Česká zemědělská univerzita v Praze

Technická fakulta

Analýza přenosových frekvencí pro bezdrátové přenosy EZS

Bakalářská práce

Vedoucí práce: Ing. Zdeněk Votruba

Autor práce: Lubomír Dostálek

PRAHA 2012

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra technologických zařízení staveb

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Dostálek Lubomír

Silniční a městská automobilová doprava

Název práce

Analýza přenosových frekvenci pro bezdrátové přenosy EZS

Anglický název

Analysis of transmission frequencies for wireless intrusion detection

Cíle práce

Klíčovým cílem práce je posoudit závislost přenosové frekvence bezdrátového datového přenosu v rámci rozvodů EZS (a souvisejících systémů) na kvalitě a bezpečnosti přenosu. Definovat min. požadavky na zabezpečení a princip použití bezdrátových přenosů v bezpečnostních systémech a eventuálně navrhnout vlastní řešení.

Metodika

Prvořadým úkolem je zpracování odpovídající literární rešerše a seznámení se s možnostmi a praxí při realizaci bezdrátových datových přenosů v zabezpečovací technice. Následně definovat klíčové parametry pro nejvíce používané typy přenosů a ověřit jejich funkčnost. Na základě těchto zjištění případně navrhnout novou technologii či princip bezdrátových datových přenosů v zabezpečovací technice. Vyslovit závěry a doporučení, definovat rizika a problémová místa při nesplnění uvedených doporučení. Zhodnotit finanční náklady.

Osnova práce

1. Úvod
2. Problematika systémů EZS
3. Datové přenosy v systémech EZS
3.1. smyčkové systémy
3.2. sběrnicové systémy
3.3. bezdrátové a hybridní systémy
4. Rozbor používaných frekvencí
4.1. 433MHz
4.2. 868 MHz
4.3. další frekvence
5. Návrh alternativní či nové varianty
6. Shrnutí a zhodnocení
7. Závěr a finanční zhodnocení

Rozsah textové části

30 stran textu včetně obrázků , grafů a tabulek

Klíčová slova

bezdrátové přenosy, EZS, CCTV, počítačové sítě

Doporučené zdroje informací

Stanislav Křeček, Příručka zabezpečovací techniky, ISBN 80-902938-2-4

T. Loveček – P. Nagy, 2008, Bezpečnostní systémy – Kamerové bezpečnostní systémy ISBN 978-80-8070-893-1

zdroj Internet např.: Komprese dat, Jakub Nerad, ČVUT Děčín, Teorie kódování
http://katka.dc.fjfi.cvut.cz/vyuka/tk/prezentace/Nerad.pdf

Vincenzo de Astis, Bruno Gasparin, Security technology handbook, published – March 2006

SECURITY Magazín ISSN 1210-8723

Vedoucí práce

Votruba Zdeněk, Ing.

Konzultant práce

Hart Jan

Termín zadání

listopad 2010

Termín odevzdání

duben 2012

doc. Ing. Miroslav Přikryl, CSc.
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
TECHNICKÁ FAKULTA

V Praze dne 4.2.2011

prof. Ing. Vladimír Jurča, CSc.
Děkan fakulty

Prohlášení

Prohlašuji, že předložená bakalářská práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze dne 1.4.2012 Podpis:……

Poděkování

Tímto bych rád poděkoval mému vedoucímu práce, panu Ing. Zdeňku Votrubovi, za vedení při tvorbě této bakalářské práce. Děkuji především za ochotu a trpělivost, kterou mi věnoval.

Abstrakt: Cílem této práce je posoudit závislost přenosové frekvence bezdrátového datového přenosu v rámci rozvodů EZS (Elektrické Zabezpečovací Systémy) a dalších souvisejících systémů na kvalitě a bezpečnosti přenosu. Definovat minimální požadavky na zabezpečení a princip použití bezdrátových přenosů v bezpečnostních systémech.

Klíčová slova: Bezdrátové přenosy, EZS (Elektrické Zabezpečovací Systémy), CCTV (Uzavřený televizní okruh), počítačové sítě.

Analysis of trensmission frequencies for wireless intrusion detection

Summary: Te aim of this Bachelor's work is to assess the frequency dependence of the transmission of wireless data transmission in the distribution of ESS (Intruder Alarm Systems) and other related systems on the quality and security of transmission. Define minimum requirements for security and the principle of using wireless transmissions in security systems.

Key words: Wireless Transmissions, ESS (Intruder Alarm Systems), CCTV (Closed Circuit Television), PC networks.

OBSAH

1 ÚVOD

Tato bakalářská práce pojednává o současném, částečně budoucím stanovisku bezdrátových systémů a zařízení v PZTS (Poplachové Zabezpečovací a Tísňové Systémy, dále jen jako „PZTS“) a jemu blízké problematice. V dnešní době jsou systémy PZTS na velmi vysoké úrovni a stále se zlepšují, ruku v ruce s vývojem techniky. To má však i svá negativa, jak je již známo, každá akce má i svou reakci a člověk jako pachatel není rozhodně pozadu. Neustále totiž vyvíjí nové propracovanější metody napadení a snaží se, aby co nejefektivněji překonal zabezpečovací zařízení. V mém případě se převážně jedná o napadení systému, buďto v klidovém stavu, kdy detektor ještě nevysílá data ústředně, nebo je již aktivní a probíhá přenos informací. Snaha je tedy o posouzení zda zvolený výrobce bezdrátových systémů splňuje požadavky zabezpečovací normy bezdrátového přenosu. V případě, že systémy nepotvrdí svoji bezpečnost udávanou výrobcem, je naší povinností zjištěná data důkladně analyzovat a patřičným způsobem kontaktovat výrobce o případných nedostatcích systému.

V teoretické části je nastíněna související problematika z pohledu platných norem a legislativy zabezpečovacích systémů. Přesněji je přiblížena funkce a charakteristika používaných systémů s jejich přednostmi a nedostatky. Pro snazší porozumění rozdílům v přenosu dat, je v práci rozveden, jak bezdrátový přenos dat od ústředny na PCO (Pult Centralizované Ochrany dále jen „PCO“), tak zároveň smysl drátové a bezdrátové komunikace mezi ústřednou a detektory, která je stěžejním obsahem praktické části této práce.

Hlavní náplní praktické části je tedy analýza komunikace mezi ústřednou a detektory. Úkolem je pak stanovit odolnost systémů proti nežádoucím rušivým vlivům, konkrétně použitím dvou základních principů měření těchto vlivů, kterými jsou detekce zarušení pásma a dohled bezdrátových detektorů. Přenosu dat v PZTS dochází ve volných pásmech ISM na frekvencích 433 MHz a 868 MHz. Pro analýzu v těchto pásmech byly vybrány bezdrátové systémy („PROFI“ pracující v pásmu 433 MHz a „OASIS“ pro pásmo 868 MHz) jednoho z předních výrobců zabezpečovací techniky a to společnosti JABLOTRON ALARMS a.s. Oba bezdrátové systémy byly testovány na stejných principech.

Alternativou pro budoucnost bezdrátových přenosů v PZTS by mohla být dle mého názoru moderní komunikační technologie „ZigBee“, která má velmi dobré předpoklady pro splnění náročných požadavků zabezpečovacích systémů.

Důležitou zmínkou je, že PZTS se stalo novým označením pro EZS (Elektronické Zabezpečovací Systémy dále jen „EZS“), které již není dle normy 50 131-1 platné, ale vzhledem k tradici se nadále v práci budu držet označení EZS.

2 PROBLEMATIKA SYSTÉMŮ EZS

Správně tedy poplachové zabezpečovací a tísňové systémy (PZTS, dříve EZS) jsou soubor zařízení, kterými se signalizuje nebezpečná situace z hlediska neoprávněného vniknutí pachatele. Tím se vytváří předpoklad k jeho rychlému zadržení. Mezi hlavní funkce systémů EZS se řadí detekce a signalizace pokusu o narušení střeženého prostoru. Pro detekci jsou pak používány různé principy a druhy detektorů. Systém EZS po zjištění poruchy či napadení poskytne informaci o čase a místě narušení, kterou odešle na PCO, příslušnému orgánu, nebo majiteli objektu. Zaslání informace o narušení je možné ve více formách, které budou rozvedeny v rešeršní části práce.

2.1 Normy EZS

Jedinou normou zabývající se problematikou Elektronických zabezpečovacích systémů byla dlouhá léta v našem systému norem norma ČSN 334590. Český normalizační úřad vydal v roce 1999 jako ČSN EN50131-1 evropskou normu EN 501131-1 zahrnující všeobecné požadavky na EZS, která normu ČSN 334590 nahrazuje. Oficiální zrušení normy bylo odsouhlaseno na základě hlasování v TNK 124 dne 14. května 2001 a ve věstníku ÚNMZ 3/2002 vyšlo oficiální oznámení o zrušení této normy.[1]

Dalším zdrojem terminologie je norma ČSN EN 50131/Z1 vydaná v roce 2000, která do systému českých technických norem zpracovává normy z oblasti EZS. Toto znění popisuje prostředí, ve kterém se předpokládá, že bude komponent EZS pracovat. Jsou zde specifikovány všechny požadavky na komponenty EZS.

Dále jsou v následujícím textu zachovány původní definice pojmů ze zrušené normy ČSN 334590, a současně tam, kde existují ekvivalentní nebo související pojmy a definice v normě ČSN EN 50131-1:1999, ČSN EN 50131-1/Z1:2000 či dalších norem řady ČSN EN 5013++, jsou uvedeny paralelně i ony.

Vzhledem k tomu, že za několik posledních měsíců došlo k několika změnám v platnosti norem i jejich obsahu, uvádíme zde výčet těchto změn. Protože však v řadě případů nedošlo k jejich zrušení, pouze k jejich částečné inovaci, ponecháváme

zde i předchozí výčet norem s jejich popisem. Je však nezbytné při podrobném procházení dané normy kontrolovat, zda se řídíme podle platného znění normy.

Norma ČSN EN 50131-1

Tato norma pro **Poplachové systémy - Elektrické zabezpečovací systémy - Část 1: Všeobecné požadavky** byla v 4/2009 **zrušena** a nahrazena normou ČSN EN 50131-1 ED. 2, která byla naposledy aktualizována 7/2011.

Norma ČSN EN 50131-6

Tato norma pro **Poplachové systémy - Elektrické zabezpečovací systémy - Část 6: napájecí zdroje** byla v 11/2010 **zrušena a nahrazena** normou ČSN EN 50131-6 ED. 2, s účinnosti 12/2008.

Norma ČSN CLC/TS 50131-2-x

Tato norma pro **Poplachové systémy - Elektrické zabezpečovací systémy - Část 2-x** byla v 11/2010 **zrušena a nahrazena** normou **ČSN EN 50131-2-x**, s účinnosti 01/2009.

Norma ČSN EN 50131-2-6

Tato norma pro **Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-6: Detektory otevření (magnetické kontakty)** je od 05/2009 nově platná**.**

Norma ČSN CLC/TS 50131-2-7-1

Tato norma pro **Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-7-1: Detektory narušení - Detektory rozbíjení skla (akustické)** je od 03/2010 **nově platná**.

Norma ČSN CLC/TS 50131-2-7-2

Tato norma pro **Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-7-2: Detektory narušení - Detektory rozbíjení skla (pasivní)** je od 03/2010 **nově platná**.

Norma ČSN CLC/TS 50131-2-7-3

Tato norma pro **Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 2-7-3: Detektory narušení - Detektory rozbíjení skla (aktivní)** je od 03/2010 **nově platná**.

Norma ČSN CLC/TS 50131-3

Tato norma pro **Poplachové systémy - Elektrické zabezpečovací systémy - Část 3: Ústředny** platná od 6/2005 byla **změněna** 1/2010.

Norma ČSN CLC/TS 50131-4

Tato norma pro **Poplachové zabezpečovací a tísňové systémy - Část 4: Výstražná zařízení** byla v 02/2008 **zrušena a nahrazena** normou **ČSN EN 50131-4**, s účinnosti 04/2010.

Norma ČSN CLC/TS 50131-7

Tato norma pro **Poplachové systémy - Elektrické zabezpečovací systémy - Část 7: Pokyny pro aplikace** byla v 11/2009 **zrušena a nahrazena** normou **ČSN CLC/TS 50131-7**, s účinnosti 05/2011.

Norma ČSN EN 50131-8

Tato norma pro **Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 8: Zamlžovací bezpečnostní zařízení/systémy** je od 04/2010 **nově platná**.

Norma ČSN 50136-1-1

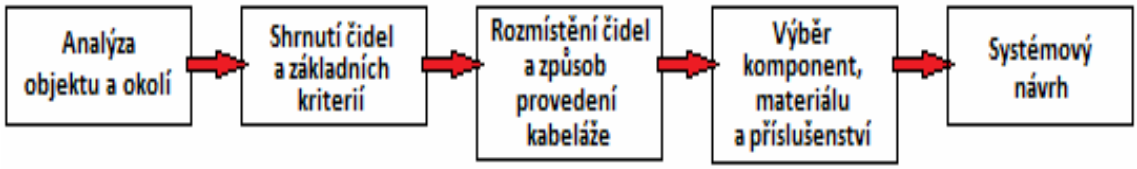
Tato norma pro **Poplachové systémy - Poplachové přenosové systémy a zařízení - Část 1-1: Všeobecné požadavky na poplachové přenosové systémy** platná od 7/1999 byla **změněna** 3/2002 a následně 2/2009.

2.2 Návrh systémů EZS

Zařízení elektrické zabezpečovací signalizace (zařízení EZS) je soubor čidel, tísňových hlásičů, ústředen, prostředků poplachové signalizace, přenosových zařízení, zapisovaných zařízení a ovládacích zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno na určeném místě narušení střeženého objektu nebo prostoru.[2]

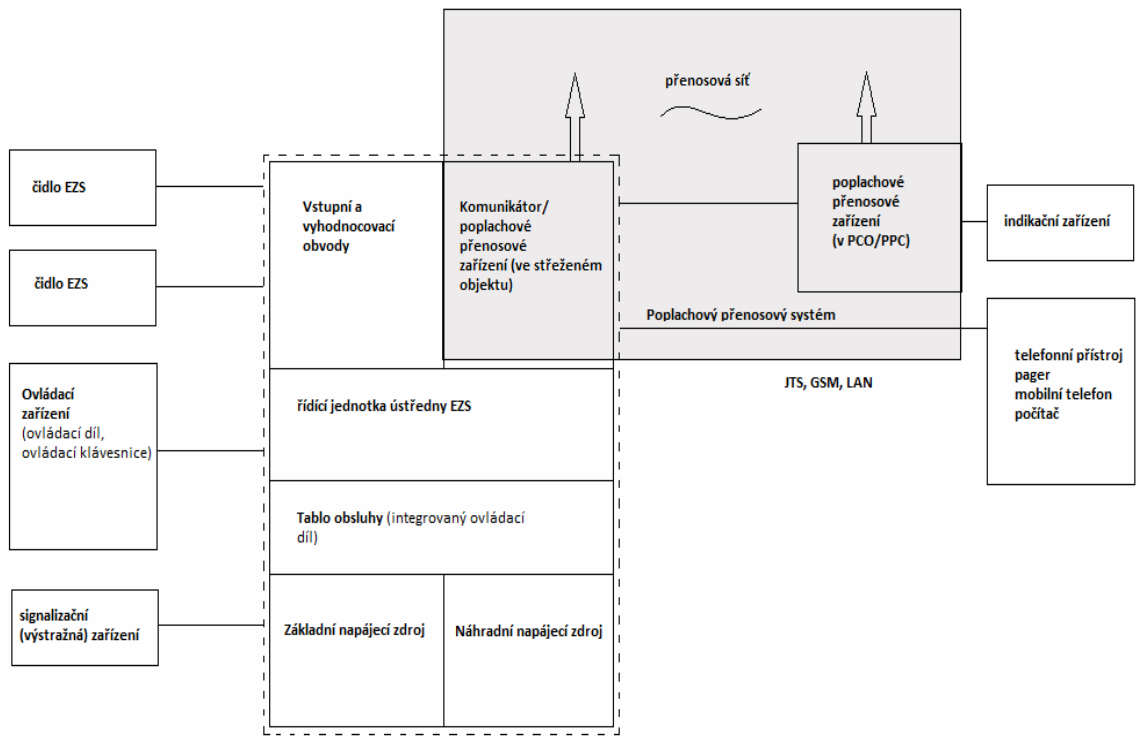
Návrh systémů EZS je charakterizován jako proces, při němž je stanovován rozsah systému, stupeň odpovídajícího zabezpečení (viz. Tab. 1), komponenty odpovídající témuž stupni zabezpečení, volby protiopatření a třídy prostředí. V průběhu procesu dochází k vhodnému výběru ústředny, způsobu provedení kabeláže, ke stanovení počtu a typu detektorů, typu ovládacích a indikačních zařízení a dalších doplňkových zařízení. Návrh systémů EZS rovněž může sloužit pro přibližný odhad ceny navrhovaného systému.

