Systémy přenosu dat ze zabezpečovacích zařízení kancelářských objektů

Systems transfer data from security device for office buildings

Ivo Čermák

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:	**Ivo ČERMÁK**
Osobní číslo:	**A08153**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Systémy přenosů dat ze zabezpečovacích zařízení kancelářských objektů**

Zásady pro vypracování:

1. **Zpracujte literární rešerši o způsobech řešení a nabídce technických prostředků pro řešenou oblast.**
2. **Sestavte seznam základních požadavků na zabezpečovací zařízení specifických kancelářských objektů.**
3. **Vypracujte vzorovou studii dvou příkladných řešení.**
4. **Zpracujte projektový záměr pro systémy přenosů dat zabezpečovacích zařízení specifických kancelářských objektů.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Křeček, S a kol.: Příručka zabezpečovací techniky / Stanislav Křeček a kolektiv. - Vyd. 2. Cricetus, 2003. - 351 s.; ISBN 80-902938-2-4**
2. **Krejčiřík A.: Střežení a ovládání objektů pomocí mobilu a SMS : GSM pagery a alarmy : princip, použití, návody, příklady / Alexandr Krejčiřík. - 1. vyd.. - Praha : BEN - technická literatura, 2004. - 303 s. : il., ISBN 80-7300-082-2 ISBN 978-80-7366-128-1**
3. **Neil Comming. Security: A Guide to Security System Design and Equipment Selection and Installation, Second Edition. ISBN-10: 0750696249**
4. **Hermann Merz, Thomas Hansemann, Christof Hübner , Automatizované systémy budov : sdělovací systémy KNX/EIB, LON a BACnet /. - 1. vyd. - Praha : Grada, 2008. - 261 s. : il. - (Stavitel), ISBN 978-80-247-2367-9**
5. **Schneider Electric CZ, I/NET Seven zabezpečovací a přístupový systém . Praha : Schneider Electric CZ, 2005**
6. **Hermann Merz, Thomas Hansemann, Christof Hübner , Automatizované systémy budov : sdělovací systémy KNX/EIB, LON a BACnet /. - 1. vyd. - Praha : Grada, 2008. - 261 s. : il. - (Stavitel), ISBN 978-80-247-2367-9**

Vedoucí bakalářské práce: **doc. Ing. František Hruška, Ph.D.**
Ústav elektroniky a měření

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **8. června 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Vladimír Vašek, CSc.
v z. *ředitel ústavu*

ABSTRAKT

Cílem této práce je pohled na zabezpečení kancelářských objektů a řešení zabezpečovacích zařízení. Ukazuje dostupné komunikační prostředky přenosu dat v budovách a informuje o možných vzniklých stavech, jako jsou poplachové a havarijní hlášení.

Klíčová slova: přenos dat, sítě, zabezpečení, sběrnice, FireWire, USB, Bluetooth

ABSTRACT

The aim of this work is to look at the security office objects solutions and security systems. Shows the available means of communication data in illegal status and inform the possible resulting states such as alarm and emergency messages.

Keywords: transfer data, network, security, bus, KNX/EIB

Poděkování, motto

Chtěl bych poděkovat vedoucímu mé práce doc. Ing. Františku Hruškovi, Ph.D. za odbornou pomoc, cenné rady a čas, který mi věnoval. Dále bych rád poděkoval mé ženě Báře, synu Jakubovi, rodině a známým za podporu a trpělivost, kterou se mnou měli při mém studiu a vzniku této 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

Cílem je seznámení s problematikou přenosu dat, požadavky a možnostmi, které nabízejí. Dnes je na trhu řada sběrnic, které nám přenos umožňují (Seriál 232, 485, USB, FireWire). Podle parametrů, např. přenosový výkon, délka vodičů, počet účastníků mají různý význam a využití konkrétních aplikací. U sběrnic jde hlavně přenést malý objem dat v co nejkratším čase (v μs, ms).

Existuje více způsobů jak zajistit přenos dat. V dnešní době se využívá především přenosu v různých kabelech, ať už metalických nebo optických, nebo bezdrátového přenosu. Kde se nepřenáší velké množství (data ze čtecích a snímací zařízení) dat bohatě postačí koaxiální kabel nebo kroucená dvojlinka, které mají dostatečnou kapacitu i rychlost pro přenos a nejsou tak nákladné. V případě přenosu velkých objemů dat (kamery) je lepší využít pro přenos optických vláken nebo sběrnice IEEE 1394. Bezdrátový přenos se využívá spíše v prostranství a budovách, kde není možné jinak přenos dat uskutečnit. Proti zneužití dat se dat často šifrují.

I. TEORETICKÁ ČÁST

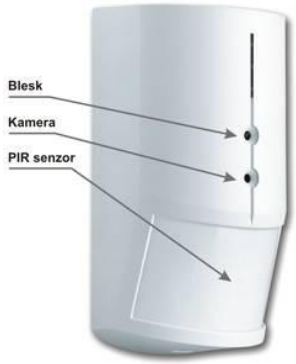
1 LITERÁRNÍ REŠERŽE O ZPŮSOBECH ŘEŠENÍ A NABÍDCE TECHNICKÝCH PROSTŘEDKŮ PRO DANOU OBLAST

1.1 Komplexní řešení zabezpečení proti narušení

U velmi důležitých objektů je vhodná integrace více způsobů zabezpečení a ochrany osob a majetku do jednoho uceleného celku, splňujícího i nejnáročnější požadavky. Do komplexního zabezpečení patří:

