dálkově, např. před příchodem z práce nebo příjezdem z dovolené. Zavlažování zahrady bude probíhat podle zvoleného časového rozvrhu.

Hlavní zásluhu na komfortu v domě má centrální vizualizační dotykový panel, díky kterému můžeme ovládat chod celého domu z jednoho místa.

Úspory – integrované systémy umožňují snížit náklady za elektrickou a tepelnou energii. Úspory elektrické energie zaručují možnosti pro ovládání osvětlení. Intenzita svítidel může být řízena podle intenzity venkovního světla. Dále je zde možnost využití pohybových snímačů, které vypnou světla po odchodu z místnosti. Osvětlení a zásuvky mohou být úplně vypnuty při odchodu z domu. Náklady na vytápění lze ušetřit omezením topení v nepřítomnosti osob, ale také snížením teploty, např. na chodbách nebo v garáži. Vhodné je také využití vazby mezi okny a vytápěním, která zajišťuje snížení vytápění při otevřeném okně. Někteří výrobci uvádí až 30 % úspory energie.

Bezpečnost – Jak již bylo v práci několikrát zmíněno, integrované systémy spojují většinu bezpečnostních technologií (PZS, EPS, CCTV, ACS, SAS). V následující tabulce jsou uvedeny akce, které mohou nastat po zastřežení/odstřežení objektu a při poplachu.

Tabulka 10: Akce při zastřežení, odstřežení a poplachu pro obytné prostředí

<u>Zastřeženo</u>	<u>Odstřeženo</u>	<u>Poplach</u>
Zapnutí zabezpečovacího systému	Vypnutí zabezpečovacího systému	Zapnutí sirény
Zamknutí všech elektronických zámků	Otevření brány	Vypnutí přívodu plynu
Zavření brány	Odemknutí určených elektronických zámků	Rozsvícení a rozblikání všech světel
Vypnutí všech světel v objektu	Zapnutí všech světel	Vypnutí vybraných elektrických okruhů
Vypnutí nepotřebných zásuvek	Zapnutí zásuvek	Odeslání informace o poplachu na PPC a na mobil
Vypnutí přívodu plynu a klimatizace	Zapnutí přívodu plynu	
Stáhnutí žaluzií	Vytažení žaluzií	Spuštění záznamu CCTV
Nastavení vytápění na nízkou teplotu	Zapnutí vytápění	Odeslání MMS
Přesměrování hovoru od branky na mobil (návštěva)	Nastavení světelné scény	Vytažení všech rolet
Simulace přítomnosti		Zapnutí vnitřní sirény pro dezorientaci pachatele

4.2 IPS v průmyslovém prostředí

Použití IPS v průmyslovém prostředí má podobné výhody, jako použití pro obytné prostředí. Ještě více je zde kladen důraz na úspory a bezpečnost. Komfort zde není hlavním požadavkem.

Úspory jsou řešeny stejným způsobem, jako v rodinných domech, tzn., že pokud se v místnosti nenachází žádná osoba, dojde k vypnutí vytápění a osvětlení.

Bezpečnost obstarává především přístupový systém společně s PZS. Neméně důležité je i zajištění bezpečnosti práce (EPS, osvětlení, klimatizace, vytápění, obsluha strojů apod.).