Obr. 1 Sled událostí při návrhu systémů EZS



[Zdroj: **(vlastní)**]

Obr. 2 Schematické znázornění systému EZS



[Zdroj: **(1)**]

2.3 Funkce EZS

Optimálně EZS zaregistruje každý pokus o neoprávněný vstup do střeženého prostoru či objektu. Toto zjištěné narušení, předá v podobě informace na předem určená místa buďto radiovými prostředky, po telefonních linkách, přes GSM bránu nebo prostřednictvím sítě LAN/WAN. Takovým místem může být například služebna policie vybavená PCO, odkud je pak zorganizován výjezd zásahové jednotky. Informaci o alarmu je také možno získat formou SMS na mobilní telefon. Hlavním prvkem a zároveň řídící jednotkou každého zabezpečovacího systému EZS je ústředna, která obsluhuje různá množství smyček, na kterých jsou připojena koncová zařízení. Popisem a přiřazením čísel jednotlivým smyčkám jsme pak schopni identifikovat místo narušení, ve kterém došlo k vyhlášení poplachu. EZS může mít i další funkce jako jsou nap: hlídání vzniku požáru, úniku plynu, zaplavení a dalších stavů v objektu. EZS také hlídá sama sebe a poplach je tak vyhlášen i při pokusu o sabotáž na jednotlivých komponentech. Proti výpadku elektrického proudu je EZS chráněna záložním zdrojem. Při dlouhodobém výpadku napájení je následně rovněž vyhlášen poplach. Celý systém lze jednoduše a intuitivně ovládat pomocí přehledné klávesnice nebo prostřednictvím bezdrátových

vysílačů či přístupového systému (ACS/ID). Může také aktivně spolupracovat i s kamerovým systémem (CCTV).[10]

2.4 Třídy EZS

Podle účinnosti, spolehlivosti a zapojení se EZS rozděluje do čtyř tříd. V nejnižší třídě je zpravidla zařazen systém, který zajišťuje pouze kontrolu vstupů do střeženého prostoru, obvykle jednoduchými magnetickými kontakty na dveřích či oknech. Nejvyšší třída je naopak určená například pro vládní objekty, kritické uzly, státní infrastruktury a bezpečnostní složky včetně centrálních bank. Zde se již používají zdvojená čidla se snímáním prostoru na dvou různých principech a kombinace více typů čidel v jednom střeženém prostoru.

Třídy (kategorie) EZS jsou odstupňovány dle normy ČSN a odborových předpisů pojišťoven. Rozdělení je znázorněno v následující tabulce.

Tab. 1 Kategorie EZS

Stupeň	Míra rizika	Předpokládaný typ narušitele
1.	**Nízké**	Narušitel má malou znalost EZS; omezený sortiment snadno dostupných nástrojů
2.	**Nízké až střední**	Narušitel má určité znalosti o EZS; omezený sortiment základních přenosných nástrojů (např. multimetr)
3.	**Střední až vysoké**	Narušitel je obeznámen s EZS; úplný sortiment základních přenosných přístrojů a elektrických zařízení
4.	**Vysoké**	Narušitel je schopen, nebo má možnost zpracovat podrobný plán vniknutí; kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků EZS

[Zdroj: **(6)**]

3 DATOVÉ PŘENOSY V SYSTÉMECH EZS

3.1 Datové přenosy mezi senzory a ústřednou EZS (místní)

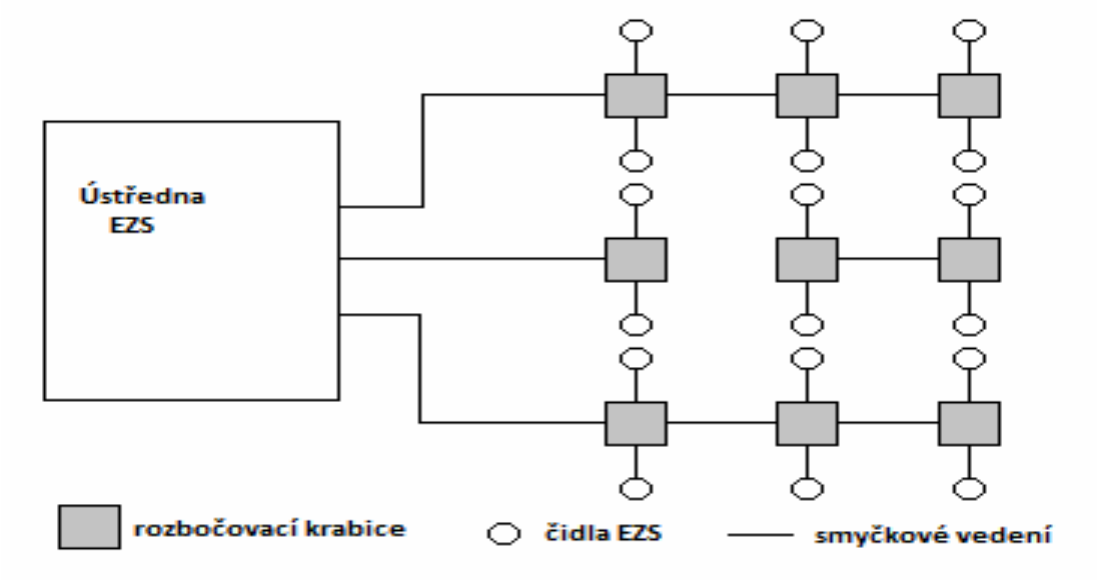
Rozdělujeme je v závislosti na použití určité ústředny EZS, která s detektory komunikuje následujícími způsoby:

- Smyčkové systémy
- Sběrnicové systémy
- Bezdrátové a hybridní systémy

3.1.1 Smyčkové systémy

Mají pro každou poplachovou smyčku vstupní vyhodnocovací obvod. Ten je řešen pro připojení proudových smyček o definované hodnotě a toleranci. Smyčka je zakončena zakončovacím odporem tak, aby vykazovala předepsanou hodnotu odporu pro příslušný typ ústředny. Změna odporu smyčky, způsobená aktivací některého z čidel smyčky nebo sabotáží na smyčce, vede k vyhlášení poplachového stavu systému EZS. Poplachové smyčky systému EZS jsou tvořeny nejčastěji sériovým zapojením rozpínacích kontaktů čidel. Smyčkový systém má rozsáhlou kabelovou síť, neboť ke každému čidlu musí být přiveden kabel příslušné smyčky, kabel musí obsahovat dva vodiče pro napájení čidla (u napájených čidel), dva vodiče pro poplachový kontakt čidla, dva vodiče pro sabotážní kontakt čidla a dále vodiče dodatkových funkcí typu paměť poplachu, test chůzí, odpojení vysílače ultrazvuku či mikrovlnného výkonu, indikace překrytí čidla apod.[1]

Obr. 3 Zapojení smyčkového systému



[Zdroj: **(1)**]

3.1.2 Sběrnicové systémy

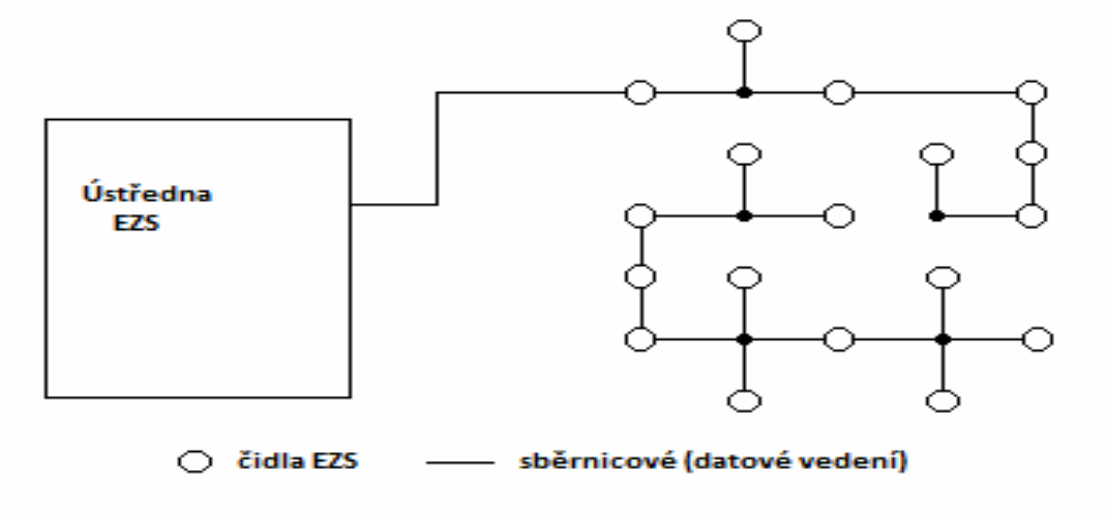
3.1.2.1 Systémy s přímou adresací čidel

Jsou založeny na principu komunikace po datové sběrnici ústředna – senzory (čidla). Ústředna periodicky generuje adresy jednotlivých čidel a přijímá příslušné odezvy. Každé čidlo je vybaveno komunikačním modulem. Kabelová síť tohoto systému je minimální, neboť je tvořena prakticky libovolnou konfigurací kabelové sítě (s max. délkou řádově stovky metrů). Jednotlivá čidla jsou připojena v libovolném pořadí na zpravidla čtyřvodičové vedení, kde dva vodiče slouží pro napájení čidla a dva jako datová sběrnice. Velkou výhodou tohoto systému je, že při narušení objektu ústředna oznámí, které konkrétní čidlo bylo aktivováno a o jaký druh narušení se jedná (poplachový kontakt, sabotážní kontakt dále indikují zkrat na lince, případně další stavy).

Tento systém přináší výhody uživateli v případě, že je v objektu místo trvalé obsluhy nebo je-li přenos na PCO či monitorovací pult hlídací služby realizován jako mnohakanálový. V jiném případě výhody přímé adresace, kterou ocení hlavně instalační firma při servisu systému.

Jednoduchost kabelové sítě je však vykoupena nemožností realizovat po datové sběrnici dodatkové funkce čidel. Rovněž konfigurace kabelové sítě má svá omezení. Jedním z nich je celková délka vedení, dále je nutné vyvarovat se uzavřených okruhů přes nezanedbatelnou plochu, do nichž by se mohlo indukovat elektromagnetické rušení. Při projekci musíme pečlivě zvažovat odběr jednotlivých částí systému a počítat úbytky na napájecích vodičích. Typický počet přímo adresovaných čidel se u systémů tohoto typu pohybuje řádově v desítkách.[1]

Obr. 4 Zapojení s přímou adresací



[Zdroj: **(1)**]

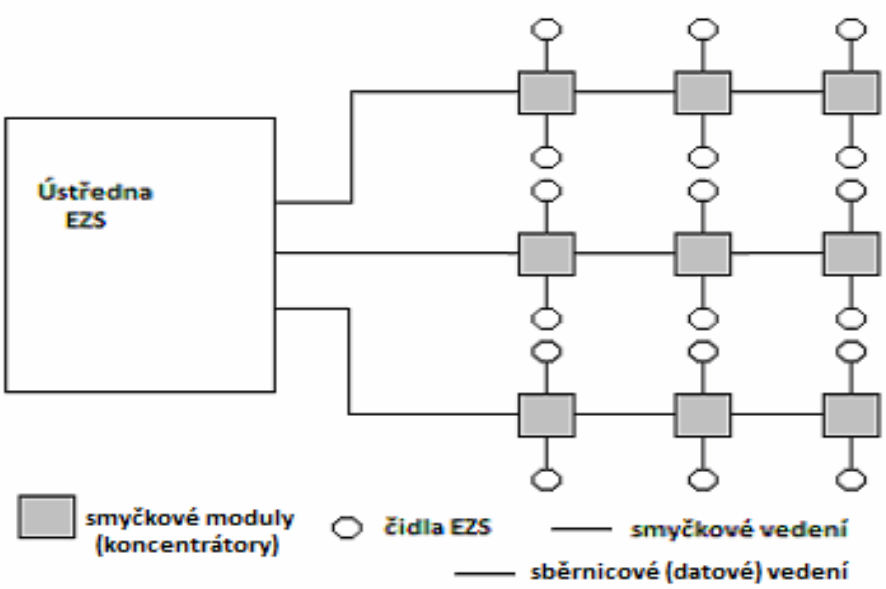
3.1.2.2 **Systémy smíšeného typu**

Pracují na principu datové komunikace ústředna – koncentrátor (sběrnicový modul smyček). Komunikace mezi ústřednou a koncentrátory probíhá pomocí datové či analogové sběrnice. Na koncentrátory jsou čidla připojena pomocí smyček jako u smyčkových systémů. Vlastní vyhodnocování probíhá podle typu ústředny různě. Jednou z variant je analogový multiplex, kdy se připojují na sběrnici postupně jednotlivé smyčky, a vyhodnocení impedance smyčky s příslušnou odezvou provádí ústředna. Další možností je integrace vyhodnocovací logiky včetně vyrovnávací paměti přímo do koncentrátoru. Komunikace však probíhá čistě v datové podobě.