Poplachové zabezpečovací a tísňové systémy

Poplachový zabezpečovací a tísňový systém (PZTS), dříve nazývaný elektrická zabezpečovací signalizace (EZS), je souhrnem technických prostředků, které řeší ochranu objektů proti neoprávněnému vstupu nepovolaných osob, a to formou detekce a indikace přítomnosti, vniknutí nebo pokus o vniknutí do střeženého prostoru, popř. poskytuje uživateli možnost úmyslného vyvolání poplachového stavu. V dnešní době, charakteristické stoupající kriminalitou, je potřeba chránit sebe i majetek vyšší než byla v minulosti. Policejní statistiky dlouhodobě uvádějí objasněnost případů vloupání kolem 20%. Svůj podíl na objasněnosti a hlavně samotném uskutečnění vloupání má i fakt, že PZTS je i přes finanční dostupnost stále málo využívaným způsobem zabezpečení. PTZS zvýší bezpečí objektu a poskytuje významnou ochranu před ztrátou majetku, financí a důležitých dokumentů. V případě instalovaného a certifikovaného systému PZTS poskytuje většina pojišťoven příznivější podmínky. Zákazník si může vybrat mezi metalickou i bezdrátovou variantou, která je šetrná k interiérům i při osazování chráněných objektů. PTZS může střežit volný prostor před objektem, plášť domu (okna, dveře) a v neposlední řadě i samotné vnitřní prostory. Používají se prostorová čidla pracující na různých principech, dveřní a okenní snímače a další prvky. Na narušení střežených prostor je možné zaslat na pult centralizované ochrany. Poplachem systém reaguje i na pokus o zničení kteréhokoliv čidla nebo narušení prostoru silným elektromagnetickým zářením (obr. 1-1).(9)



Obr. 1-1 Pohybový senzor

Perimetrické zabezpečení

Velmi účinný a stále častější způsob střežení vybraných prostor je tzv. perimetrická ochrana objektu. Perimetrie je venkovní obvodová hranice (areálu, budovy, pozemku). Systém perimetrického zabezpečení může být řešen za využití kombinace elektronických a mechanických systémů a slouží k zaznamenání případného narušitele ještě dříve, než se prostorem areálu přiblíží ke střeženým objektům. Základní perimetrická ochrana bývá tvořena oplocením a detekce pohybu (pohybové senzory, mikrovlnné bariéry, zemní detekční kabel, termovize…)(9)

Kamerový systém CCTV

Uzavřený televizní okruh (Closed Circuit TV – CCTV) je systém, který umožňuje sledování dění v zájmových zónách střeženého prostoru pomocí instalovaných kamer a dohledového centra. Lze je používat samostatně pro monitorování veřejných prostranství, budov nebo jiných prostorů. Využívá se s dalšími systémy jako komplexní celek. Podle individuálních požadavků se společně se systémy elektronického zabezpečení (EZS), s identifikačními a docházkovými systémy, s perimetrickým zabezpečením a dalšími systémy. Všechny uvedené systémy jsou přeneseny do jednoho řídícího pracoviště – velína. U přístěn střežených objektů se instalují kamery s detekcí pohybu. (9)

Elektronický identifikační systém kontroly vstupu (EKV)

Přístup do objektu je umožněn pouze oprávněným uživatelům. Pro ovládání vstupních bran, vrat, dveří nebo turniketů se používá různých identifikačních médií a čipových karet, číselných klávesnic ale i smart karty atd. Bránu lze ovládat i dálkově z dohlížecího centra –

návštěvník se ohlásí komunikačním systému (interkomem) ubrány nebo vjezdu, po ověření kamerou může být obsluhou vpuštěn do objektu. (9)

1.2 Směry vývoje

Dnes se klade stále větší důraz na uživatelský komfort, snadnou obsluhu. Mezi požadavky patří:

- snadné a jednoduché ovládání a obsluha, přehled o všech funkcí, dostupný z více míst
- možnost specifických úprav přímo samotnými uživateli
- návaznost na systémovou techniku v budovách, multimédia, internet a telekomunikace.

1.2.1 Dotykové displeje

Displeje orientované na design a snadnou obsluhu, tzv. dotykové displeje nabízí požadovanou funkcionalitu spojenou s větším uživatelským komfortem a širší využitelností. Dotykový displej nabízí následující výběr možností:

- K dispozici jsou stovky spínacích a řídících funkcí.
- Jednotlivé stránky se mohou libovolně vzájemně spojovat a volitelně nastavit.
- Na displeji můžou být ikony nebo rovnou velké ovládací tlačítka, které je možno ovládat dotykem tužky nebo konečky prstů.
- V nabídce možností zobrazení můžou být různé struktury konstrukce domů nebo funkcí skupiny.
- Integrací stránek médií a spojení s přídavnými zařízeními se zabezpečuje možnost ovládat systémy přímo z jednoho místa.

1.2.2 Integrace do systémové techniky budov

Uvnitř mnoha budov se společně se sítí KNX/EIB nacházejí ještě i lokální sítě s internetovým spojením. Oba systémy lze dnes spojit a využít síťovou strukturu pro rychlý přenos dat mezi jednotlivými oblastmi. Spojení KNX/EIB s LAN se provádí rozhraním IP

(IP-Gateway). Je to spojovací člen mezi sítěmi KNX/EIB a sítěmi IP. Jeho prostřednictvím se realizuje výměna dat mezi sítěmi a sběrnicemi. Doporučuje se tam, kde se přijímají velké objemy dat, buď v plném rozsahu, nebo jejich výběrem. Přes sítě LAN se přenáší mnohem větší objemy dat než u sběrnicového systému. (3)

1.3 Digitální přenos dat

Data získaná automatizovaným sběrem prostřednictvím, sběrnic a sítí se přenášejí v číslicové podobě, tzn. digitálně. Základním předpokladem všech technických zařízení do uceleného systému je komunikační propojení.

Při správě budov se mezi automatizačními místy a centrálním nadřízeným počítačem předává tisíce různých informací. Tuto funkci řeší již dlouho systém sběrnic (Bus Systém).