Tabulka 11: Akce při zastřežení, odstřežení a poplachu pro průmyslové prostředí

<u>Zastřeženo</u>	<u>Odstřeženo</u>	<u>Poplach</u>	<u>ACS – vstup do prostoru</u>
Zapnutí zabezpečovacího systému	Vypnutí zabezpečovacího systému	<u>EPS</u> Zapnutí sirény	Odstřežení místnosti
Zamknutí všech elektronických zámků	Odemknutí určených elektronických zámků	Odeslání informace o požáru na pracoviště HZS (Hasičský Záchraný Sbor)	Provedení záznamu do evidenčního SW docházka
Vypnutí příslušných světel v objektu	Zapnutí všech světel	Zastavení přívodu plynu Rozsvícení všech světel	
Vypnutí nepotřebných zásuvek	Zapnutí zásuvek	Otevření elektronických zámků	Povolení pro ovládání strojních zařízení
Vypnutí klimatizace	Zapnutí klimatizace	Vypnutí vybraných elektrických okruhů	
Omezení teploty	Zapnutí vytápění	<u>PZS</u>	Spuštění počítačů
Zastavení výtahů	Zapnutí výtahů	Zapnutí sirény a záznamu CCTV	
Blokování čteček karet u vybraných vchodů	Odblokování čteček karet u vybraných vchodů	Rozsvícení všech světel	
		Zamknutí všech elektronických zámků	Zapnutí zásuvek
Zatažení žaluzií	Vytažení žaluzií	Zapnutí vnitřní sirény pro dezorientaci pachatele	Zapnutí světel
		Vytažení všech rolet	

4.3 Dílčí závěr

Za nejběžnější funkce při zastřežení lze považovat zapnutí zabezpečovacího systému, zamknutí elektronických zámků, vypnutí nepoužívaných zásuvek, osvětlení a omezení teploty v objektu. Při odstřežení se naopak vypne zabezpečovací systém, zapne se vytápění, osvětlení, zásuvky a dojde k odemknutí elektronických zámků. Hlavní funkcí při poplachu, je jeho signalizace, tzn., zapnutí sirény, rozsvícení světel nebo také odeslání informace o poplachu na PPC. Může se také zapnout záznam CCTV.

Pro průmyslové prostředí je přidána kategorie: ACS - vstup do prostoru. Touto činností může být např. vstup zaměstnance do laboratoře. Při této akci může dojít k odstřežení, zapnutí světel, zásuvek a počítačů. Může být proveden záznam o docházce do evidenčního SW a povolení ovládat příslušná zařízení.

ZÁVĚR

V úvodní části byla provedena analýza technických požadavků v souladu se stávající legislativou. Nejdříve byly popsány požadavky, které jsou stanoveny v právních předpisech. Zde je zařazen zákon č. 22/1997 Sb. o technických požadavcích na výrobky. Dále nařízení vlády č. 616/2006 Sb. o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility. Technické požadavky na elektrická zařízení nízkého napětí a požadavky na rádiová a na telekomunikační koncová zařízení, obsahují nařízení vlády č. 17/2003 Sb. respektive NV č. 426/2000 Sb. Je důležité, aby integrovaný systém splňoval nejdříve své produktové (aplikační) normy a následně také normy pro integrované systémy. Mezi aplikační patří především normy, které se vztahují k jednotlivým systémům, které se integrují (PZS, EPS, ACS, CCTV, SAS apod.). Integrovanými poplachovými systémy se v rámci technických předpisů platných v ČR zabývá norma ČSN CLC/TS 50398.

Ve druhé kapitole je zpracován návrh kvalifikace způsobů integrace. Prvním způsobem integrace je propojení vstupů a výstupů. Tento způsob využívá především pomocná relé, bezdrátové přijímače a vysílače, GSM ovladače a alarmové vstupy a výstupy. Další možností je integrace přes sběrnici s využitím modulů. Zde je integrace umožněna díky modulům, které se připojují na sběrnici. Integrace v rámci domácí automatizace X10 využívá stávajících elektrických rozvodů v domě, pro posílání signálů k ovládaným zařízením. Inteligentní elektroinstalace využívá vzájemně propojené akční členy a snímače. Snímače vysílají povely, na které akční členy reagují provedením požadované funkce.

V praktické části byla provedena analýza produktů, které jsou vhodné pro integraci a zároveň jsou dostupné na trhu. Jsou uvedeny HW i SW produkty jednotlivých firem a dodavatelů. Následně byla provedena komparace mezi HW prvky. Výsledkem bylo zjištění, že pro menší rodinné domy je nejvhodnější systém domácí automatizace X10. Naopak pro rozsáhlé objekty je vhodná integrace přes sběrnici a integrace v rámci inteligentní elektroinstalace.