Pokud je kapacita ústředny dostatečná, lze na jednotlivé vstupy koncentrátorů připojit přímo jednotlivá čidla. Tím přechází tento typ systému na systém s přímou

adresací čidel se všemi jejími výhodami. Limitujícím faktorem zde však většinou budou celkové náklady na takto vybudovaný systém. Z tohoto důvodu je potřebné navrhnout optimální rozdělení čidel do smyček tak, aby byla zachována z hlediska uživatele účelná úroveň adresace. Důležitým aspektem návrhu systému zůstává, obdobně jako u předešlých systémů, dostatečné dimenzování napájecích i datových vodičů zvláště u rozsáhlých systémů (délka jedné datové sběrnice až do 1 km, s opakovači i více). Navíc tato skupina většinou umožňuje realizaci dodatkových funkcí přímo přes datovou sběrnici.[1]

Obr. 5 Zapojení smíšeného typu



[Zdroj: **(1)**]

3.1.3 Bezdrátové a hybridní systémy

3.1.3.1 Systémy s bezdrátovým přenosem od čidel

Nejčastěji se používá pásmo telemetrie (433 MHz) s výkony okolo 10mW. Další možností je pak využití pásma 868 MHz. Jedná se o vysílací zařízení, které spadá pod působnost legislativy. Přenos poplachového signálu je nejčastěji 8bitový, kódovaný a adresa senzoru je 4bitová. Výběrem vhodného návrhu je dosaženo minimálního klidového odběru (cca 10-20 μA). Vlastní dosah ve volném prostředí je 100 – 200 m. V objektu je třeba počítat s menšími vzdálenostmi. Čidla jsou napájena buď lithiovou

baterií, nebo 9V destičkovým článkem. Napětí baterie je hlídáno a podle provedení, buď dojde při poklesu napětí k místní akustické signalizaci interním bzučákem, což upozorní obsluhu na nutnost výměny, nebo je tato informace přenášena do poplachové ústředny.[1]

Mezi výhody je zahrnuta rychlá a snadná instalace systému, možnost instalace do hotových objektů bez zásahu nebo s minimálním stavebním zásahem, dále je také možno snadno rozšířit systém doplněním dalších prvků EZS a jejich snadná změna konfigurace.

Systémy s jednosměrnou komunikací (simplex)

Přenos je zajištěn jednosměrně, tzn., že v čidle je vysílač a v ústředně přijímač. Pracují na principu pravidelné kontroly přenosové cesty vysíláním kontrolních telegramů. Problémem je však rozpor mezi požadavkem na co nejvyšší četnost kontrol a požadavkem na velkou výdrž baterií napájejících jednotlivé prvky. [11]

V praxi jsou kontroly s četností několika hodin. To ovšem znamená, že je ústředna o nefunkčnosti prvku informována s určitým zpožděním. Jestliže u tohoto systému poškodí pachatel detektor, může uživatel systém zapnout s mylným přesvědčením, že je objekt plně zabezpečen. Vzhledem k tomu, že je nutné vyloučit nebo alespoň omezit plané poplachy vzniklé náhodným výpadkem signálu, způsobené nejrůznějšími příčinami, vyhodnocuje se stav, obvykle jako poruchový nebo poplachový až tehdy, nedojde-li několik po sobě jdoucích kontrolních relací. Tím je ale opět prodloužena doba, během níž systém nemusí zaznamenat poplach nebo poruchu. Nedoporučuje se používat systém tam, kde je velký pohyb osob (např. veřejné budovy) a to proto, že jednotlivé prvky nemají informaci o tom, zda je systém v klidovém nebo střežícím stavu. Tedy při každém pohybu, nebo zjištění poplachového stavu v dosahu detektoru musejí vždy vyslat signál ústředně což má za následek vyčerpávání energie napájecího zdroje. Toto je řešeno časovačem (součást detektoru), který blokuje po odeslání zprávy po dobu několika minut vysílání. Sice tato metoda šetří energii zdroje, ale zároveň to ztěžuje vyhodnocení pohybu pachatele, protože jeho pohyb po první aktivaci není v dalších minutách monitorován.[1]

Systémy s obousměrnou komunikací (duplex)

Každý prvek systému je vybaven jak vysílací, tak přijímací elektronikou (modulem vysílač/přijímač). Tyto inteligentní moduly mají schopnost si najít ve vyhrazeném kmitočtovém pásmu dva volné kanály pro přenos a automaticky se na ně naladit. V případě rušení těchto kanálů jsou schopny se přeladit na jiné, které jsou nezarušené. Zavedení obousměrné komunikace mezi ústřednou a všemi prvky zabezpečovacího systému odstraňuje výše jmenované nedostatky jednosměrných systémů.[1]

Hlavními přednostmi obousměrné komunikace je při zapnutí systému kontrola stavu všech prvků ústřednou. Čidla, která jsou, v klidovém stavu nevysílají a tak neplýtvají energií, zároveň nemusejí být vybaveny časovačem. Ústředna je schopna si ověřit, zda je došlá poplachová informace skutečný poplach, což umožňuje vyloučit plané poplachy způsobené rušením. Jako nevýhoda je uváděn zvýšený nárok na pravidelnou kontrolu baterií senzorů.

Kódování přenosu a prvků

Přednostním požadavkem je samozřejmě u bezdrátových prvků kódování komunikace mezi jednotlivými prvky systému. To znemožňuje zkreslení během přenosu a znesnadňuje tak neoprávněné vniknutí do systému s cílem vyřadit systém z provozu. Kromě toho je nutno jednotlivé prvky v systému identifikovat. U jednodušších systémů se kódování prvků uskutečňuje obvykle naprogramováním mechanickými přepínači binárním způsobem (tzv. DIP – switch), případně programováním pomocí připojeného počítače. U sofistikovaných systémů mají prvky kód pevně přidělen již při výrobě a jejich čísla se programují do ústředny při instalaci systému. Tím je znesnadněno cílené nahrazení (substituce) prvky s konkrétní adresou při pokusu o kvalifikované nabourání systému.[1]

3.1.3.2 Hybridní systémy

Skládají se jak z prvků drátových tak bezdrátových, využití je platné zejména při rozšíření stávajícího drátového systému bez nutnosti instalovat dodatečně kabeláž. Spojují tedy výše uvedené systémy. Vše záleží na zvolené ústředně, která je schopna pracovat jak s drátovými tak s bezdrátovými prvky.

3.2 Datové přenosy od ústředny EZS k PCO (dálkové)

I ten nejlepší systém EZS je pouze shromaždištěm informací a tedy jeho využití je velmi omezeno, to však pouze za předpokladu, že není napojen na komunikační kanál, se kterým je spojen PCO. Tímto spojením dosáhneme maximálního využití systému EZS. Tato spojení jsou:

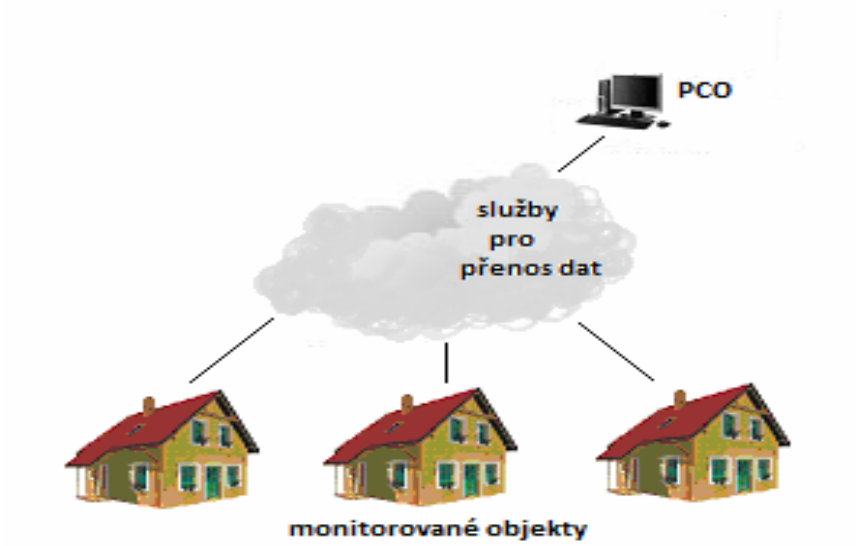
- Přenos prostřednictvím jednotné telefonní sítě (JTS)
- Přenos prostřednictvím textových zpráv (SMS – pomocí GSM)
- Přenos prostřednictvím datové sítě (GSM/GPRS)
- Přenos prostřednictvím internetu (TCP/IP)
- Kombinované přenosy

3.2.1 Jednotné telefonní sítě (JTS)

Jedná se o nejsnazší způsob připojení k PCO. Jsou definovány jako fyzické připojení koncových zařízení ke spojovacím systémům. Úkolem je zajistit přesnost elektrických signálů pomocí metalického vedení. Koncovým zařízením je nejčastěji klasický analogový telefon nebo ISDN telefon, telegraf, fax a další telefonní komponenty. Spojovacími systémy jsou míněny telefonní ústředny různých generací. Přenosem elektrických signálů má být zajištěna telefonní signalizace a přenos hlasu v elektrické podobě.[12]

- Mezi klady tohoto systému přenosu dat je možno zařadit snadnou instalaci a zprovoznění, dále skutečnost kdy moderní EZS již dnes zpravidla obsahují JTS komunikátor.
- Nevýhodou jsou však telefonní poplatky. Každá odeslaná informace odečte impulz, který je následně vyúčtován poskytovatelem telekomunikačních služeb. Další nevýhodou je testování přenosu mezi EZS a PCO, které se nejčastěji nastavuje 1× za 24 hodin, což pro bezpečnostní zařízení není ideální.

Obr. 6 Schéma přenosu JTS



[Zdroj: **(vlastní)**]

3.2.2 Textové zprávy (SMS přenos přes GSM sítě)

Tento přenos je určen pro základní zabezpečení objektů na místech, která nemají pokrytí JTS ani GPRS. Jeho využití je vhodné například u rekreačních objektů. Testování přenosu mezi EZS a PCO, které je zpravidla nastavováno jako u JTS, tedy 1× za 24 hodin, je ovšem pro tento typ objektů dostačující.[13] Informace je zasílána prostřednictvím GSM sítě zařízením nazývaným GSM pager, který má v sobě zabudovaný GSM modul a je tak schopen zaslat buďto zprávu o narušení, nebo prozvonit číslo tónovým signálem.

- Výhodou je možnost zadávat periodu testování systému libovolně. Další výhodou je možnost využití obousměrné komunikace, samozřejmě v závislosti na použití zvoleného GSM pageru.

- Určitou nevýhodou může být občasné zpoždění v doručení informační SMS. Za nevýhodu se také pokládá nebezpečí provolání vysokých částek. Z tohoto důvodu se doporučuje používat raději kreditních SIM karet a ty postupně dobíjet.

3.2.2.1 **Síť GSM**

Síť GSM tvoří soustavy BTS stanic. Jsou to vysílače (i přijímače) mobilního signálu na frekvenci 900/1800 MHz. Každá BTS stanice má svůj kanál, aby se vzájemně nerušili. Ve vesnicích jsou BTS stanice v malém množství, někde i jedna na tři vesnice. V centru Prahy připadá na každou větší ulici jedna BTS stanice. Jedna BTS stanice je schopna z rozdělení časového kmitočtového pásma obsloužit až 8 telefonních hovorů.[14]

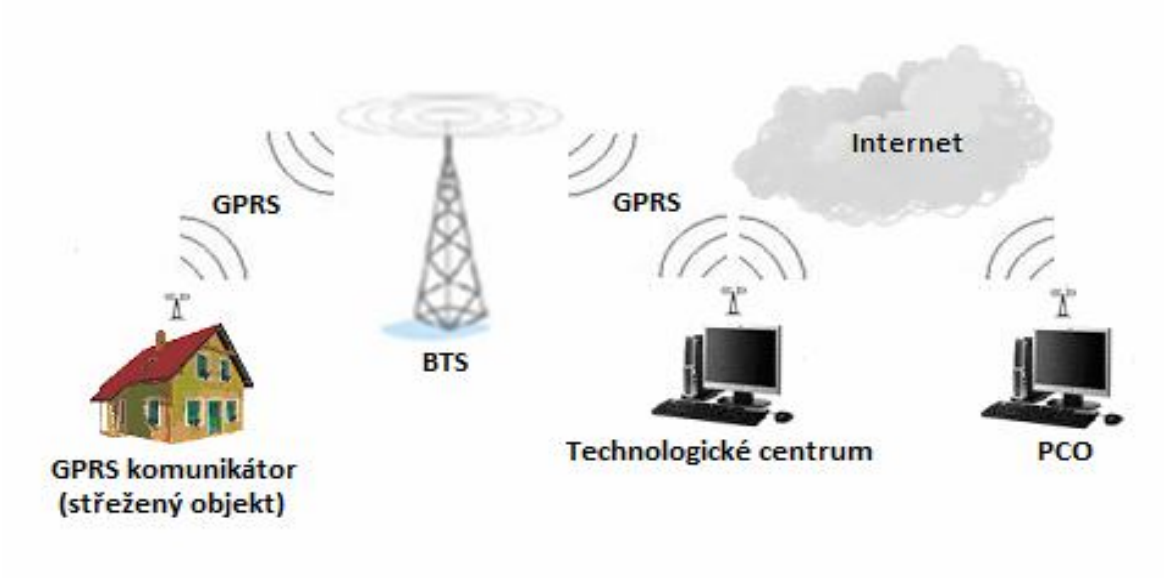
3.2.3 Datové sítě (GPRS)

General Packet Radio Service (Univerzální rádiová packetová služba) je nástavbou sítě GSM pro přenos dat. Jde vlastně o nejrozšířenější alternativu přenosu dat. Pomocí datové sítě jsou přenášena všechna důležitá data. Rychlost přenosu dat je až na 108 kbps, záleží na použitém mobilu či modemu, na kvalitě signálu a zatížení BTS. Ovšem rychlost odezvy (ping, latence) není příliš příznivá. U GPRS se platí za objem přenesených dat nebo paušálem za neomezené připojení.[13]

- Velkou výhodou je díky paušálním platbám možnost nastavit kontrolu spojení v řádech minut. Pomocí přenosu GPRS je možné přenášet téměř neomezené množství informací z EZS, a tak využít maximum jeho možností. Další výhodou je spolehlivé pokrytí signálem GPRS nejen po celé ČR, ale i po celé Evropě.

- Nevýhodou je spolehlivost závislá na momentálním zatížení sítě GSM, systém je možno napadnout rušením a v neposlední řadě finanční náklady spojené s instalací (GSM) modulu což jsou pořizovací cena + práce.