Původně výrobci systémů vyvíjeli sběrnice pro přenos dat nezávisle a využívali již známé řešení ze systémů automatizace výrobních procesů. Výrobci museli propojit jednotlivé provozní instalace ovládané vlastními, individuálně zkonstruovanými Direct Digital Control moduly (DDC).(3)

1.4 Požadavky na sběrnice a sítě

V průběhu nedávné minulosti vyvstal požadavek, aby se mohly integrovat různá zařízení vybavená řídícími jednotkami od různých výrobců, které řídí systém. Např. poplachové zařízení proti vloupání se muselo zapojit tak, aby umělo komunikovat mezi dvěma různými sběrnicemi. Proto bylo nutné vytvořit společný veřejný komunikační protokol. (3)

1.5 Oblasti aplikace systémů sběrnic a sítí v budovách

Přední výrobci elektroinstalační techniky dohodli na vývoji vzájemně kompatibilní sběrnice – European Installation Bus (EIB). Po sloučení EIBA s dalšími evropskými organizacemi do sdružení Asociace KNX se používá pro tyto systému označení KNX/EIB. Tato standardizovaná sběrnice zajišťuje výměnu dat mezi různými zařízeními a systémy nezávisle na výrobci. Tato sběrnice pokrývá všechny technické systémy budov tak, aby ji byl schopný naprogramovat a uvést do provozu každý kvalifikovaný elektroinstalatér. Přenosová rychlost je nízká, ale pro povely sepnutí nebo regulační řídící, dostatečná.

Pro regulaci a řízení provozně – technických zařízení je nutno přenášet a zpracovávat velké množství naměřených hodnot, referenčních hodnot a dalších parametrů. Aplikace, které jsou požadovány, vykazují vyšší nároky na procesor. Proto se na evropském trhu pro náročnější aplikace vyčlenila technologie LONWORKS (LON). Tento universální systém vyvinutý americkou firmou Enchalon umožňuje řízení výkonných aplikací na úrovni centrálně nadřízených jednotek (DDC – modulů), tak i u decentralizovaných komponent techniky systému budov. Funkčnost mezi jednotlivými zařízeními od různých dodavatelů zabezpečuje certifikace ze strany LONMARK Interoperability Association.

V budovách o velké plošné výměře se aplikace týká větších obslužných stanovišť. Takové struktury se využívají na vysokých školách nebo vládních budovách.

Jako standardní komunikační systém se uplatnil Bulding Automation and Control Network (BACnet), vyvinutý americkými inženýry a techniky z Americké asociace stavebních inženýrů.

BACnet se vyznačuje objektově orientovanou strukturou s velkým výkonovým rozsahem. Je svým původem a kapacitními možnostmi šita na míru aplikacím technických zařízení budov (TZB). Přesto nenachází uplatnění kvůli vysokým nákladům.(3)

1.6 Komunikace na sběrnici pole (Field Bus)

Na provozní úrovni (v místě, v instalaci zařízení, v procesu) se nacházení snímače a akční členy, tzn. provozní zařízení. Typickými funkcemi, které se na této úrovni provádějí, jsou sepnutí obvodu, nastavení, hlášení (reporting), měření, načítání hodnot. Zařízení na této procesní úrovni lze připojit na sběrnici a jsou vybaveny mikroprocesory, z tohoto důvodu se označují jako „inteligentní“. Vysílají a přijímají bitové informace, jakými jsou datové telegramy, prostřednictvím průmyslové sběrnice Field Bus (dle ČSN EN 61158-2). To se děje mezi nimi vzájemně a v komunikaci s nadřazenými řídícími jednotkami.

Sběrnice pole(Field Bus) je digitální sériová datová sběrnice pro použití ke komunikaci mezi zařízeními automatizační techniky, jako jsou např. měřící prostředky, řadiče, regulátory a řídící jednotky s programovatelnou pamětí (jak ji definují normy IEC 61158, resp. DIN EN 61158, resp ČSN 61158-2 ed. 2, Přenos digitálních dat pro měření a řízení-Sběrnice pole pro průmyslové a řídící systémy, Část 2.a IEC 61748, resp. DIN EN 61784,

resp. ČSN EN 61784 – 1 a ČSN EN 61784 – 2 Přenos digitálních dat pro měření a řízení, části 1. a 2.).

Technika sběrnic pole se rozvinula v 80. letech 20. Století v důsledku pokračující decentralizace automatizačních řešení. Sběrnice měla vyřešit problém značných nároků na kabelové rozvody, neboť tehdejší převážně analogový přenos dat to vyžadoval. Ten byl pak postupně nahrazen přenosem digitálních dat sériovou technikou. V dnešní době se na trhu nabízí řada sběrnic. Jejich parametry, např. přenosový výkon, délka vodičů, počet účastníků mají různý význam podle využití konkrétních aplikací. Charakteristickou vlastností sběrnic je, že malé objemy digitálních datových prvků (bity, byty) se musí přenést v krátkém čase (v µs, ms).(3)

1.7 Komunikace v sítích

Sítí rozumíme integraci (prostřednictvím vodičů anebo bezdrátových spojů) různých technických systémů (např. počítačů, řídících jednotek), která umožňuje a zajišťuje vzájemnou komunikaci mezi těmito jednotlivými systémy. Tato komunikace se uskutečňuje v rámci určitých definovaných pravidel (protokolů), která jsou strukturována referenčním modelem ISO/OSI.

V rámci BACnet si mohou jednotlivá zařízení a jednotlivé subsystémy navzájem mezi sebou vyměňovat informace. Přenos dat prostřednictvím BACnet může být realizován různých sítích. BACnet podporuje technologie LAN typu MS/TP (Master-Slave/Token-Passing), LON, ARCNET[www.arcnet.de], Ethernet a také různá volitelná spojení prostřednictvím telefonních sítí. (3)

1.8 Důležité pojmy digitálního přenosu dat

Prostřednictvím sběrnic a sítí se data získaná automatizovaným sběrem přenášejí v číslicové podobě, tzn. digitálně; jedná se tedy o digitální přenos dat. (3)

1.8.1 Bity a byty

Bit je zkratka z anglického „Binary digit“, tzn. binární číslice, která je nejmenší jednotkou informace. Reprezentuje 2 možné stavy např. ano/ne, ven/dovnitř. Pro binární informaci se

používá tzv. dvojková číselná soustava. Bit nabývá hodnoty buď 0 (nulový bit) nebo 1 (jednotkový bit).