Poslední kapitola obsahuje návrh činností, které mohou nastat při zastřežení, odstřežení, poplachu a při vstupu do místnosti. Mezi nejběžnější funkce lze zařadit zapnutí a vypnutí zabezpečovacího systému, zapnutí sirény, ovládání elektronických zámků, osvětlení, zásuvek, žaluzií a rolet.

Výsledky bakalářské práce mohou být využity projektanty IPS, výrobci a dodavateli zabezpečovacích produktů. Dále lze práci využít jako podklad pro další rozpracování tématu a v neposlední řadě také jako informační materiál pro seznámení zákazníků s jednotlivými typy integrace.

ZÁVĚR V ANGLIČTINĚ

In the introductory part was carried out analysis of technical requirements in accordance with existing legislation. In one of the first chapters are described the requirements. These requirements are set out in the legal regulations. We can find there the act no. 22/1997 Sb. about technical requirements for products. Further government regulation no. 616/2006 Sb. about technical requirements for products in terms of their electromagnetic compatibility. Technical requirements for electrical equipment low voltage and requirements for radio and telecommunications terminal equipment, contains government regulation no. 17/2003 Sb. respectively government regulation no. 426/2000 Sb.

At first it is very important that the integrated system have to fulfill the norms of product (application) and then norms for integrated systems. Among the application norms which relate to individual systems which are integrated, we include (IAS, EPS, ACS, CCTV, SAS etc.). ČSN CLC/TS 50398 deals with integrated alarm systems within applicable technical standards in Czech republic.

Second chapter is focused on suggestion of qualification methods of integration. The first method of integration is based on connect inputs and outputs. This method uses especially auxiliary relays, wireless receivers and transmitters, GSM drivers and alarm inputs/outputs. The other method is integration across the BUS with the use of modules. The integration is allowed by modules that are attached to the BUS. Integration within the home automation X10 uses existing electrical distribution which are used for sending signals for controlled device. Intelligent electrical installation uses mutually connected actors and sensors. The sensors send commands to actors which are responding by executing the required functions.

Practical part of this bachelor thesis describes the analysis of products which are useful for integration and they are available on the market. The products offered in the market include HW and SW products of individual companies and suppliers. After these findings was carried out the comparison between HW products. The result was the finding that for smaller family houses is the most suitable system for home automation X10. On the contrary, for large objects are the most suitable integration across the BUS and integration within the intelligent electrical installation.

The last chapter contains a suggestion for activities which may occur when the system is: ARM, DISARM, alarm, and at entry in the room. Among the most common functions can

be classify: turn ON/OFF alarm system, turn ON siren, control locks, lighting, electric sockets, blinds and roller blinds.

The results of the Bachelor thesis can be used by the designers of IPS, manufacturers and suppliers of security products. Further the results can be used as a basis for elaboration of the topic and also as information material for familiarize customers with different types of integration.

SEZNAM POUŽITÉ LITERATURY

- [1] UHLÁŘ, Jan. *Technická ochrana objektů. II. díl, Elektrické zabezpečovací systémy II.* 2. vyd. Praha: Policejní akademie ČR v Praze, 2009, 229 s. ISBN 978-80-7251-313-0.
- [2] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky.* 3. vyd. Blatná: Cricetus, 2006, 315 s. ISBN 80-902938-2-4.
- [3] Česká republika. Zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů. In *Sbírka zákonů.* 1997, 6, s. 128-136.
- [4] Česká republika. Nařízení Vlády České republiky č. 616/2006 Sb., o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility. In *Sbírka zákonů.* 2006, 191, s. 8109-8116.
- [5] Česká republika. Nařízení Vlády České republiky č. 17/2003 Sb., technické požadavky na elektrická zařízení nízkého napětí. In *Sbírka zákonů.* 2003, 9, s. 306-310.
- [6] Česká republika. Nařízení Vlády České republiky č. 426/2000 Sb., technické požadavky na rádiová a na telekomunikační koncová zařízení. In *Sbírka zákonů.* 2000, 119, s. 5738-5750.
- [7] ČSN CLC/TS 50398. *Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. 20 s.
- [8] Automatizace - Systém OASiS. *Zabezpečení, alarmy, detektory | Jablotron* [online]. © 2008 - 2012 [cit. 2012-04-21]. Dostupné z: <http://www.jablotron.cz/cz/sekce/vyrobky/automatizace+system+oasis/>
- [9] Digitální vstupy a výstupy (I/O) | netcam.cz. *IP kamery pro zabezpečovací a dohledové systémy | netcam.cz* [online]. [cit. 2012-02-12]. Dostupné z: <http://www.netcam.cz/encyklopedie-ip-zabezpeceni/digitalni-vstupy-vystupy.php>
- [10] GD-04 DAViD - Inteligentní dálkový ovladač a hlásič řízený pomocí mobilu. [online]. © 2008 - 2012 [cit. 2012-04-21]. Dostupné z: <http://www.david.jablotron.cz/pouziti.htm>
- [11] *Katalog produktů 2010 – 2011.* Třebíč: VARIANT plus, 2010. 280s.