Obr. 7 Schéma přenosu GSM/GPRS



[Zdroj: **(vlastní)**]

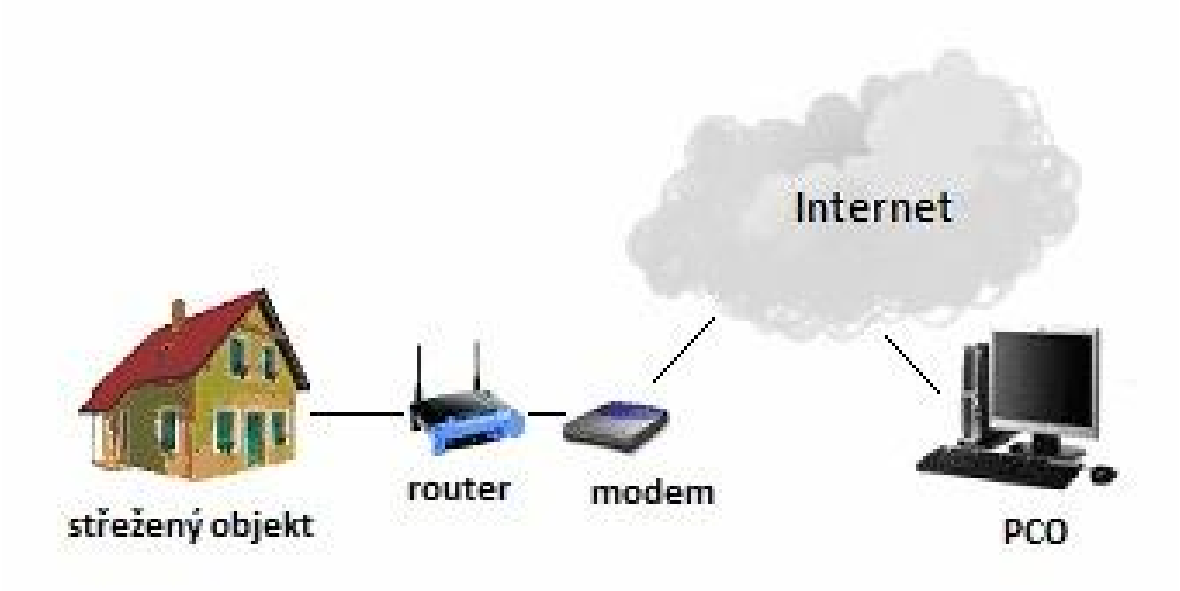
3.2.4 Internet (TCP/IP)

V poslední době je na trhu tato technologie velmi žádaná. A to díky jejím přednostem, kdy je schopna uživateli poskytnout okamžitý přehled nad zabezpečovacím systémem prostřednictvím počítače a počítačové sítě. Následně umožňuje rozesílat poplachovou a technickou informaci pomocí elektronické pošty. Další eventualitou je změna konfigurace a nastavení touto sítí odkudkoli. Připojení k počítačové síti je v podstatě technologicky na stejném principu jako do sítě GSM. Jde o bránu, v tomto případě o IP bránu, která je tvořena kartou s routerem, pomocí kterého je možno sledovat a měnit vlastnosti EZS.[8]

- Hlavní výhodou je provoz s nulovými náklady. Lze nastavit kontrolu spojení v řádech sekund a přenášet všechny informace z EZS. V případě kombinování IP adres a dalšího záložního systému se z něj stává skutečně bezpečné moderní a využitelné připojení.

- Nevýhodou je riziko napadení při nedostatečném nastavení zašifrování konfigurace a služeb (absolutně nevhodný je například nezabezpečený přenos HTTP, FTP nebo TELNET). Tento problém by měl být řešen tak, že brána musí pracovat zároveň jako firewall s možností nastavení přístupu minimálně podle MAC adres.

Obr. 8 Schéma přenosu přes Internet



[Zdroj: **(vlastní)**]

3.2.5 Kombinované přenosy

Kombinace přenosu je v závislosti na použitém zařízení. Kombinovaným připojením je například internet společně s JTS nebo SMS, kdy jsou veškeré informace primárně přenášeny přes internet, ale v případě jeho poruchy je aktivován systém záložní, který z ekonomických důvodů přenáší pouze celkové stavy EZS. Pokud je tedy vyhlášen poplach v objektu, informace je záložní cestou doručena na PCO.

4 ROZBOR POUŽÍVANÝCH FREKVENCÍ

Bezdrátový přenos mezi ústřednou a detektory je prozatím umožněn na dvou technologických frekvencích, konkrétně jde o 433 a 868 MHz, ale v souladu s vývojem je možné, že v nejbližší době budou ústředny s detektory schopny komunikovat i v jiných frekvenčních pásmech. Jelikož jsou tyto pásma přenosu všeobecně používané, může poměrně jednoduše dojít k interakci s jinými zdroji. Obě frekvence spadají do bezlicenčního ISM pásma a vyhovují předpisům FCC (Federal Communications Commission) a ETSI (European Telecommunications Standarts Institute). Rádiovým spojením v EZS se zabývá normalizační výbor CENELEC TC-79 v normě EN 50131-5-3. Tato evropská norma se týká zabezpečovacích a tísňových systémů používajících rádiové spojení umístěných ve střežených prostorech. Netýká se rádiových dálkových přenosů. Z hlediska náročnosti na rádiové spojení tato norma uvádí funkční požadavky na tato zařízení a metody zkoušek.

Hlavní požadavky na rádiové spojení

Útlum signálu

Degradace radiového signálu způsobená změnou v pasivním prostředí systému po jeho instalaci (např. vznik, přemístění odrazivých nebo pohltivých materiálů). Vzhledem ke skutečnosti, že může po instalaci dojít ke změnám v pasivním prostředí, musí být možné během instalace nebo údržby přechodně snížit úroveň přenosového signálu o hodnoty 3, 6, 9, 12 dB dle stupňů zabezpečení uvedených v normě k ověření, že je spojení bez závad.

Kolize

Současné vysílání dvou nebo více rádiových komunikačních zařízení náležících témuž systému o úrovni dostatečné ke způsobení poškození nebo maskování rádiových signálů. Důvodem tohoto požadavku je zajištění vysoké úrovně spolehlivosti přenosu poplachových a monitorovacích zpráv, a tím snížit pravděpodobnost, že by ostatní prvky téhož systému mohly svou konstrukcí způsobit, že by došlo ke ztrátě nebo narušení přenášené informace.

Průchodnost

Poměr celkového počtu zpráv vyslaných vysílajícím zařízením k celkovému počtu zpráv správně interpretovaných přijímacím zařízením. Předmětem tohoto požadavku je stanovit schopnost přijímacího zařízení, což je přesně interpretovat a zpracovat poplachové zprávy.

Odolnost proti neúmyslné a úmyslné záměně komponent a zpráv

Úmyslnou záměnou zpráv je obvykle pokus o snížení úrovně zabezpečení systému především falešným nastavením do klidového stavu. Neúmyslná záměna obvykle způsobí falešné poplachy nebo falešné hlášení sabotáže, které jsou obtěžující. Aby bylo zamezeno možnosti vzniku jak úmyslných, tak neúmyslných záměn zpráv, musí být každý vysílající prvek identifikován prostřednictvím identifikačního kódu jako prvek patřící k systému. Počet možných identifikačních kódů musí odpovídat minimálně požadavkům uvedených v normě.

Odolnost proti rušivým vlivům

Vlivy mající původ uvnitř nebo vně systému a mající za následek narušení přenosu anebo zpracování dat v systému. Mohou být škodlivé neúmyslně nebo úmyslně. Příčinami mohou být snížení úrovně, kolize, nechtěná nebo záměrná náhrada zpráv a další rušivé vlivy rádiového přenosu. Důsledky, které mohou mít rušivé vlivy na signály, jsou:

- Žádný vliv na rádiový signál
- Poškození rádiového signálu nemající za následek žádné porušení zpráv
- Poškození rádiového signálu mající za následek částečné porušení zpráv
- Úplné znemožnění přenosu rádiového signálu (neschopnost příjmu)

Účelem tohoto požadavku je ověřit schopnost zařízení rozlišit mezi užitečným signálem a rušivými rádiovými signály. Tyto požadavky se vztahují na veškeré přijímací zařízení pracující s rádiovými signály. Proto zde musí být aplikovány veškeré rušivé signály uvedené v normě, aniž by způsobily falešné poplachy nebo indikaci ztráty periodické komunikace. Během trvalé aplikace rušivých signálů, daných úrovní, musí být

daných 20 systémových relevantních zpráv (vyslaných vysílacím zařízením používaným pro testovací účely) správně přijato a zpracováno.

Monitorování rádiových přenosových cest

Musí provádět všechna přijímací zařízení. Monitorování musí odpovídat příslušnému stupni zabezpečení a stavu zařízení a typu rušení detekovaného během monitorování. Detekována musí být porucha v periodické komunikaci a rušení cizím signálem.[5]

Testování spolehlivosti bezdrátových systémů

Bezdrátové systémy mají bohužel i značné nevýhody jak už je uvedeno výše. Největší nevýhodou je však právě bezpečnost přenosu informace z detektoru do ústředny. Při přenosu informace je možné frekvenci (po které bezdrátový detektor komunikuje s ústřednou) zarušit nízkofrekvenční rušičkou (které jsou pro tyto pásma běžně dostupné na trhu v cenách několika set korun) a znemožnit neboli sabotovat tak komunikaci. Proto je důležité, aby tyto systémy dokázaly pokusy o zarušení detekovat a správně vyhodnotit. Používají se dva základní způsoby testování a ochrany proti těmto druhům napadení:

- Detekce zarušení pásma
- Dohled bezdrátových detektorů

Detekce zarušení pásma

Funguje na principu skenování pásma, které detektory využívají ke komunikaci s ústřednou. Při jeho obsazení (na výrobcem definovanou dobu) indikuje ústředna toto zarušení. Systém po indikaci zarušení frekvence zareaguje podle naprogramování. Nejčastěji vyhlásí poplach nebo poruchu systému.

Dohled bezdrátových detektorů

Kontroluje přítomnost detektoru. Jedná se v podstatě o pravidelné přihlášení se detektoru k ústředně po určité době. Pokud se detektor z různých důvodů (sabotáž nebo porucha detektoru apod.) nepřihlásí, pak ústředna po definované době indukuje jeho ztrátu a následně zareaguje podle toho, jak je nastavena.

4.1 433 MHz

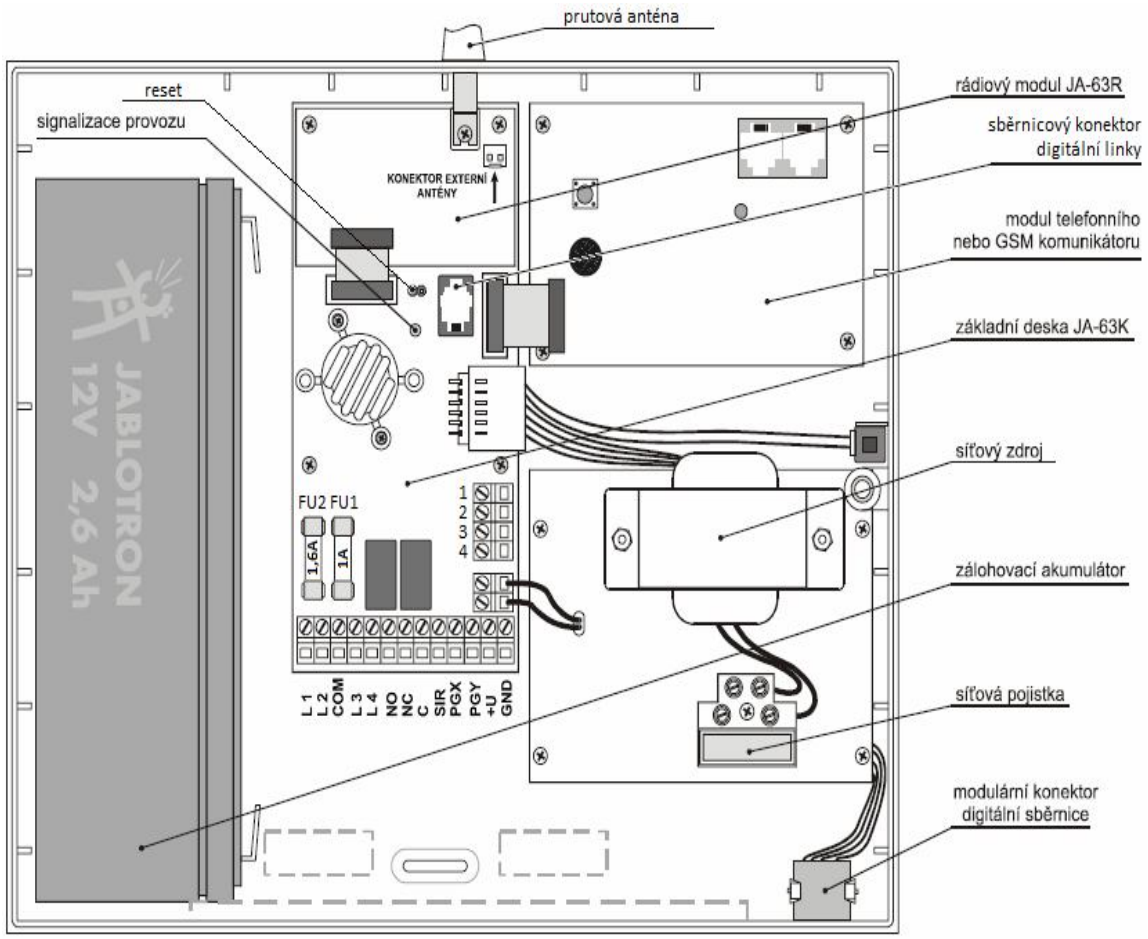
Vhodná pro vzdálenosti několika desítek metrů, vlnová délka je 0,69 m a rychlost přenosu do 9600 b/s s výkony do 10mW.

Spolehlivost přenosu na frekvenci 433 MHz je testována na smyčkovém hybridním zabezpečovacím systému (společnosti ©2008 – 2012 JABLOTRON ALARMS a.s.) JA-63 „PROFI“.

4.1.1 JA-63 „PROFI“

Systém je certifikován podle ČSN EN 50131-1 do stupně 2 (nízká až střední rizika). Certifikace systému a certifikace montážní firmy je podmínkou pro uznání systému dle podmínek asociace pojišťoven. Podmiňuje výplatu pojistné náhrady v plné výši, případně se uplatňuje jako podmínka pro uznání slevy na pojistném.

Obr. 9 Rozmístění jednotlivých prvků ve skříni ústředny



[Zdroj: **(15)**]

4.1.1.1 **Architektura ústředny**

Ústředna JA-63 má sběrnicovou koncepci. V plastové skříni ústředny je síťový zdroj a je zde prostor pro akumulátor 1,3 nebo 2,6 Ah.

Na základní desce ústředny jsou čtyři vstupní svorky pro drátové smyčky (s možností jednoduchého nebo dvojitého vyvažování).

S osazeným rádiovým modulem (JA-63R) má ústředna 16 bezdrátových zón pro snímače řady JA-60 (lze jich přiřadit až 32). Použít lze též až 8 bezdrátových klávesnic nebo dálkových ovladačů, bezdrátové sirény JA-60 a bezdrátové vstupní moduly řady UC. Systém JA-63 je kompatibilní se systémem JA-60 a JA-65. Ve velkých objektech je možno spojovat více systémů – architektura nadřízené a podřízené ústředny (informace z podřízené ústředny se přenášejí do ústředny nadřízené, ovládání obou systémů může být buď nezávislé, nebo může ústředna nadřízená ovládat tu podřízenou).

Telefonní komunikátor JA-65x předává hlasové zprávy, SMS zprávy prostřednictvím SMS serveru, komunikuje s PCO a umožňuje dálkový přístup z počítače instalatéra nebo uživatele (užitím SW ComLink a modemu JA-60U).

Telefonní komunikátor JA-60GSM odesílá informační SMS, zavolá na nastavená čísla a přehraje akustické upozornění, komunikuje s dvěma PCO, umožňuje dálkový přístup z klávesnice telefonu a nastavení prostřednictvím webové stránky.