Spojením 8 (osmi) bitů vzniká byte (z anglického byte – slabika), nebo okten (octen). Podle DIN IEC 60027-2 je bit jednotkou SI pro tzv. ekvivalentní kapacitu paměti Me. Symbolické označení jednotky bit v SI je bit, nebo „b“. Symbolem pro byte je „B“ (velké B), které však není jednotkou SI. Ekvivalentní binární kapacita se vypočítává pro n možných stavů určité datové paměti následovně.

$$M_e = lb\ n,\ kde\ „lb“\ je\ symbol\ pro\ binární\ logaritmus\ (logaritmus\ při\ základu = 2)$$

Když např. datová paměť může uložit n = 256 možných stavů, pak

$$M_e = lb\ 256 = 8\ bitů = 1\ B.$$

K vyjádření kapacity paměti M_e se povoluje jednotka SI bit (symbol jednotky bit, nebo b) a jednotka byte (symbol B) s SI předponami pro binární anebo decimální násobky nám ukazuje Tab. 1-1. (3)

Binární předpony [e]				
10^k	2^n	Znak	Název	Hodnota
103	210	Ki	*kibi*	1 024
106	220	Mi	*mebi*	1 048 576
109	230	Gi	*gibi*	1 073 741 824
1012	240	Ti	*tebi*	1 099 511 627 776
1015	250	Pi	*pebi*	1 125 899 906 842 624
1018	260	Ei	*exbi*	1 152 921 504 606 846 976
1021	270	Zi	*zibi*	1 180 591 620 717 411 303 424
1024	280	Yi	*yobi*	1 208 925 819 614 629 174 706 176
Poznámka: 10^k není rovno 2^n, je to jen nejblíže odpovídající mocnina.				

Tab. 1-1 Převodová tabulka

1.8.2 Přenosová rychlost (propustnost kanálů)

Rychlost přenosu binárních číslicových dat υ_{bit}, propustnost („bit rate“) je počet binárních jednotek, bitů, které se v daném časovém intervalu přenesou, vydělený délkou trvání tohoto intervalu (označuje se řeckým písmenem υ, vyslov „ný“). Jednotkou je bit za sekundu. Může být uváděn s předponou násobného množství kbit/s nebo Mbit/s.

Analogicky lze uvádět přenosovou rychlost v B/s, kB/s nebo MB/s. Například u protokolu KNX/EIB se přenese 9600 bitu za sekundu, tzn., přenosová rychlost je 9/6 kbit/s.(3)

1.8.3 Modulační rychlost

Modulační rychlost *u* je definována jako převrácená hodnota délky nejkratšího časového intervalu prvku signálu, který je používán při kódování přenosové linky a který je přenosový systém schopen přenést. Jestliže všechny prvky signálu mají stejnou délku intervalu, rovná se počtu přenesených prvků signálu v daném časovém intervalu.

Jednotka SI pro *u* Baud, pojmenovaná podle francouzského telegrafního technika Émile Bauda (1845-1903). Symbolické značení jednotky je „Bd“. Modulační rychlost se udává v násobných jednotkách s předponami např. kBd nebo MBd.(3)

1.8.4 Binární a hexadecimální čísla

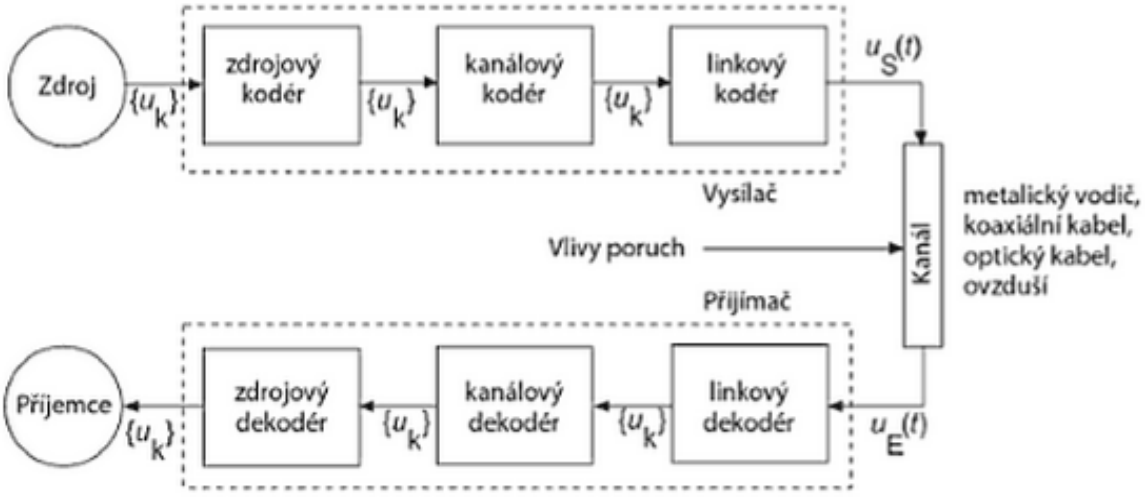
Reprezentace řad bitů pomocí binárních číslic vede k nepřehledným sledům binárních číslic, např. 0101 1101 0011 1100 0010. Proto je výhodnější prezentace v hexadecimálními číslicemi. K tomu, aby se binární číslo převedlo na hexadecimální (šestnáctkové), stačí souvislá řada 4 bitů, viz Tab. 1-2. (3)

Binární číslo	Hexadecimální číslo	Binární číslo	Hexadecimální číslo	Binární číslo	Hexadecimální číslo	Binární číslo	Hexadecimální číslo
0000	0	0100	4	1000	8	1100	C
0001	1	0101	5	1001	9	1101	D
0010	2	0110	6	1010	A	1110	E
0011	3	0111	7	1011	B	1111	F

Tab. 1-2 Vztah mezi čtyřmístným binárním číslem a hexadecimálním číslem

1.8.5 Digitální systém přenosu dat

Datové bity se digitálním systémem přenosu dat přenášejí od zdroje k příjemci. Bity ze zdroje – vysílače mohou např. popisovat stav nějakého procesu. Mapa procesu, získaná binárními snímači se musí přenést do programovatelné paměti, kde se uloží a dále zpracuje. Z hlediska přenosu dat odpovídá toto paměťové místo příjemci. Příslušný snímač (slangově senzor, čidlo) jako vysílač, sběrnice pole jako kanál a programovatelná paměť jako přijímač mohou být modelovány jako digitální systém přenosu dat. Základní uspořádání takového systému ukazuje (obr. 1-2). (3)



Obr. 1-2 – Základní uspořádání systému digitálního přenosu dat

Vysílač přejímá ze zdroje byty, které se mají přenášet. Posloupnost bitů pak prochází komponentami zdrojového kodéru, kanálového kodéru a kodéru linky (vedení) a nakonec se dostane jako fyzikální signál $u_s(t)$ na kanál.