- [12] *Průvodce návrhem systému Galaxy Dimension* [online]. ADI Global Distribution, 2011 [cit. 2012-04-28]. Dostupné z: [http://www.adiglobal.cz/iiWWW/docs.nsf/all/6A2AA5D42325098EC12578D500569CF1/\\$FILE/KL_Pruvodce_navrhem_Galaxy_2011.pdf](http://www.adiglobal.cz/iiWWW/docs.nsf/all/6A2AA5D42325098EC12578D500569CF1/$FILE/KL_Pruvodce_navrhem_Galaxy_2011.pdf)
- [13] *Integrované bezpečnostní systémy* [online]. Honeywell, 2007 [cit. 2012-04-28]. Dostupné z: <http://www.security.honeywell.com/partnerplusee/documents/HSCE-MBRANGE-01-CZ%280807%29SB-E.pdf>
- [14] *Magellan 6060 + Automatizace X10* [online]. Třebíč: Variant plus, 2007 [cit. 2012-04-28]. Dostupné z: <http://www.elektromahl.cz/dokumenty/MAGELLAN/manual-MG-6060-X10-automatizace.pdf>
- [15] *ABB i-bus KNX - Systém inteligentní elektroinstalace - Popis systému* [online]. Jablonec nad Nisou: ABB, [cit. 2012-04-28]. Dostupné z: [http://www05.abb.com/global/scot/scot209.nsf/veritydisplay/f8364a3ffd2404f9c125773d0033fe47/\\$file/elektronicky_prospekt_05.pdf](http://www05.abb.com/global/scot/scot209.nsf/veritydisplay/f8364a3ffd2404f9c125773d0033fe47/$file/elektronicky_prospekt_05.pdf)
- [16] *ABB i-bus KNX – Systém inteligentní elektroinstalace a řízení budov - Preferovaná technologie* [online]. Jablonec nad Nisou: ABB, [cit. 2012-04-28]. Dostupné z: [http://www05.abb.com/global/scot/scot209.nsf/veritydisplay/96152e3786e4c8a7c125783b0034c6b6/\\$file/Preferovana%20technologie_2CDC500064M0201_bel%20110113.pdf](http://www05.abb.com/global/scot/scot209.nsf/veritydisplay/96152e3786e4c8a7c125783b0034c6b6/$file/Preferovana%20technologie_2CDC500064M0201_bel%20110113.pdf)
- [17] *Inteligentní elektroinstalace budov – systém Nikobus, Uživatelský manuál v.1.0* [online]. Ústí nad Orlicí: Eaton, 2004 [cit. 2012-04-28]. Dostupné z: <http://www.eatonelektrotechnika.cz/pdf/manual%20nikobus.pdf>
- [18] *Inteligentní elektroinstalace Ego-n: Návrhový a instalační manuál. 5. vyd.* [online]. Jablonec nad Nisou: ABB, 2011 [cit. 2012-04-28]. Dostupné z: www117.abb.com/viewDocument.asp?document=5580&type=
- [19] LUKÁŠ, Luděk, et al. *Bezpečnostní technologie, systémy a management I.* Zlín : Radim Bačuvčík - VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.