Při plné konfiguraci (osazení všech modulů) získáte 16-zónový bezdrátový plus čtyřsmyčkový drátový systém. Ústřednu je možno rozdělit programově na dva uživatelsky nezávislé sektory se sdílenou částí (režim dělené ústředny). Ovládání a programování ústředny je možné systémovou klávesnicí JA-60E, doplňkové též vstupní smyčkou. Pokud je osazen rádiový komunikační modul JA-63R je možno systém ovládat a programovat též bezdrátovou klávesnicí JA-60F. Pro ovládání lze v tomto případě užít i dálkové ovladače RC-40 (klíčenka), RC-60 (univerzální ovladač), RC-22 (nástěnný vypínač) a klávesnici JA-60D (ovládací klávesnice). Ústřednu je také možno ovládat, programovat a spravovat počítačem za pomoci programu ComLink, který je dodáván zdarma.[15]

4.1.1.2 Přiřazování (učení) bezdrátových periferií

Pokud je ústředna vybavena modulem R, je možno přiřadit až 32 detektorů (do každé zóny max. 2) a max. 8 dálkových ovladačů či klávesnic. Přiřadit lze, též bezdrátovou sirénu JA-60A a případně také další ústředny JA-63 či JA-65 jako podřízený systém. Při montáži a přiřazování jednotlivých detektorů do systému výrobce doporučuje, řídit se dodávaným návodem. Nastavení probíhá ve 36 krocích, jak je uvedeno v instalačním manuálu, pro nás jsou ovšem důležité jen ty, se kterými jsou porovnávána naměřené data, proto je tedy shrnu do následujících kroků:

Nastavení doby poplachu

Dobu poplachu je možno nastavit v rozmezí 1 až 8 nebo 15 minut (případně 10 s. pro testování).

Hlídání rušení rádiového signálu

Ústředna vybavená modulem R je schopna hlídat rušení pracovního pásma systému. Je-li tato funkce zapnuta, rušení delší než 30 s vyhlásí poruchu ústředny (poplach, je-li systém zajištěn). V některých instalacích může být systém opakovaně rušen (blízkou rádiovou stanicí, TV vysílačem, apod.). V takovémto případě nebude možné hlídání rušení použít, úroveň rušení a kvalitu signálu je možné sledovat počítačem s programem ComLink.

Pravidelná kontrola spojení s bezdrátovými detektory

Ústředna vybavená modulem R je schopná pravidelně kontrolovat spojení s přiřazenými bezdrátovými prvky. Pokud zjistí opakovaný výpadek spojení, vyhlásí stav poruchy tohoto prvku (je-li systém zajištěn, reakce závisí na nastavení). V některých instalacích může díky intenzivnímu vnějšímu rušení docházet k opakovaným výpadkům komunikace. Přesto je obvykle systém schopen pracovat jak udává výrobce. Zároveň nedoporučuje v takové situaci pravidelnou kontrolu spojení používat.

Upozornění na závadu periferie při zajištění

Systém průběžně kontroluje stav periferií (detektorů, klávesnic, atd.). Touto volbou je možné nastavit akustické upozorňování (4 rychlá pípnutí) na případnou závadu

při zajištění. Příčinu závady (např. trvale aktivní detektor, otevřený kryt, ztráta spojení, apod.) klávesnice zobrazí. Pokud obsluha nevěnuje této informaci dále pozornost, systém se po uplynutí odchodového zpoždění zajistí a vadný prvek bude vyřazen ze sledování.[15]

4.1.1.3 **Technické parametry ústředny JA-63**

Tab. 2 Technické parametry ústředny JA-63

Napájení ústředny	230 V / 50 Hz, max. 0,1 A, třída ochrany II
Zálohovací akumulátor	12 V, 1,3 nebo 2,6 Ah, systém akumulátor automaticky dobíjí a kontroluje jeho stav, běžná životnost je cca 5 let
Výstup zálohovaného napájení	Max. trvalý odběr 0,4 A, krátkodobě lze odebírat až 1,2 A po dobu max. 15 min.
Klidový odběr ústředny	30 mA, klávesnice JA-60E = 25 mA
Počet bezdrátových zón	16 (max. 32 detektorů, do každé zóny dva)
Počet drátových zón	4, volitelný typ aktivace (dvojité vyvážení, jednoduché vyvážení)
Systémová klávesnice	JA-60E – drátová (max. 4) nebo JA-60F* – bezdrátová (až 8)
Počet bezdrát. ovladačů	Max. 8 (klávesnice JA-60F, JA-60D, klíčenky RC-40, tlačítka RC-22 a ovladače RC-60)
Vstupní poplachové relé	Přepínací kontakt 60 V=1 A
Volitelné výstupy	PgX, PgY max. 0,1 A, spínají na GND, programovatelná funkce
Výstup sirény	Max. Zátěž 0,7 A
Paměť událostí	127 posledních událostí včetně data a času
Pracovní frekvence	433,92 MHz
Vf. výkon	10 mW
Stupeň zabezpečení	2 dle ČSN EN 50131-1, ČSN EN 50131-6
Určeno pro prostředí	II. vnitřní všeobecné (-10 až +40°C) dle ČSN EN 50131-1

[Zdroj: **(15)**]

4.1.1.4 **Výběr bezdrátového detektoru**

Bezdrátový detektor pohybu PIR JA-60P (JABLOTRON ALARMS a.s.)

PIR (Pasivní infračervená čidla) – tyto detektory jsou nejčastěji používanými v prostorové ochraně. Nevyzařují žádnou energii, navzájem se neovlivňují a mohou být nainstalovány tak, že se jejich detekční zóny (aktivní, neaktivní) překrývají. Jsou založeny na principu zachycení změn vyzařování elektromagnetického záření v infračerveném pásmu kmitočtového spektra. Každé těleso, jehož teplota je vyšší než 273 °C (absolutní nula) a nižší než 560 °C, je zdrojem vyzařování vlnění v infrapásmu odpovídajícím teplotě tělesa.[1]

Detektor JA-60P je určen k detekci pohybu člověka v hlídaném prostoru. Vysokou odolnost proti falešným poplachům a účinnou teplotní kompenzaci zajišťuje digitální zpracování signálu. Testování snímače usnadňuje automatický testovací režim. Nežádoucí manipulace s výrobkem nebo snaha o jeho odstranění vede k vyslání sabotážního signálu. Detektor provádí pravidelně autotest a hlásí svůj stav kontrolním přenosem do systému.[16]

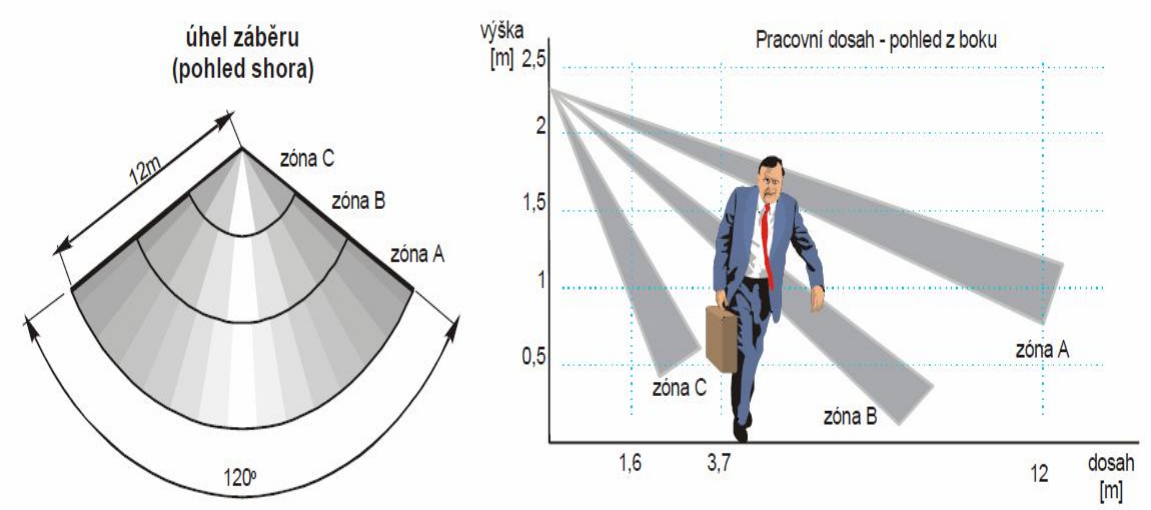
Tab. 3 Technické parametry PIR čidla

Detekční metoda	Duální PIR s digitálním zpracováním
Napájecí napětí	3 V – 2 × alkalická baterie 1,5 V typ AAA
Průměrná doba životnosti	Cca. 1 rok
Doporučená výška pro instalaci	2 až 2,5 m nad úrovní podlahy
Pokrytí prostoru	12 m / 120°(se základní čočkou)
Detekuje pohyby s rychlostí	0,1 m/s až 4 m/s
Doba stabilizace po zapnutí	60 sec.
Pracovní kmitočet	433,92 MHz
Dosah komunikace	Max. 100 m na přímou viditelnost

[Zdroj: **(16)**]

Při návrhu systému je důležité správně zvolit tvar zorného pole. V závislosti na tvaru střeženého prostoru se volí čočka s odpovídajícím zorným polem. Tvar zorného pole je závislý na provedení optiky čidla, dosah čidla je závislý na kvalitě optiky, citlivosti senzoru a způsobu vyhodnocení. Alternativní čočky (dlouhá chodba, zóna pro domácí zvířata, apod.) dodává výrobce samostatně.

Obr. 10 Pokrytí prostoru



[Zdroj: **(16)**]

4.1.1.5 **Testovaná data**

V rámci jednotlivých pokusů se především testovala schopnost reakce ústředny na různé metody narušení přenosu poplachové informace. Porovnávány byly především obě základní metody detekce pokusu o sabotáž – metoda dohledu a metoda detekce zarušení, které jsou charakterizovány výše.

Při každém testu se vždy měřil čas od okamžiku vniku narušení bezdrátové přenosové trasy (rušení pásma) do okamžiku vyhlášení poplachu, čas od okamžiku generování poplachové informace detektorem a jeho pokus o předání rušeným bezdrátovým kanálem do okamžiku vyhlášení poplachu a následně doba od okamžiku ukončení rušení přenosu do vyhlášení poplachu (předání zarušené poplachové informace ústředně).[9]

Ústředna a detektor byly testovány se softwarem ComLink v. 62. Jednotlivé testy se v čase několikráte opakovaly, za účelem vyloučení náhodných vlivů.

4.1.1.6 **Zhodnocení JA-63 „PROFI“**

Všemi realizovanými testy bylo ověřeno, že veškerá naměřená data odpovídají zveřejňované dokumentaci společnosti Jablotron alarms a.s. Detekce zarušení pásma zareaguje do 30 vteřin, tedy funguje, ale při obvyklém nastavení systému (defaultním) je detekce zarušení signálu na ústředně vypnuto. Tato reakce je spolehlivá, dokonce, i když se rušení na krátký interval (řádově sekund) přeruší a následně se rušení opět aktivuje. Částečně funkční je i detekce dohledu bezdrátových detektorů, která ztrátu čidla detekuje po dvou hodinách (poměrně dlouhý interval). Nejkratší časový interval dohledu je 20 min. Pro srozumitelnost a přehlednost jsou výsledky značně zjednodušeny.

4.2 868 MHz

Přenos na této frekvenci je vhodný pro vzdálenosti až několik stovek metrů, to však může mít negativní dopad z hlediska překrytí pásma (např. u sousedů). Jeho vlnová délka je 0,34 m a pracuje s výkony do 7 mW.

Spolehlivost přenosu v pásmu 868 MHz je testována na systému JA-83k „OASIS“ s křížovou kontrolou vzájemné kompatibility (společnosti ©2008 – 2012 JABLOTRON ALARMS a.s.).

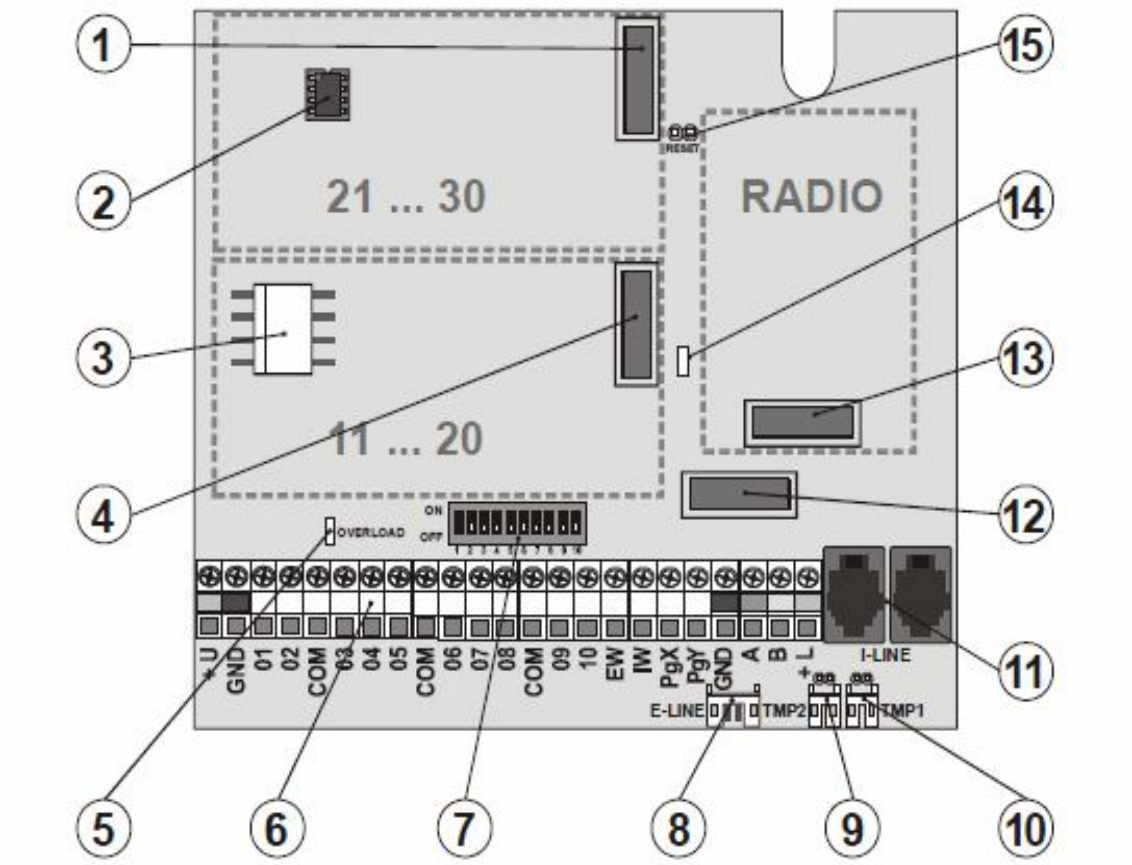
4.2.1 JA-83k „OASIS“

Certifikace systému je stejně jako v předešlém případě dle ČSN EN 50131-1 do stupně 2 (nízká až střední rizika). OASIS umožňuje oproti PROFI řídit přístup (otevírat elektrické zámky, garážová vrata, brány, apod.). Otevření je možné buďto zadáním číselného kódu, přiložením bezdotykového čipu nebo dálkovým ovladačem (např. z auta). Otvírání je přitom logicky spojeno s funkcí střežení.

OASIS vychází koncepčně ze staršího typu systému PROFI. Používá však modernější bezdrátový protokol (prvky mají delší komunikační dosah a nepotřebují viditelné antény), jeho baterie mají delší životnost a celkově má modernější design.

Unikátní jsou v OASISU detektory pohybu se zabudovanou kamerou, které při poplachu posílají fotografie ze střeženého objektu na mobilní telefon či počítač a tak je přesně vidět co se v místě poplachu skutečně děje.