U přenosu realizovatelného pevným rozvodem z metalických (měděných) nebo koaxiálních vodičů se většinou jedná o napěťové signály. Mohou to však být i optické signály, které jsou vedeny optickým kabelem, anebo bezdrátové rádiové spoje, kde jako kanál působí ovzduší. Vlastnost kanálu a vlivy poruch (rušení) přetvářejí signál na signál vysílače.

Přijímač se svými komponentami – linkovým dekodérem, kanálovým dekodérem a zdrojovým dekodérem rekonstruuje z přijímaného signálu $u_E(t)$ posloupnost bitů a ukládá je u příjemce. Komponenty vysílače a přijímače plnily úlohy, jak jsou uvedené v (Tab.1-3). (3)

Komponent	Účel/úloha
zdrojový kodér	vyjmutí zdrojových redundantních datových bitů
zdrojový dekodér	doplnění zdrojových redundantních datových bitů
kanálový kodér	doplnění bitů k zabezpečení dat, s tím spojené navýšení redundance
kanálový dekodér	odstranění zabezpečovacích bitů
linkový kodér	transformace bitové posloupnosti na fyzikální signál
linkový dekodér	transformace fyzikálního signálu na posloupnost bitů

Tab. 1-3 – Komponenty vysílače a přijímače a jejich úlohy

1.8.5.1 Zdrojové kódování a dekódování

Při přenosu bitů převládá snaha, aby se informace vyjádřila co nejúsporněji, s co nejmenším počtem bitů, aby se zkrátila doba přenosu. Využívá se kombinace bitů, které se vyskytují častěji než jiné. Zdrojová kódová slova se zakódují tak, aby nejčastěji se vyskytující bitové kombinace byly přiřazeny nejkratším kódovým slovům a naopak, ty kombinace, jejichž výskyt je nejméně častý, se přiřazují nejdelším kódovým slovům. Tím se dosáhne redukce potřebné délky kódového slova.

Velmi často využívaná metoda překódování je kódování Shannon – Fano. Překódování se požadovaná průměrná délka kódovaného slova při přenosu výrazně zredukuje. Redundance obsažená ve zdrojových kódových slovech se rovněž sníží. (3)

1.8.5.2 Kódování a dekódování kanálu

Při přenosu bitů se vyskytují chyby, tzn. je vysílána bitová jednička a je přijata jako nula, nebo naopak. Zatím neexistuje žádný zaručeně bezchybný přenos dat a chyby přenosu se vyskytují náhodně. Jestliže se datový přenos opakuje, chyby se zpravidla nevyskytnou.

Kódování kanálu má za cíl změnit posloupnost bitů tak, aby datový přenos byl pokud možno bezchybný a bezpečný. To znamená:

a) chyby se (na straně příjemce) zjistí a přenos dat se zopakuje – to je hlavní metoda,

b) chyby se zjistí a opraví.

Při plnění toho zadání se přidělí odeslané posloupnosti bitů dodatečné bity, což sice zvýší nadbytečnost, ale zároveň se tím zvýší bezpečnost dat.

Při kanálovém kódování se využívá nejčastěji tří postupů:

- kontrola paritou,
- křížová kontrola paritou (kontrola podélnou paritou bloková kontrola),
- cyklická redundantní kontrola (CRC – Cyclic Redundancy Check). (3)

Kontrola paritou

Kontrola paritou se provádí tak, že k přenášené posloupnosti bitů se přidává, tzn. paritní bit, jehož hodnota je pevně stanovena, takže buď:

a) celá posloupnost bitů (datové bity včetně paritního) má sudý počet jedničkových bitů, což se nazývá sudá parita (*even parity*), příklad: 01000011 1;

b) celá posloupnost bitů (datové bity včetně paritního) má lichý počet jedničkových bitů, což se nazývá lichá parita (*odd parity*), příklad: 01000011 0.

Vysílač i přijímač musí požadovat stejné kontroly paritou.

Tento postup má následující charakteristické vlastnosti:

- zjistí lichý počet chyb bitů,
- sudý počet chyb bitů se nezjistí,
- není možná oprava chyb, nelze stanovit, kolik bitů a na jakých místech je transponovaných – „obrácených“,
- opatření při zjišťování chyb je opakování přenosu dat. (3)

Křížová kontrola paritou (kontrola podélnou paritou, bloková kontrola)

Přenášená posloupnost bitů se rozdělí do skupin bitů, např. do skupin po 8 bitech. Taková skupina se označí. Ta se uspořádá do maticové struktury (do „bloku“) a každý její řádek a sloupec se označí paritním bitem.

U vysílače a přijímače se musí u kontroly sloupců i řádků používat stejný druh kontroly paritou. Vlastnosti tohoto postupu s ohledem na datové zabezpečení jsou následující:

- v případě aplikace tohoto postupu a při výskytu 1bitové chyby, lze tuto chybu zjistit a opravit,
- 2bitovou a 3bitovu chybu lze nají, ale nelze je opravit,
- 4bitou chybu lze jen poznat, a to pouze pokud se nevyskytne „v z rohů čtyřúhelníku“,
- Obvyklým korekčním opatřením při výskytu chyb je opakování datového přenosu. (3)

Cyklická redundantní kontrola (CRC – Cyclic Rendundancy Check)

CRC je jednou z nejčastěji používaných metod zabezpečení datového přenosu u sběrnic pole (průmyslových sběrnic). Slouží ke zjištění chyb. Při rozpoznání chyby se přenos dat opakuje.