- [20] *Katalogový list ALViS* [online]. ADI Global Distribution [cit. 2012-04-28].
Dostupné z:
[https://www.adiglobal.cz/iiWWW/cz/Produkty110.nsf/wp/katalogy/\\$file/kl_alvis_www.pdf](https://www.adiglobal.cz/iiWWW/cz/Produkty110.nsf/wp/katalogy/$file/kl_alvis_www.pdf)
- [21] *Katalogový list ALViS WEB 3.2* [online]. ADI Global Distribution [cit. 2012-04-28].
Dostupné z:
[https://www.adiglobal.cz/iiWWW/cz/Produkty110.nsf/wp/katalogy/\\$file/kl_alvis32_web.pdf](https://www.adiglobal.cz/iiWWW/cz/Produkty110.nsf/wp/katalogy/$file/kl_alvis32_web.pdf)
- [22] *Katalogový list Tegal 5* [online]. ADI Global Distribution [cit. 2012-04-28].
Dostupné z:
[http://www.adiglobal.cz/iiWWW/docs.nsf/all/457B949CCA91B33CC12574110000D529/\\$FILE/KL_Tegal_v5_cz_oc.pdf](http://www.adiglobal.cz/iiWWW/docs.nsf/all/457B949CCA91B33CC12574110000D529/$FILE/KL_Tegal_v5_cz_oc.pdf)
- [23] *Integra 3 – jednotné řízení všech bezpečnostních technologií v organizaci. CIO Business World.cz* [online]. 01.02.2011 [cit. 2012-04-28]. Dostupné z:
<http://businessworld.cz/it-strategie/integra-3-jednotne-rizeni-vsech-bezpecnostnich-technologii-v-organizaci-7019>
- [24] *Uživatelský manuál Tegal 5* [online]. ADI Global Distribution, 2003, [cit. 2012-04-28].
Dostupné z:
[https://www.adiglobal.cz/iiWWW/docs.nsf/all/4EEED42C8A770CC9C12574110000D5A7/\\$FILE/UM_Tegal_5_cz_oc.pdf](https://www.adiglobal.cz/iiWWW/docs.nsf/all/4EEED42C8A770CC9C12574110000D5A7/$FILE/UM_Tegal_5_cz_oc.pdf)
- [25] *Prezentační DVD* [DVD-ROM]. Jablotron, 2011.
- [26] *David – GSM ovladač a hlásič* [online]. Jablonec nad Nisou: Jablotron alarms, [cit. 2012-04-28].
Dostupné z:
http://www.jablotron.cz/upload/download/david_2011_cz.pdf
- [27] *TotalGuard - bezdrátový zabezpečovací systém X10. X10 Powerhouse - automatizace a zabezpečení domu* [online]. © 2003 [cit. 2012-04-28]. Dostupné z:
<http://www.powerhouse.eu/totalguard-bezdratovy-zabezpecovaci-system-p-89.html?language=cz>
- [28] *Inels – Inteligentní a komfortní elektroinstalace* [online]. Holešov: ELCO EP, 2012 [cit. 2012-04-28].
Dostupné z:
http://www.inels.cz/index.php?sekce=ke_stazeni