Obr. 11 Základní deska ústředny



Popis: 1. konektor pro JA-82C adresy 21-30; 2. výměnná paměť ústředny; 3. konektor napájení; 4. konektor pro JA-82C adresy 11-20; 5. indikace přetížení +U; 6. svorkovnice; 7. povolení vstupů 01-10; 8.konektor externí sběrnice; 9,10. konektor pro přední a zadní tamper; 11. konektory pro interní sběrnici; 12. konektor pro JA-8xY; 13. konektor pro JA-82R; 14. indikace chodu ústředny; 15. propojka RESET

[Zdroj: **(17)**]

4.2.1.1 **Architektura ústředny**

Ústředna JA-83K je stavebnicový systém, který má 50 adres (označených 01 – 50), na které lze přiřadit až 50 bezdrátových periferií (detektory, klávesnice, ovladače,

sirény atd.). Základem systému je deska ústředny Ja-83K, která má 10 drátových vstupů viz obr. 11. Na tuto desku lze doplnit další rozšiřující moduly:

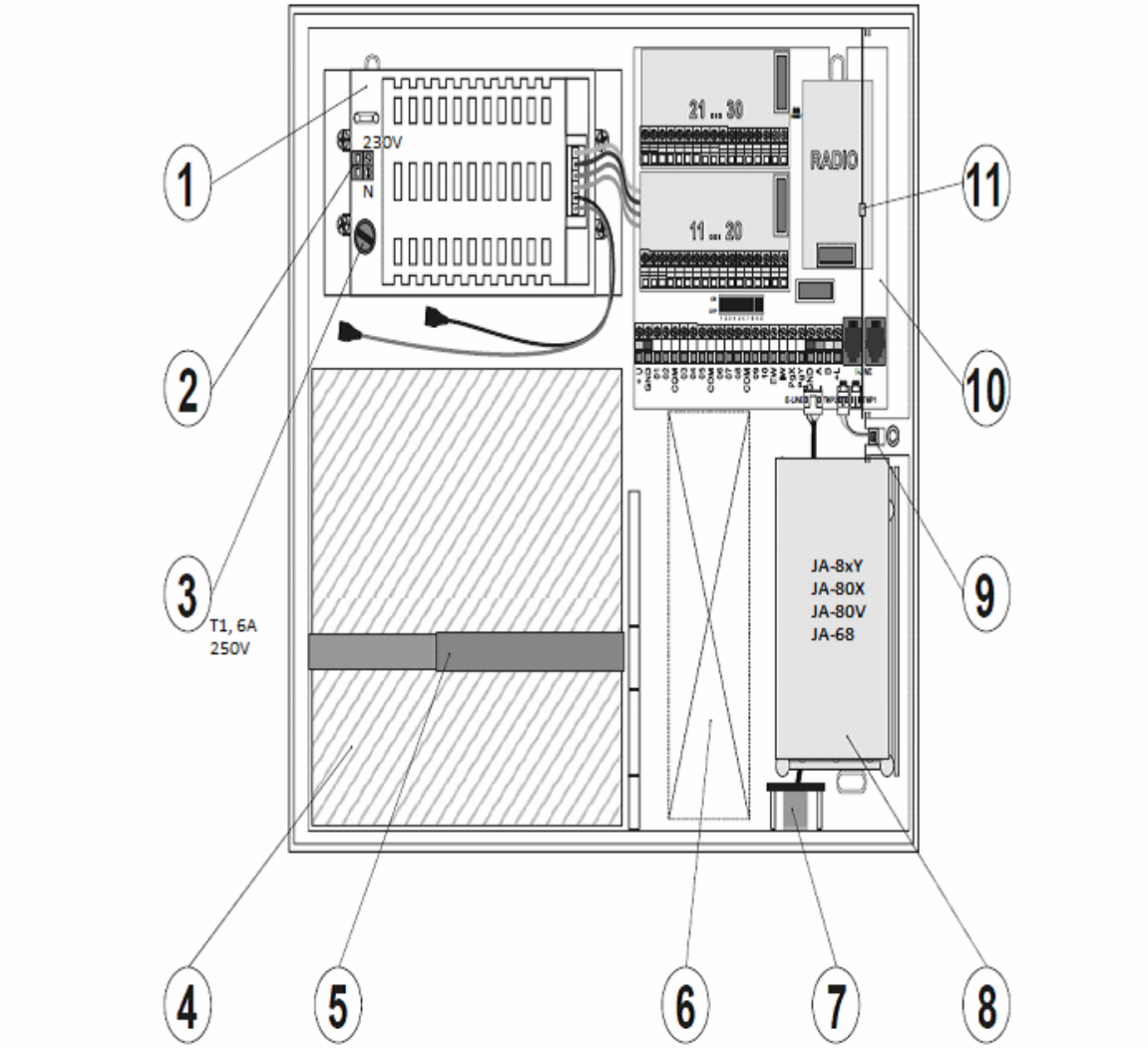
- JA-82R – rádiový modul, pomocí kterého lze do ústředny naučit až 50 bezdrátových periferií řady JA-8x a RC-8x.
- JA-82C – modul 10 drátových vstupů, který rozšíří kapacitu ústředny na 20 resp. 30 drátových vstupů. Lze použít jeden nebo dva moduly.

Jako komunikátor je možné použít:

- JA-8xY – GSM komunikátor, jímž ústředna předává poplachové zprávy uživateli a komunikuje na PCO v pásmu GSM. Umožňuje dálkový přístup z klávesnice telefonu a správu systému z aplikace GSMLink.
- JA-80V – komunikátor pro komunikaci po počítačových sítích LAN (Ethernet) v kombinaci s komunikátorem na pevnou telefonní linku. Umožňuje komunikaci na PCO po LAN a předává zprávy pomocí pevné linky. Stejně tak lze spravovat z aplikace GSMLink.
- JA-80X – komunikátor na pevnou linku, který umí komunikovat na PCO a předat hlasovou zprávu uživateli podle druhu poplachu. Komunikátor JA-80X lze v ústředně kombinovat s JA-80Y – záloha GSM sítě pevnou telefonní linkou.
- JA-80Q – pokud je v systému použit PIR detektor s kamerou.

V ústředně je možné také použít modul výstupů JA-68 – například pro vazbu na objektový vysílač pro komunikaci s dohledovým centrem. Ve skříni ústředny (viz Obr 12) je dále umístěn síťový zdroj a prostor pro akumulátor, který má až 18 Ah.[17]

Obr. 12 Rozmístění ve skříni ústředny



Popis: 1. modul spínaného zdroje; 2. svorkovnice síťového napájení; 3. pojistka síťového napájení; 4. prostor pro záložní akumulátor; 5; pásek zamezující vypadnutí akumulátoru ze skříně; 6. možný průchod pro kabeláž; 7. konektor externí sběrnice (OLink; servisní klávesnice); 8. prostor pro komunikátor nebo modul výstupů; 9. sabotážní kontakt víka skříně; 10. základní deska ústředny (bližší viz obr. 1); 11. anténa pro rádiový modul (je-li osazen)

[Zdroj: **(17)**]

4.2.1.2 **Přiřazení (učení) bezdrátových periferií**

Periferii lze na adresu přiřadit buď naučením, nebo zadáním jejího výrobního čísla v režimu ústředny „servis“. Jako v předešlém případě se při montáži a přiřazování jednotlivých detektorů do systému doporučuje výrobce, řídit se dodávaným návodem. Nastavení probíhá ve 48 krocích, jak je uvedeno v instalačním manuálu. Dále vybírám opět jen ty, se kterými jsou porovnávána naměřené data.

Nastavení doby poplachu

Doba poplachu se odměřuje od jeho vyvolání. Po uplynutí této doby se ukončí signalizace poplachu a systém zůstane ve stejném stavu jako před poplachem. Poplach lze ukončit platným přístupovým kódem nebo kartou.

Hlídání rušení rádiového signálu

Ústředna pro 868 MHz má stejné vlastnosti jako ústředna 433 MHz při hlídání rušení komunikačního pásma jak udává výrobce.

Kontrola spojení s periferiemi

Ústředna pravidelně kontroluje spojení s přiřazenými bezdrátovými periferiemi. A to konkrétně každých 9 minut. Pokud není kontrolní spojení aktivní s detektorem po dobu 2 hodin, je vyhlášena jeho ztráta. V detektorech, které lze použít pro střežení auta (JA-85P, JA-85B) je možné vypnout kontrolu spojení přepínačem v detektoru. Tím je umožněno, aby ústředna kontrolovala spojení s ostatními detektory, a nevyhlašovala ztrátu detektoru v autě, pokud odjedete. Tak jako u 433 MHz v některých instalacích může při častém rušení docházet k příležitostným výpadkům kontrolního spojení. Přesto je obvykle systém schopen fungovat (přenosy důležitých informací jsou několikanásobně opakovány).[17]

Potvrzování poplachu

Snižování rizika falešného poplachu je v systému zabezpečeno logikou potvrzování poplachu (standart BSI DD243). Tato logika funguje následujícím způsobem.

Dojde-li během střežení k aktivaci detektoru (s okamžitou, zpožděnou či následně zpožděnou reakcí), tak se nevyvolá poplach, ale v ústředně se zaznamená tzv. nepotvrzený poplach, poté je-li do 40 minut od vzniku nepotvrzeného poplachu aktivován jiný detektor, vyvolá se poplach. Není-li žádný jiný detektor v uvedené době aktivován, ústředna ukončí čekání na potvrzení. Potvrzení poplachu musí potvrdit jiný detektor než ten, který byl aktivován jako první. Jedná-li se o detektory pohybu, nemají se překrývat jejich zorná pole (nutno zajistit jejich umístěním).[17]

Nepotvrzený poplach ústředna zaznamená do paměti události a může jej reportovat na PCO a nebo formou SMS uživateli v závislosti na nastavení.

Pokud má první aktivovaný detektor nastavenou zpožděnou reakci, začne se odměřovat tzv. nepotvrzené příchodové zpoždění. Je signalizováno stejně jako běžné příchodové zpoždění, ale pokud jej nepotvrdí jiný detektor, nedojde na jeho konci k vyhlášení poplachu. Přetečení časovače se v takovém případě zapisuje jako nepotvrzený poplach. Je-li během nepotvrzeného příchodového zpoždění aktivován jiný zpožděný či následně zpožděný detektor, tak se příchodové zpoždění mění na potvrzené a jeho případné přetečení vyvolá poplach.[17]

Následně je-li do 40 minut od vzniku nepotvrzeného poplachu nebo od přetečení nepotvrzeného příchodového zpoždění aktivován detektor s nastavenou zpožděnou reakcí, začne se odměřovat potvrzené příchodové zpoždění a jeho případné přetečení vyvolá poplach. Je-li nepotvrzené příchodové zpoždění potvrzeno detektorem s okamžitou reakcí, aktivuje se okamžitě interní poplach sirény IW a v případě přetečení časovače se aktivuje i externí poplach sirény EW, aktivaci prvního detektoru může potvrdit kterýkoliv jiný detektor vloupání v systému, jehož sekce je zajištěna (to znamená i detektor z jiné zajištěné sekce). Potvrzování poplachů se týká pouze detektorů vloupání s reakcemi: zpožděná, okamžitá a následně zpožděná. Netýká se ostatních typů reakcí: požár, panik, 24h, sabotáž a technický poplach (jejich vyhlášení je okamžité).[17]

Jednoduše shrnuto, pokud jde o funkci potvrzování poplachu lze o ní říci, že první aktivace detektoru je po vloupání, následně se zahájí pouze čekání na potvrzení (nepotvrzený poplach) dalším detektorem. Během doby čekání, která je 40 minut, se systém chová přesně tak, jako kdyby potvrzování poplachu nebylo vůbec zapnuto. Z výše uvedeného plyne, že při zapnuté logice potvrzování poplachu je nutné v objektu instalovat více detektorů tak, aby při pohybu pachatele pouze v určité části objektu byla splněna podmínka aktivace alespoň dvou samostatných detektorů.

4.2.1.3 **Technické parametry ústředny JA-83K**

Tab. 4 Technické parametry ústředny JA-83K

Napájení ústředny	230 V / 50 Hz, max. 0,1 A, třída ochrany II
Zálohovací akumulátor	12 V, 7 až 18 Ah, maximální doba na dobití akumulátoru je 72 h
Výstup zálohovaného napájení +U	Max. trvalý odběr 1,1 A (při použitém akumulátoru 18 Ah a na dobu zálohy 12 hod)
Výstup zálohovaného napájení +L	Max. trvalý odběr 0,2 A, výstupy napájení +U, +L jištěny elektronicky
Počet adres pro bezdrátové periferie	Až 50 (s modulem JA-82R)
Počet drátových vstupů	10 na základní desce (až 30 s moduly JA-82C) dvojitě vyvážené vstupy rozlišující aktivaci a sabotáž, reakce je nastavitelná
Výstup poplachu EW	Spíná na GND, max. zátěž 0,5 A (externí poplach)
Výstup poplachu IW	Spíná na GND, max. zátěž 0,5 A (interní poplach)
Programovatelné výstupy	PgX, PgY max. 0,1 A, spínají na GND
Paměť událostí	255 posledních událostí včetně data a času
Zpráva o narušení	Po 1. nebo 2. události podle nastavení
Zpráva o sabotáži	Po 1. události
Zpráva o chybných ovládacích kódech	Po 10. chybných zadáních
Signál (zpráva o poruše)	Po 1. události
Pracovní frekvence	Rádiový modul JA-82R - 868 MHz ISM pásmo
Bezpečnost	ČSN EN 60950-1
Stupeň zabezpečení	2 dle ČSN EN 50131-1, ČSN EN 50131-3, ČSN EN 50131-6
Určeno pro prostředí	II. vnitřní všeobecné (-10 až +40°C) dle ČSN EN 50131-1

[Zdroj: **(17)**]

4.2.1.4 **Výběr bezdrátového detektoru**

Bezdrátový detektor pohybu PIR s kamerou JA-84P (JABLOTRON ALARMS a.s.)

Umožňuje detekovat pohyb ve střeženém prostoru včetně vizuálního potvrzení poplachu. Kamera detektoru je vybavena bleskem s infračerveným přisvícením pro focení v noci. Je schopna pořizovat černobílé statické snímky v rozlišení 160×128 bodů. Je-li zaznamenán pohyb, je pořízena sekvence fotografií. Ty jsou uloženy v interní paměti detektoru a bezdrátově přenášeny do ústředny v komprimované podobě, odkud jsou posílány datovým modulem na server (prostřednictvím komunikátoru). Celkový čas k přenesení snímků na server je kolem 20 vteřin, v případě špatného signálu může být přenos delší (ztracená data jsou posílána znovu). Každý snímek obsahuje datum a čas, kdy byl pořízen.[18]

Tab. 5 Technické parametry PIR čidla s kamerou

Napájení	2× lithiová baterie type CR123 (3 V/2,4 Ah)
Typická životnost baterie	Cca. 2 roky (1 poplach měsíčně, zpožděná reakce)
Komunikační pásmo	868 MHz, protokol Oasis
Komunikační dosah	Cca. 300m (přímá viditelnost)
Doporučená instalační výška	2.0 až 2.5 m nad úrovní podlahy
PIR úhel detekce / délka záběru	50°/12 m (se základní čočkou)
Rozlišení kamery	160 × 128 bodů, ČB
Formát snímku vnitřní / přenášený	BMP / JPG
Úhel zorného pole kamery	50°
Dosah blesku	Max. 3 metry
Čas předání snímku ústředně / serveru	25 sec. / 15 s (GPRS – JA-80Y)

[Zdroj: **(18)**]

Normální funkce kamery

Pohyb v okamžité smyčce detektor hlásí ústředně a vyfotí sekvenci 4 snímků. První snímek je pořízen okamžitě bez blesku a následující 3 snímky (každou sekundu) každý s bleskem. Po vyfocení je pohyb před detektorem ignorován a snímky jsou předány na ústřednu. Po přenesení snímků je detektor 5s neaktivní, poté je při detekovaném pohybu opět fotit.