Princip zjištění chyby CRC spočívá v tom, že se přenášené datové posloupnosti bitů doplní kontrolní posloupností bitů a dále se na straně příjemce celá posloupnost bitů beze zbytku vydělí posloupností zkušebních (testovacích) bitů poté, co proběhne přenos. Jestliže, je dělení beze zbytku možné, považuje ji příjemce jako bezchybnou. I když tato metoda ujistí značně více chyb než kontrola paritou nebo křížová (bloková) kontrola, není ani tato metoda perfektní a některé chyby nepozná. (3)

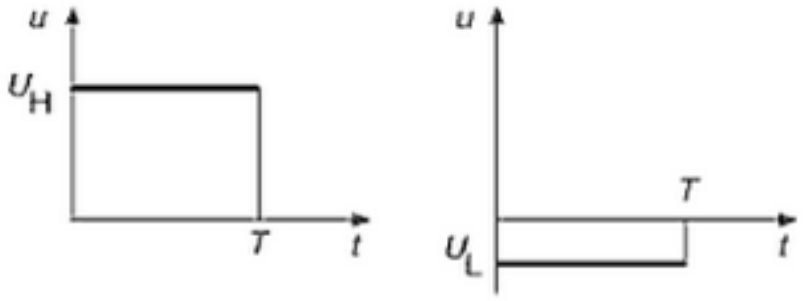
1.8.5.3 Kódování linky

Výstupní bitová posloupnost z kanálového kodéru musí být transformována na fyzikální signál, aby ji bylo možno přenést prostřednictvím kanálu (jako přenosového média). U sběrnice se používá převážně jako přenosného média metalického (měděného) kabelu a posloupnost bitů je přeměněna na napěťové signály. Je to zpravidla binární signál, který tvoří dva prvky signálu: jeden představuje nulová bit a druhý bit jedničkový. Celkový počet signálních prvků odpovídá počtů bitů v přijaté posloupnosti.

Při určování prvků signálu se musí brát v úvahu více hledisek, např. disponibilní šíře pásma kanálu, schopnost vyrovnání napětí signálu a možnost pravidelné obnovy signálu a co možná nejjednodušší technická proveditelnost spojení. Počet kódů v lince vedení je velký. Často používané kódy linky Non-Return-to Zero (NRZ) a dvě varianty Manchasterského kódu (Manchaster code – Biphase – OL – Code a Differntial Manchaster Code). (3)

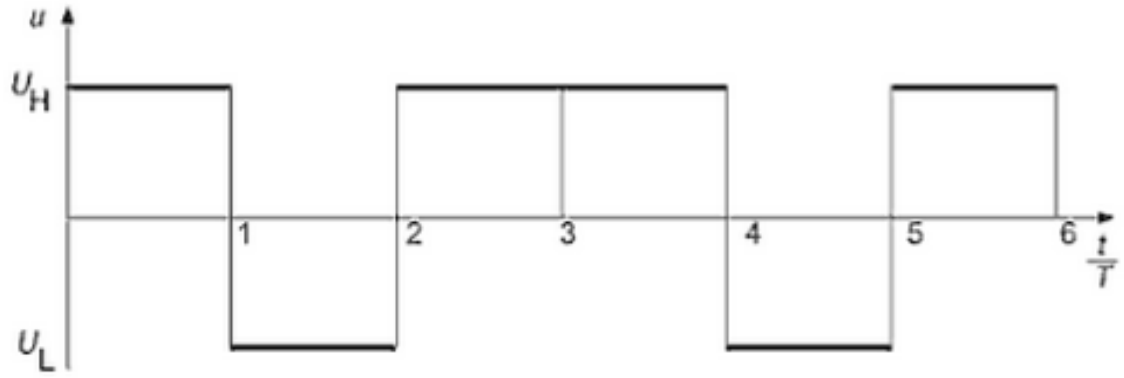
NRZ-Code

Při kódování NRZ se používá signálních prvků s konstantní úrovní *UH*, resp. *UL* v časovém intervalu *T* (obr. 1-3).



Obr. 1-3 Prvky signálu při použití NRZ-Code

Např. bitová posloupnost 010010 bude kodérem linky přeměněna na následující signál (Obr. 1-4).

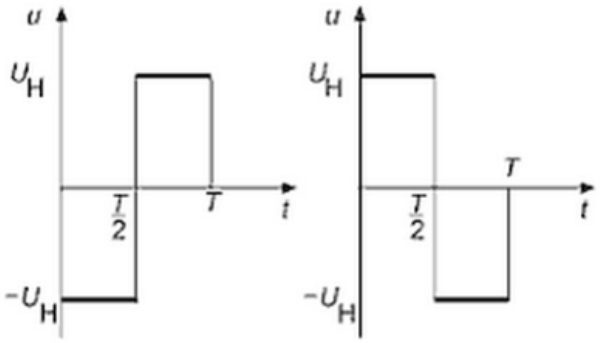


Obr. 1-4 Napěťový signál kódovány NRZ rozhraní RS-232

Signály kódování NRZ nejsou všeobecně dále dělitelné. U delších nulových nebo jedničkových posloupností nemůže příjemce dále předávat délku intervalu *T* signálu, neboť tento signál neobsahuje žádnou další změnu hladiny (čela impulsu). Manchesterský kód tyto nedostatky nemá. (3)

Manchasterský kód (Manchaster Code – Biphase L)

Manchasterský kód ve variantě Biphase L jsou dva signální prvky se dvěma intervaly *T*, přičemž po *T/2* se hladina U_H změní na hladinu $-U_H$ a naopak (Obr.1-5).