- [29] *Sběrníkový systém Nikobus – Hlavní katalog 2009-2010* [online]. Ústí nad Orlicí: Eaton, 2009 [cit. 2012-04-28]. Dostupné z: http://www.xcomfort.cz/techinfo/cs-tiskoviny-sbernicovy_system_nikobus_a_audio_ozvuceni-8
- [30] SPIRIT a.s. *SPIRIT - ALVIS* [online]. [cit. 2012-04-28]. Dostupné z: <http://www.alvis.sk/>
- [31] *VAR-NET INTEGRAL – Vizualizace* [online]. Třebíč: VARIANT plus, [cit. 2012-04-28]. Dostupné z: <http://www.variant.cz/dokumenty/obchod/prospekty-a-tabla/>
- [32] *Integra 3* [online]. Praha: Integoo, [cit. 2012-04-28]. Dostupné z: http://www.integoo.cz/sites/default/files/integoo_integra3_leaflet_cz-2011.pdf
- [33] *Integra 3 – Technický leták* [online]. Praha: Integoo, [cit. 2012-04-28]. Dostupné z: <http://www.integoo.cz/sites/default/files/technicky-letak-integra.pdf>
- [34] Program SIMS. *SW SIMS* [online]. © 2011 [cit. 2012-04-28]. Dostupné z: <http://www.simsweb.eu/cz/programsims>
- [35] IPR512 podporuje český Software SIMS. *Eurosat CS* [online]. 23. 03. 2009 [cit. 2012-04-28]. Dostupné z: <http://www.eurosat.cz/1/1321-ipr512-podporuje-cesky-software-sims.html>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Access Control System – systém kontroly vstupu
ALVIS	Alarm Visualization System – Grafický systém
ATS	Alarm Transmission System – poplachový přenosový systém
BUS	Anglické označení pro sběrnici
CCF	Central Control Facility – ústřední ovládací zařízení
CCTV	Closed circuit television – uzavřený televizní okruh
CIB	Common Instalation Bus – Instalační sběrnice INELS
CLC/TS	Technická specifikace převzatá z CEN/CENELEC
ČR	Česká republika
ČSN	Česká technická norma
DDE	Dynamic Data Exchange – dynamická výměna dat
EHS	Evropské hospodářské společenství
EN	Evropská norma
EPS	Elektrická požární signalizace
ES	Evropské společenství
EU	Evropská unie
GSM	Global System for Mobil Communications
HTTPS	HyperText Transfer Protocol – Secure – bezpečná verze hypertextového přenosového protokolu
HW	Hardware – technické vybavení
HZS	Hasičský Záchranný Sbor
I/O	Input/Output – vstup/výstup
IE	Inteligentní elektroinstalace
IP	Internet Protocol – protokol internetu
IPS	Integrovaný poplachový systém

KNX	Konnex Bus – standard evropské elektroinstalační sběrnice
LAN	Local Area Network – lokální počítačová síť
LCD	Liquid Crystal Display – displej z tekutých krystalů
LED	Light Emmiting Diode–svítivá dioda
NVR	Network Video Recorder – síťový video rekordér
PGM	Programmed – programovatelný výstup ústředny
PIR	Passive Infrared Sensor – pasivní infračervený senzor
PPC	Poplachové Přijímací Centrum
PZS	Poplachový zabezpečovací systém
PZTS	Poplachový zabezpečovací a tísňové systém
RF	RadioFrequency
RS	Recommended Standard – komunikační standard (RS 232, RS 485...)
SAS	Social Alarm System – systém přivolání pomoci
SELV	Safety Extra-Low Voltage – bezpečné malé napětí
SIMS	Safety Informational Monitory Software – monitorovací software
SMS	Short Message Service – krátká textová zpráva
SW	Software – programové vybavení
TCP/IP	Transmission Control Protocol/Internet Protocol - Řídící přenosový protokol/protokol Internetu
TTL	Transistor Transistor Logic – tranzistorově tranzistorová logika
ÚDP	Úplný Provozní Deník
WAN	Wide Area Network – rozlehlá počítačová síť