Vestavěný blesk detektoru osvětluje scénu, ale má také další důležité funkce patentované Jablotronem:

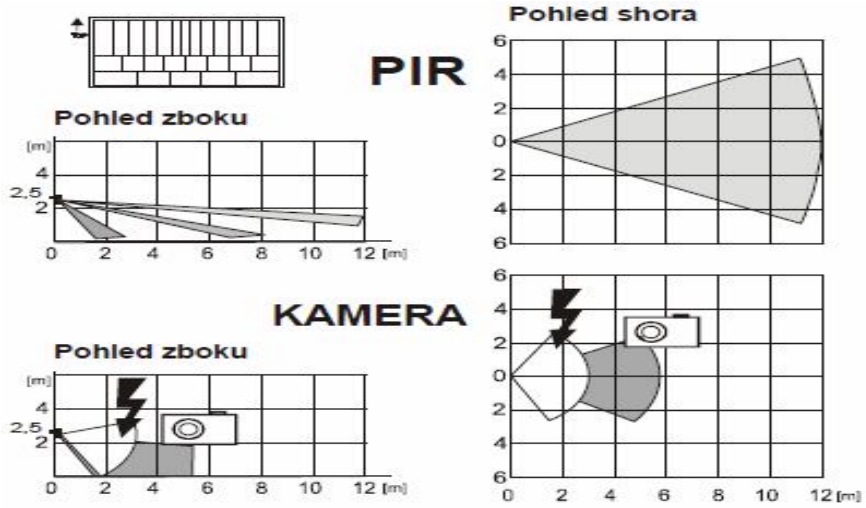
- Neočekávané světlo blesku upoutá pozornost pachatele na detektor a to výrazně zvýší pravděpodobnost, že na dalším snímku bude vidět pachatelova tvář.

- Blesk také jasně dává najevo, že pachatel byl detekován, což jej může přimět k útěku. Pokud ne, pokusí se detektor zničit a vyvolá sabotážní poplach, kterým potvrdí svoji přítomnost daleko rychleji, než jsou přeneseny fotografie.

Detekční charakteristika

Detekční charakteristika čočky PIR nemá žádný vliv na kamerovou část detektoru. Z výroby je detektor osazen základní čočkou se zúženým záběrem 50°/12m.

Obr. 13 Charakteristika pokrytí



[Zdroj: **(18)**]

4.2.1.5 **Testovaná data**

Testování probíhalo na stejném principu jako v případě ústředny pro pásmo 433 MHz v zásadě proto, abychom mohli analyzovat rozdíly mezi těmito pásmy přenosu. Rozdíl byl pouze v použitém softwaru, tedy ústředna a detektor byly testovány se softwarem Olink v. 2.0.2. Stejně tak se testy opakovaly pro vyloučení náhodných vlivů.

4.2.1.6 **Zhodnocení JA-83k „OASIS“**

Všemi realizovanými testy bylo ověřeno, že veškerá naměřená data odpovídají zveřejňované dokumentaci společnosti Jablotron alarms a.s. Detekce zarušení pásma funguje velice spolehlivě, ovšem pouze v místě ústředny. Systém není schopen reagovat na rušení na trase. Výsledky detekce dohledu bezdrátových detektorů jsou shodné s ústřednou pro pásmo 433 MHz. Uvedené poznatky vyplývají z toho, že „Oasis“ vychází koncepčně ze staršího systému „Profi“.

4.3 Další frekvence

Přenosy dat v pásmu ISM je možné realizovat nejen ve volných pásmech, jako jsou 433 MHz a 868 MHz. Další kmitočtová pásma jsou uvedena v následující tabulce. Podmínky pro provoz datových a jiných zařízení ve volných pásmech jsou pro tuzemské prostředí stanoveny generálními licencemi (dříve generální povolení), které vydal Český telekomunikační úřad číslem GL-12/R/2000, případně GL-30/R/2000.

Tab. 6 Kmitočtová pásma rádiových vln

Kmitočet	Délka vlny	Název pásma	Symboly	Český název
3 – 30 kHz	100 – 10 km	myriametrické	VLF	velmi dlouhé
30 – 300 kHz	10 – 1 km	kilometrické	LF	dlouhé
300 – 3000 kHz	1000 – 100 m	hektometrické	MF	střední
3 – 30 MHz	100 – 10 m	dekametrické	HF	krátké
30 – 300 MHz	10 – 1 m	metrické	VHF	velmi krátké
300 – 3000 MHz	10 – 1 dm	decimetrické	UHF	ultra krátké
3 – 30 GHz	10 – 1 cm	centimetrické	SHF	centimetrové
30 – 300 GHz	10 – 1 mm	milimetrické	EHF	milimetrové
300 – 3000 GHz	1 – 0,1 mm	decimetrické	-	-

[Zdroj: **(7)**]

5 NÁVRH ALTERNATIVNÍ VARIANTY

Možnou alternativou budoucnosti bezdrátového přenosu dat v rámci EZS, by se mohla stát komunikační technologie „ZigBee“, která má velmi dobré předpoklady, pro splnění náročných požadavků zabezpečovacích systémů. ZigBee patří do skupiny bezdrátových sítí PAN (Personal Area Networks dále jen „PAN“). Do této skupiny patří také známý „Bluetooth“. Z důvodů, že Bluetooth není možné použít u spousty průmyslových aplikací. Byl založen komunikační standard ZigBee vhodný i pro účely průmyslové automatizace. Hlavními přednostmi ZigBee jsou spolehlivost, jednoduchá a nenáročná implementace, velmi nízká spotřeba energie a také příznivá cena.

5.1 ZigBee

ZigBee je bezdrátová komunikační technologie vystavěná na standardu IEEE 802.15.4. ZigBee je poměrně novým standardem platným od listopadu roku 2004. Podobně jako bluetooth je určena pro spojení nízko výkonových zařízení v sítích PAN (Personal Area Networks) na malé vzdálenosti do 75 metrů. Díky použití multiskokového ad-hoc směrování umožňuje komunikaci i na větší vzdálenosti bez přímé rádiové viditelnosti jednotlivých zařízení. ZigBee je navržen jako jednoduchá a flexibilní technologie pro tvorbu i rozsáhlejších bezdrátových sítí, u nichž není požadován přenos velkého objemu dat. Pracuje v bezlicenčních pásmech přibližně 868 MHz, 902 - 928 MHz a 2,4 GHz, přenosové rychlosti se pohybují okolo 20, 40, 250 kbit/s.[19]

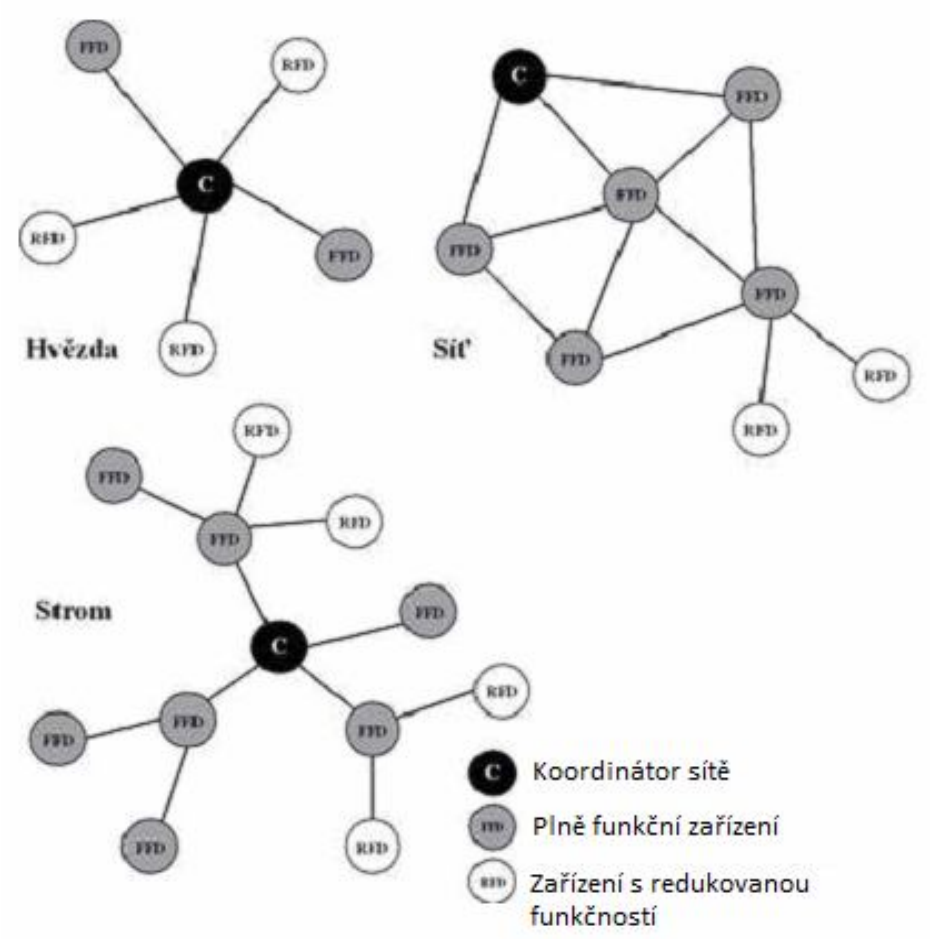
Tento standard definuje tři základní režimy přenosu dat:

- Periodicky se opakující (přenos dat z detektorů).
- Nepravidelné přenosy (externí události, např. stisknutí tlačítka uživatelem).
- Opakující se přenosy, u nichž je požadavek na malé zpoždění (bezdrátové počítačové periferie – klávesnice a myši).

5.1.1 Topologie sítě

Topologie ZigBee je postavená na fyzické linkové vrstvě IEEE 802.15.4 a definuje tři různé síťové topologie. Základní je topologie hvězdicová s centrálním řídícím uzlem (koordinátorem sítě). Druhým typem je stromová struktura, jež umožňuje zvětšit vzdálenost mezi koordinátorem a koncovým zařízením. Protokol též umí vytvořit redundantní spojení a vzniká tak topologie typu MESH, s jejíž pomocí je pak možné vytvořit prakticky libovolné uspořádání sítě. Topologie sítí je přiblížena v navazujícím obrázku.[19]

Obr. 14 Topologie sítí ZigBee



[Zdroj: **(19)**]

Standard ZigBee dělí zařízení (viz. Obr 14) na zařízení FFD (Full Functional Device dále jen „FFD“) a RFD (Reduced Functionality Device dále jen jako „RFD“). FFD zařízení implementují kompletní protokolový rámec a zajišťují veškeré služby,

které standard ZigBee stanovuje. RFD zařízení implementují pouze nezbytné protokolové knihovny z důvodu maximálního omezení hardwarové náročnosti. Tato zařízení mohou pracovat pouze jako koncová. Mohou komunikovat pouze s koordinátorem sítě a jsou omezeny na hvězdicové uspořádání topologie (koncové větve). Koordinátor sítě a směrovače jsou realizovány FFD zařízeními.[19]

5.1.2 Zabezpečení sítě

Základním zabezpečením ZigBee je AES (Advanced Encryption Standart dále jen „AES“) s klíčem o délce 128 bitů, jež je implementován v síťové vrstvě. Síťová vrstva je zabezpečena SSP (Security Services Provider dále jen jako „SSP“). Touto vrstvou je zajištěno zabezpečení odchozích rámců, dekódování a ověřování pravosti příchozích rámců. Zabezpečovacím algoritmem je AES v mírně modifikovaném módu označeným jako CCM. Síťová vrstva je odpovědná za realizaci zabezpečení. Vyšší vrstvy mají na starost o nastavení SSP (nastavení klíčů a způsob použití CCM pro jednotlivé rámce).[19]

5.1.3 Souhrn poznatků

Závěrem lze o ZigBee říci, že není prozatím použito v elektronických zabezpečovacích systémech, z důvodů nesplňujících níže uvedených požadavků.

- Normalizované definice přenosových tras
- Relativně nízká vzdálenost dosahu
- Nutnost změny topologie sítě

Nízká vzdálenost dosahu by byla ovšem vyřešena přenosem informace z jednoho detektoru na druhý, tzn. že každý detektor by byl zároveň přijímačem i vysílačem přihlašovací i sabotážní informace, aniž by byla ovlivněna výdrž baterie jednotlivých detektorů, na kterou je kladen veliký důraz z hlediska zabezpečovací normy. To proto, že ZigBee disponuje velmi nízkým objemem struktury přenosových protokolů, která nezabere více než 30 kB programové paměti.

6 SHRNUTÍ A ZHODNOCENÍ

Shrnutí bych rozdělil do dvou zásadních kroků, kdy nejprve porovnám a zhodnotím systémy společnosti JABLOTRON ALARMS a.s., dále pak shrnu základní rozdíly mezi oběma pásmy přenosu.

6.1 Porovnání a zhodnocení rozdílů mezi systémy Oasis a Profi

Tab. 7 Porovnání Oasis a Profi

VLASTNOST	OASIS	PROFI
Počet použitelných prvků	50	32+8
Počet uživatelských kódů	50	14
Kamerové detektory pro přenos snímku z objektu	+	-
Komunikační obsah	+	-
Životnost baterií	+	-
Dostupnost a cena baterií	-	+
Vzhled prvků	+	-
Schopnost eliminovat falešné poplachy	+	-
Služba střežení pultem na půl roku zdarma	+	-
Ovládání pomocí bezdotykových čipů a karet	+	-
Funkce pro řízení přístupu (el. Zámky, garážová vrata)	+	-
Funkce garážových vrat (prodlužování odchodu)	+	-
Dálkový ovladač pro ovládání z auta	+	-
Funkce pro řízení teploty v domě	+	-
Intuitivnost konfigurace a ovládání	+	-
Pořizovací cena systému	-	+
- je ve srovnání horší, + je ve srovnání lepší		

[Zdroj: **(20)**]

Tabulka ukazuje, že modernější systém „Oasis“ má mnohem rozsáhlejší možnosti, a tak je pro náročného uživatele vhodnou volbou. Bohužel tato rozsáhlá působnost má za následek vysokou pořizovací cenu. Naproti tomu „Profi“ také dokáže uspokojit i ty náročné, avšak z rozdílu nižších nákladů na pořízení, které určitě ocení uživatelé s nižšími finančními možnostmi. Důležité je říci, že z provedených měření oba systémy vyhovují bezpečnostním normám. A v zásadě se i shodují s výrobcem udávanými vlastnostmi obou systémů.

6.2 Porovnání a zhodnocení pásem 433 MHz a 868 MHz

Výchozí pro porovnání bylo měření dvěma základními metodami detekce pokusu o sabotáž, jak je uvedeno pro každé pásmo – metoda dohledu a metoda detekce zarušení, ovšem pro přiblížení rozdílů mezi pásmy bych rád uvedl ještě další testy, které byly již provedeny dříve na základě posuzování obou frekvenčních pásem.