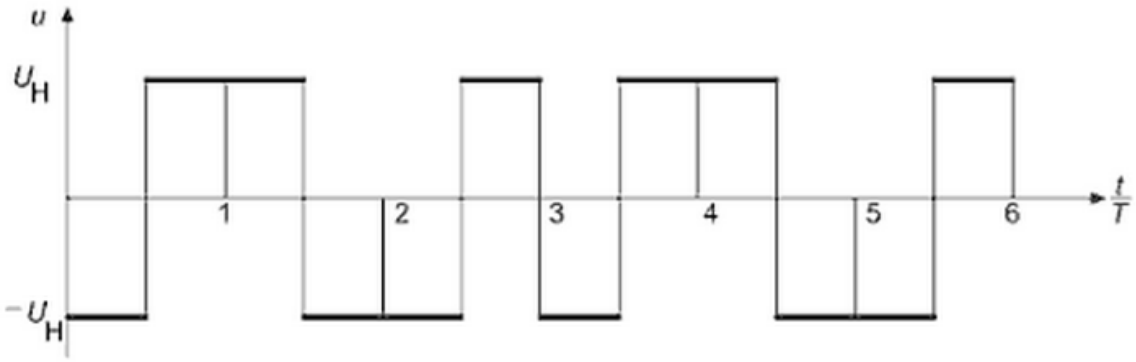
Obr. 1-5 Prvky signálu u Manchasterského kódu

Přiřazení prvků signálu k logickým stavům „0“ a „1“ vypadá takto:

- stav „0“ se prvku signálu přiřadí, pokud uprostřed intervalu hrana impulsu vzrůstá,
- stav „1“ se prvku signálu přiřadí, pokud uprostřed intervalu hrana impulsu klesá.

Pravidlo je možno aplikovat i v obráceném pořadí.

Bitová posloupnost 010010 bude kodérem linky změna na Manchesterský kód (Obr.1-6).

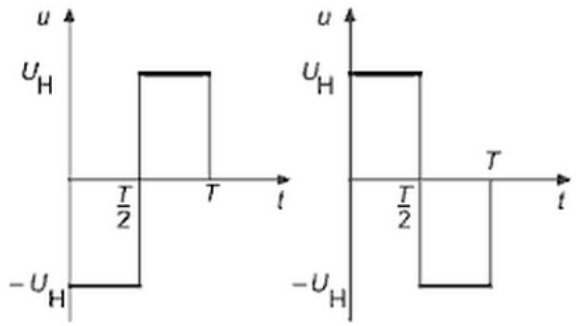


Obr.1-6 Zakódování podle Manchesterského kódu (Biphase – L)

Výhodou Manchasterského kódu je dělitelnost a v tom, že cyklus přenosu obsahuje dostatečné množství informace: nejpozději v tobě *T* však vyžaduje Manchasterský kód dvojnásobnou šíři kanálu v porovnání s NRZ – Code, neboť pravoúhlé impulsy mají dvojnásobnou frekvenci. Důležitou oblastí aplikace Manchasterského kódu je přenos dat v lokálních sítích Ethernetu. (3)

Diferenciální – Manchesterský kód

Differential Manchaster Code (DMC) využívá vedle možnosti Manchaster Code ještě dalších dvou prvků signálních prvků v šířce impulsu *T*. Uprostřed intervalu *T/2* se vždy hladina U_H změní na hladinu $-U_H$ nebo naopak (Obr.1-7).



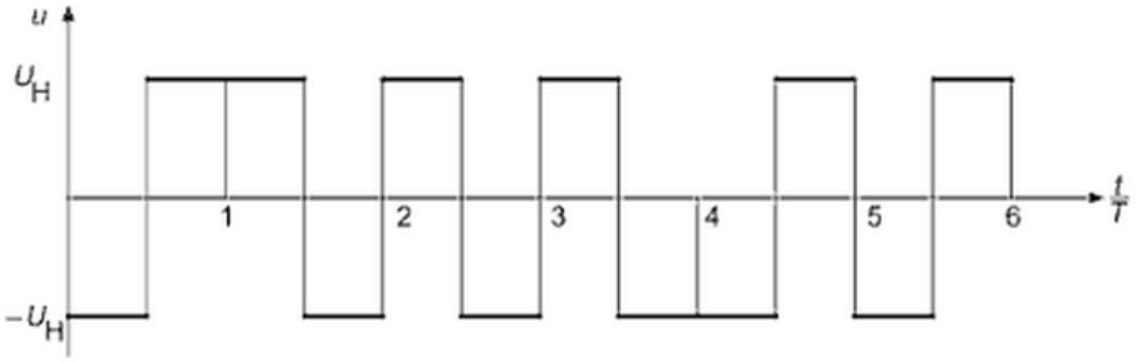
Obr. 1-7 Prvky signálu při aplikaci DMC

Přiřazením prvků signálu logickým stavům „0“ a „1“ není pevné, ale závisí na poslední hladině předchozího prvku signálu:

- v případě stavu „1“ se poslední hladina (U_H resp. $-U_H$) předcházejícího prvku signálu zachová,

- v případě stavu „0“ se poslední hladina (U_H resp. $-U_H$) předcházejícího prvku signálu mění ve svůj opak (na $-U_H$ resp. U_H).

Při posloupnosti bitů 010010 se například bude kodérem linky v DMC měnit na signál takto (obr. 1-8).



Obr.1-8 Kódování při Differential Manchaster Code

Důležitou aplikační oblastí pro DMC je datový přenos v síti LON. (3)

1.8.6 Referenční model ISO/OSI

Referenční model ISO/OSI je kodifikován mezinárodním standardem [ISO 7498] a popisuje, jak mohou vytvářet vrstvené protokoly (Pravidla o provádění komunikace). Dále se uvádí popis úkolů, které se implementují v jednotlivých vrstvách protokolu. Dobré datové technické spojení není ještě samo o sobě dobrou komunikací. Při výměně informací může dojít k nedorozumění. (3)

1.8.6.1 Pravidla úspěšné komunikace

K zajištění bezchybného průběhu komunikace vybavení automatizační, řídící a přenosovou technikou nestačí. Komunikační systém musí mít kromě technických funkcí přenosu dat i postranné komunikační funkce, které vyžadují soustavu závazných pravidel, podle nichž se bude probíhající komunikace řídit. Takovýto soubor standardizovaných pravidel se nazývá protokol.

Protokol je soustava definovaných pravidel, podle nichž se musí uskutečňovat a probíhat komunikace mezi komunikačními partnery.