SEZNAM OBRÁZKŮ

Obr. 1: Integrovaný systém rodinného domu	11
Obr. 2: První varianta konfigurace typu 1 [7], <i>upravil Kovařík, 2012</i>	21
Obr. 3: Druhá varianta konfigurace typu 1 [7], <i>upravil Kovařík, 2012</i>	22
Obr. 4: První varianta konfigurace typu 2 [7], <i>upravil Kovařík, 2012</i>	23
Obr. 5: Druhá varianta konfigurace typu 2 [7], <i>upravil Kovařík, 2012</i>	23
Obr. 6: Integrovaný poplachový systém	28
Obr. 7: Pomocné relé [8].....	29
Obr. 8: Bezdrátový magnetický snímač [8]	30
Obr. 9: Bezdrátový modul silových relé [8]	30
Obr. 10: Síťová kamera s I/O konektory [9], <i>upravil Kovařík, 2012</i>	31
Obr. 11: Příklad propojení ústředny PZS a elektrického okruhu.....	32
Obr. 12: Ovládání vytápění.....	33
Obr. 13: Ovládání topení pomocí termostatu, ústředny a GSM ovladače	33
Obr. 14: Zapojení GSM ovladače pro ovládání zavlažování a klimatizace [10].....	34
Obr. 15: Síťová kamera s digitálními I/O	35
Obr. 16: Připojení detektoru na sběrnici	36
Obr. 17: Zapojení modulů na sběrnici RS 485 [12].....	36
Obr. 18: Využití převodníků [12]	37
Obr. 19: Posilovač sběrnice [11].....	38
Obr. 20: Struktura sběrnicevého systému [13] <i>upravil Kovařík, 2012</i>	39
Obr. 21: Propojení ústředny se sítí 230V [14] <i>upravil Kovařík, 2012</i>	41
Obr. 22: Zásuvkový spínací modul, spínací modul do objímky, spínací modul na DIN lištu [14].....	41
Obr. 23: Struktura systému domácí automatizace X10 [14].....	42
Obr. 24: Klasická elektroinstalace	43
Obr. 25: Inteligentní elektroinstalace [16]	43
Obr. 26: Struktura inteligentní elektroinstalace [17]	44
Obr. 27: SW nástavba [21]	46
Obr. 28: První varianta propojení	47
Obr. 29: Druhá varianta propojení	47
Obr. 30: Prostředí programu [24]	48
Obr. 31: Jablotron Oasis [25].....	51

Obr. 32: Příklad použití GSM ovladače David [26]	52
Obr. 33: Příklad použití IP kamery AXIS 210 [9]	52
Obr. 34: Struktura Honeywell – MB 48 [13]	53
Obr. 35: Topologie ústředen Galaxy Dimension [12]	54
Obr. 36: Topologie systému Galaxy DIGIPLEX EVO [11], <i>upravil Kovařík 2012</i>	55
Obr. 37: Topologie systému TotalGuard [27]	56
Obr. 38: Topologie inteligentní elektroinstalace iNELS [28]	57
Obr. 39: Topologie systému Nikobus [29]	58
Obr. 40: Topologie systému ABB i-bus KNX [16]	59
Obr. 41: Struktura systému ALVIS [30]	61
Obr. 42: Okruhy systému VAR-NET INTEGRAL [11]	63
Obr. 43: Prostředí systému VAR-NET INTEGRAL [31]	64
Obr. 44: Možnosti propojení [24]	66
Obr. 45: Procesní schéma systému Integra 3 [33]	67
Obr. 46: Architektura systému [23]	68
Obr. 47: Prostředí programu [33]	68
Obr. 48: Kompatibilita zařízení [32]	69
Obr. 49: Prostředí SW SIMS [35]	71

SEZNAM TABULEK

<i>Tabulka 1: Rozsahy napětí pro elektrické zařízení nízkého napětí.....</i>	<i>15</i>
<i>Tabulka 2: Všeobecné požadavky na CCF</i>	<i>26</i>
<i>Tabulka 3: Produkty jednotlivých systémů</i>	<i>62</i>
<i>Tabulka 4: Kompatibilita technologií s programem.....</i>	<i>65</i>
<i>Tabulka 5: Podporování výrobci PPC.....</i>	<i>70</i>
<i>Tabulka 6: Komparace HW produktů pro integraci.....</i>	<i>72</i>
<i>Tabulka 7: Komparace podle vhodnosti použití</i>	<i>73</i>
<i>Tabulka 8: Podpora bezpečnostních technologií.....</i>	<i>74</i>
<i>Tabulka 9: Ceny produktů</i>	<i>74</i>
<i>Tabulka 10: Akce při zastřežení, odstřežení a poplachu pro obytné prostředí</i>	<i>77</i>
<i>Tabulka 11: Akce při zastřežení, odstřežení a poplachu pro průmyslové prostředí.....</i>	<i>78</i>