- Jednoduché testy provedené společností EUROSAT demonstrují vliv frekvence na dosažitelné vzdálenosti u typických detektorů:

Tab. 8 Dosažitelné vzdálenosti detektorů

Vzdálenost	868 Mhz		433 Mhz	
m	MG – PMD186P	MG – PMD758	MG – PMD1P	MG – PMD75
8	10	10	7	7
25	7	7	6	7
35	6	7	4	7
45	4	4	2	4
55	3	1	2	3

[Zdroj: **(5)**]

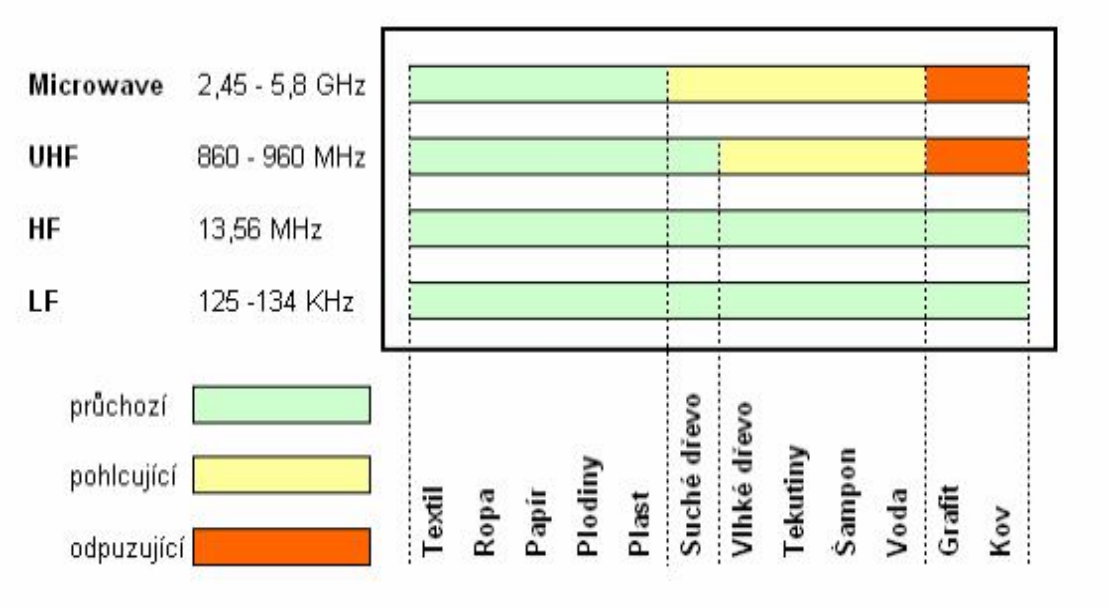
Z výsledků je zřejmé, že rozdíly nejsou příliš velké. Nicméně je zvláštní, že 433 MHz má o trochu lepší intenzitu signálu na delší vzdálenost a 868 MHz naopak. Správná funkce detektoru je zajištěna do intenzity signálu 3.

Výkonnost systémů může být nepříznivě ovlivněna kapalinami nebo mokrým povrchem. HF signály, vzhledem k jejich relativně dlouhé vlnové délce, jsou mnohem

lépe proniknout do vody, než UHF a MW signály. Signály vysokých frekvencí mají tedy větší šanci být absorbovány v kapalině. Rovněž kov je elektromagnetický reflektor, kterým rádiové signály nemohou proniknout. V důsledku toho kovy nejen brání komunikaci, nacházejí-li se mezi detektorem a ústřednou, ale i samotná přítomnost kovu může mít negativní vliv na funkci systému (dochází k nežádoucím odrazům a tím i k vzniku stojatého vlnění).[5]

- V dalším testu je přesně vidět jak jsou frekvenční pásma ovlivněna kovy a jinými materiály.

Graf. 1 Ovlivnění frekvenčních pásem



[Zdroj: **(5)**]

Z grafu je patrné, že vysoká frekvenční pásma jsou kovy ovlivněna daleko více než pásma na nižších frekvencích.

Shrneme-li veškeré poznatky, můžeme říci, že není jednotné stanovisko výběru systému o frekvenci 868 MHz nebo 433 MHz. Z čehož plyne závěr, že 868 MHz lze doporučit v podstatě tam, kde má zákazník problémy se systémem 433 MHz. Důvodů je mnoho – př. Rušení jiným bezdrátovým zařízením. Výhoda pásma 868 MHz oproti pásmu 433 MHz je v poloviční délce vlnové délky pásma (poloviční anténa), což má efektivní vliv na velikost výsledného zařízení – je menší. Vzhledem k obsazenosti je pásmo 868 MHz méně využívané než 433 MHz. Na druhou stranu u 433 MHz ovšem

používané RF moduly (samostatně fungující moduly, po připojení antény na modul je pak možné vysílat data) dosahují většího maximálního výstupního výkonu.

Testování spolehlivosti bylo realizované na základě platných norem, především normy 50 131. Vzhledem k tomu, že se jedná o bakalářskou práci, převzal jsem podstatnou část výsledků měření, dle závěrečné zprávy projektu 31170/1312/3135 autorů Votruba Z., Hart J., Kotek T. Následně jsem provedl vlastní kontrolní měření potvrzující předchozí uváděné výsledky, proto je samostatně nediskutuji a nadále uvádím souhrnné výsledky získané, jak z uvedeného zdroje, tak i z vlastního měření. Podrobnější měření a zpracování předpokládám v navazující diplomové práci.

Celkové výsledky měřených parametrů lze shrnout v níže uvedené tabulce.

Tab. 9 Celkové výsledky měření

Frekvence 433 MHz		
Systém	Software	Problém
JA-63 „PROFI“ Zab.: Třída II	ComLink v. 62	• Detekce zarušení signálu – funguje – při obvyklém nastavení ústředny je tato funkce vypnuta. • Dohled bezdrátu – splňuje požadavky normy zabezpečení – nejkratší časový interval je 20 min.
Frekvence 868 MHz		
Systém	Software	Problém
JA-83K „OASIS“ Zab.: Třída II	Olink v. 2.0.2.	• Detekce zarušení signálu – funguje velice spolehlivě, pouze však v místě ústředny, systém není schopen reagovat na rušení v přenosové trase. • Dohled bezdrátu – stejně jako v předchozím případě splňuje požadavky a nejkratší časový interval je 20 min.

[Zdroj: **(9)**]

7 ZÁVĚR A FINANČNÍ ZHODNOCENÍ

Cílem práce bylo analyzovat schopnost systémů EZS reagovat na různé způsoby zarušení a napadení (sabotáže) přenosového pásma, konkrétně pro bezdrátové systémy společnosti JABLOTRON ALARMS a.s. smyčkový hybridní systém „PROFI“ v přenosových pásmech 433 MHz a hybridní systém s křížovou kontrolou vzájemné kompatibility „OASIS“ pro pásma 868 MHz. Testování se provádělo s ohledem na bezpečnostní třídy ústředen a detektorů, na příslušných verzích softwarů dodávaných k testovaným systémům.

Vlastní měření jsem prováděl dle obou základních měřících principů pro narušení přenosového pásma. První metodou je „Dohled bezdrátového detektoru“, kdy se detektor po určité době pravidelně přihlašuje ústředně. Což znamená, že po nastavenou dobu detektor vysílá klidovou informaci ústředně a tím prokazuje svojí přítomnost v systému. Tato metoda je dost účinná při krátkých intervalech, ovšem nastavení intervalu přihlášení v krátkém čase má za následek rychlejší vybíjení baterie detektoru. Proto se v praxi nastavují od několika minut, až po několik hodin. A zde se objevuje další problém, protože i několik minut stačí člověku k napáchání škody v objektu a ústředna ho nemusí, ani zaregistrovat. Druhá metoda je založena na principu detekce intenzity okolního vysílání v daném pásmu, a pokud je po určitou dobu tato intenzita souvisle vyšší než určená mez, vyhlásí systém poplach typu zarušení pásma. Metoda „Zarušení pásma“ jak ji nazýváme, umožňuje výrazně rychleji odhalit možný pokus o zarušení pásma.

Měření probíhalo za použití frekvenční rušičky, kdy se rušil přenos dat, jak v místě ústředny, tak u detektoru a na konec v trase mezi detektorem a ústřednou. Při testech se pokaždé měřil čas, od vniku narušení přenosové trasy, až do vyhlášení poplachu. Dále čas od okamžiku generování poplachové informace detektorem a jeho snahu o předání informace rušeným bezdrátovým kanálem, do vyhlášení poplachu a nakonec čas od ukončení rušení přenosu dat, do vyhlášení poplachu. Každý test se několikráte opakoval, aby bylo vyloučeno ovlivnění výsledků náhodnými vlivy. Oba systémy prošly testy z hlediska zabezpečovacích norem a pro danou třídu zabezpečení s uspokojivými výsledky (viz. Tab. 9), které také odpovídají publikované dokumentaci výrobce.

Je tedy vidět, že bezdrátová technologie má své klady i zápory, nicméně velmi dobrou variantou je kombinace s drátovým systémem, která vykazuje velmi spolehlivou funkci a do vysoké míry plní požadavky majitele. Zároveň mírní náklady na pořízení, z hlediska levnějších drátových detektorů. Prostě řečeno pokud je to možné, je doporučováno, aby zákazník zvolil z počátku drátový systém, který je později možno zkombinovat s bezdrátovým, bez narušení stavebních částí objektu.

Závěrem bych rád dodal, že testované systémy jsou na trhu EZS špičkou v bezdrátových systémech a budoucím zákazníkům bych je doporučil. Při volbě systému s nižšími náklady, doporučují systém „PROFI“ (viz. Tab. 10). Do budoucna bych se chtěl zaměřit na testování systémů jiných výrobců například firma VARIANT plus, spol. s.r.o. a zjištěné výsledky a porovnání uvézt v případné diplomové práci.

Nakonec pro porovnání, do následující tabulky uvedu finanční zhodnocení používaných systémů.

Tab. 10 Finanční zhodnocení

Prvky zabezpečení	Částka [Kč včetně DPH]
Sada JA-63 „PROFI“ + moduly	14 098
Sada JA-83K „ OASIS“ + moduly	20 412
PIR 433 MHZ JA-60P	1 374
PIR 868 MHZ JA-84P	3 215
Celkem	39 099

[Zdroj: **(21)**]

Zároveň je nutné uvažovat v systému zabezpečení další detektory, které jsou nutné pro kompletní zabezpečení objektu, z čehož plyne, že cena systému ještě stoupne. Zde jsou použity jen ty detektory, pomocí kterých bylo prováděno měření, a tak je cena bezdrátového zabezpečovacího systému neúplná. Avšak sady zabezpečovacích ústředen jsou v těchto verzích kompletní.

POUŽITÁ LITERATURA

[1] Křeček, S., a kol.: Příručka zabezpečovací techniky, Blatná, Blatenská tiskárna 2003, 351 s, ISBN 80-7251-189-0.

[2] Loveček, T., Nagy, P.: Kamerové bezpečnostní systémy, Žilina, EDIS 2008, 283 s, ISBN 978-80-8070-893-1.

[3] Uhlář, J.: Technická ochrana objektů, I.díl, Mechanické zábranné systémy II, Praha, PA ČR, 2004, 179 s, ISBN 80-7251-172-6.

[4] Uhlář, J.: Technická ochrana objektů, II.díl, Elektrické zabezpečovací systémy II, Praha, HIO PA ČR, 2005, 229 s, ISBN 80-7251-189-0.

[5] SECURITY MAGAZIN: č. leden/únor, 2008, ISSN 1210-8723.

[6] přednášky TF ČZU – Elektronické instalace budov III (TGT46E): přednáška č. 2 Systémy EZS (elektronické zabezpečovací systémy), EPS (protipožární systémy), CCTV (CCD kamerové systémy + IP kamery).

[7] přednášky TF ČZU – Elektronické instalace budov III (TGT46E): přednáška č. 5 Bezdrátová komunikace.

[8] přednášky TF ČZU – Elektronické instalace budov III (TGT46E): přednáška č. 7 signalizace komunikace 2.

[9] Závěrečná zpráva projektu 31170/1312/3135

INTERNET

[10] http://www.systemy-stech.cz/EZS [cit 2012-02-28]

[11] http://micro.feld.cvut.cz/home/X34EZS/prednasky/04%20Ustredny%20EZS.pdf [cit 2012-03-10]

[12] http://amapro.cz/public/tele/jts_1.php [cit 2012-02-28]

[13] http://europatron.cz/cs/bezpecnostni-sluzby/technologie-pro-prenos-signalu [cit 2012-02-28]

[14] http://radio2.iglu.cz/gsm.html [cit 2012-02-28]

[15] http://jablotron.cz/upload/download/mgk55401-cz1213608075845864945.pdf [cit 2012-03-19]

[16] http://www.jablotron.cz/upload/download/mdr52402.pdf [cit 2012 -03-19]

[17] http://www.jablotron.cz/upload/download/JA-83K_CZ_MKG51001.pdf [cit 2012-03-19]

[18] http://www.jablotron.cz/upload/download/JA-84P_CZ_MHP56004.pdf [cit 2012-03-26]

[19] http://cs.wikipedia.org/wiki/ZigBee [cit 2012-03-30]

[20] http://zabezpeceni-objektu.jablotron.cz/cz/sekce/vyrobky/oasisnew/ [cit 2012-03-30]

[21] http://www.jablotron.cz/upload/download/jablotron_ezs_cenik_12_02.pdf [cit 2012-03-30]

SEZNAM OBRÁZKŮ A TABULEK

Seznam obrázků

Seznam tabulek

SEZNAM POUŽITÝCH ZKRATEK

ACS/ID – Identifikační systémy

AES – Advanced encryption standart (symetrická blokovací šifra)

BTS – Base transceiver station (vysílač/přijímač rádiových signálů)

CCTV – Closed circuit television (uzavřený televizní okruh)

CCM – Modifikovaný mód šifrování AES

CENELEC – Evropský výbor pro normalizaci v elektrotechnice

ČTÚ – Český telekomunikační úřad

DIP – SWITCH – ruční elektrické spínače

EHF – Extremely high frequency

EW – Externí siréna (Jablotron)

EZS – Elektronické zabezpečovací systémy

FFD – Full functional device

FTP – File transfer protocol

GND – Ground

GPRS – General packet radio service

GSM – Globální systém pro mobilní komunikaci

HF – High frequency

HTTP – Hypertext transfer protocol

IP – Internetový protokol

ISDN – Integrated services digital network

ISM – Volná pásma pro radiové vysílání

IW – Interní siréna (Jablotron)

JTS – Jednotné telefonní sítě

LAN – Local area network

LF – Low frequency

MAC – Media access control

MF – Medium frequency

PAN – Personal area network

PCO – Pult centralizované ochrany

PIR – Pasivní infračervený senzor

PZTS – Poplachové zabezpečovací a tísňové systémy

RFD – Reduced functionality device

SHF – Super high frequency

SMS – Short message service

SSP – Poskytovatel bezpečnostní služby

SW – Software

TCP/IP – Rodina protokolů pro komunikaci v počítačové síti

TELNET – Telecommunication network

TNK – Odborné poradné orgány

UHF – Ultra high frequency

ÚNMZ – Úřad pro technickou normalizaci, metrologii a státní zkušebnictví

VHF – Very high frequency

VLF – Very low frequency

WAN – Wide area network