V každém protokolu musí být dodrženy např. tyto podmínky:

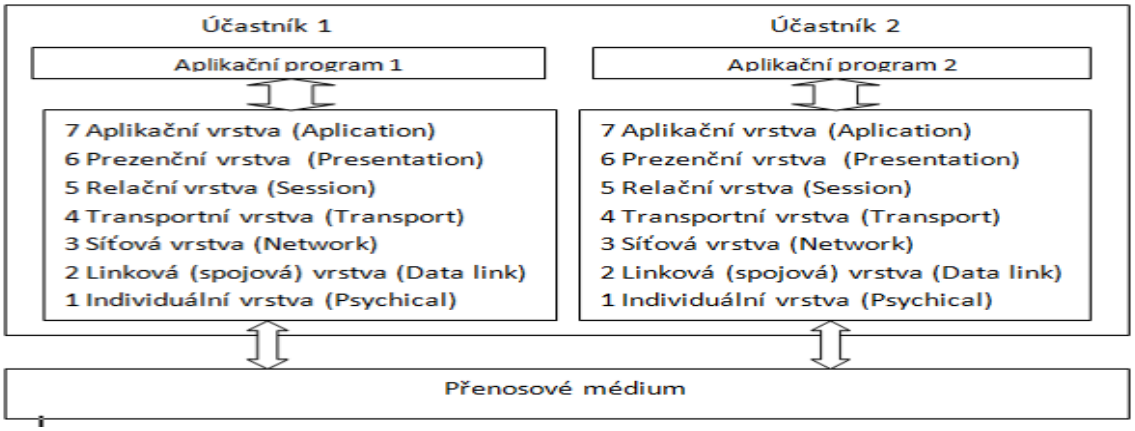
- Kdo se smí připojit do prostředí přenosového média?
- Jak se zjistí chyby při přenosu data a co se stane, když se nějaká chyba zjistí?
- Co se stane, když příjemce dostane víc dat, než kolik jich může v daném časovém úseku zpracovat?
- Jak se datové telegramy dostanou ke správnému adresátovi?

V tomto složitém komunikačním procesu se vyskytly různé pokusy jak ho logicky rozložit na předem nezávislé dílčí procesy, které by byly propojeny vzájemně definovaným interfacem (přechodem).

Velmi často používaným modelem je Referenční model OSI pro otevřené systémy (ISO Reference Model for Open Systems Standardization), zkrácené Referenční model OSI/ISO. Zkratka ISO znamená Interanzional Organization for Standardization (Mezinárodní organizace pro normalizaci).(3)

1.8.6.2 Referenční model ISO/OSI

Každý otevřený informační systém má za úkol zajistit, aby se data z jednoho aplikačního procesu přenesla k procesu dalšímu (obr. 1-9).



Obr.1-9 Sedmivrstvý referenční model OSI

Pracovní postup systému OSI zahrnuje:

- Komunikační vrstva od aplikační vrstvy k přenosovému médiu prochází sedmi vrstvami, a to od vysílače sestupně „dolů“ a u přijímače vzestupně směrem

„nahoru“. Systém OSI je tedy hierarchicky strukturován a postupně provádí transformaci z dat získaných v aplikaci až po fyzikální signál a naopak.

- Každá vrstva přejímá omezené množství komunikačních služeb.
- Každá vrstva předává nadřazené vrstvě své služby, např. individuální vrstva (vrstva 1) vrstvě linkové (vrstva 2).
- Mezi dvěma (vertikálně sousedícími vrstvami jednoho účastníka je pevně definované stanovené komunikační rozhraní.
- Jestliže nadřazená vrstva převezme službu, vydá podřízené vrstvě k dispozici paket, který obsahuje řídící informace vrstvy a data. Z těchto důvodů počet přenášených bitů od vrstvy k vrstvě „směrem dolů“ vždy narůstá, kdežto na opačně orientované cestě „ směrem nahoru“ se stále snižuje.
- Dvě vzájemně si odpovídající vrstvy dvou systémů OSI (tzv. „partnerské vrstvy“) např. linkové (spojové) vrstvy účastníků 1 a 2 se mezi sebou vyměňují data – tzv. datové jednotky protokolu (Data Unit Prototocol - UDP). Výměna dat mezi partnerskými vrstvami se provádí na základě dohodnutého souboru pravidel, tzn. Protokolu vrstvy, takž např. Linkový protokol přísluší linkové vrstvě. Odpovídající vrstvy 2 až 7 systému OSI dvou účastníků takto zůstávají logicky navzájem ve spojení a realizují „svou“ komunikaci podle příslušného protokolu vrstvy

Každá vrstva se může vyměnit, pokud jí zůstane funkčnost. Např. u individuální vrstvy se může přenos dat provést kroucenou metalickou dvojlinkou, silovým vodičem nebo bezdrátovým přenosem. Není však nutné, aby se v každém komunikačním systému implementovalo všech sedm vrstev. U systému sběrnic jsou realizovány vrstvy 1,2, 3, 4 a 7. (3)

1.9 Důležité pojmy z oblasti sběrnic a sítí

Součásti sběrnic, resp. sítí, jsou navzájem fyzicky spojeny určitým způsobem. Toto uspořádání se nazývá topologie sběrnic nebo sítí. Jestliže účastník chce přistoupit na sběrnici nebo síť, musí se tak stát podle určitých pravidel, aby se vysílané signály při současném přístupu více účastníků nepřekrývaly a nevznikaly tak chyby. Toto řeší spojový přístupový protokol kanálu. (3)

1.10 Rozdělení sítí

Počítačovou sítí rozumíme spojení dvou a více počítačů tak, aby mohly navzájem mezi sebou sdílet své prostředky. Přitom se jedná o prostředky hardwarové nebo softwarové.

Lokální síť – LAN (Local Area Network). Skupina počítačů a dalších zařízení vzájemně propojená komunikačním spojem v malé oblasti (do několika km), který umožňuje zařízením vzájemnou komunikaci v rámci určité skupiny (firma, banka, škola, úřad nebo domácnost.

Rozlehlá síť – WAN (Wide Area Network). Datová komunikační síť, která pokrývá rozsáhlé území a využívá spojení veřejných poskytovatelů přenosových služeb. Typickým příkladem je internet.

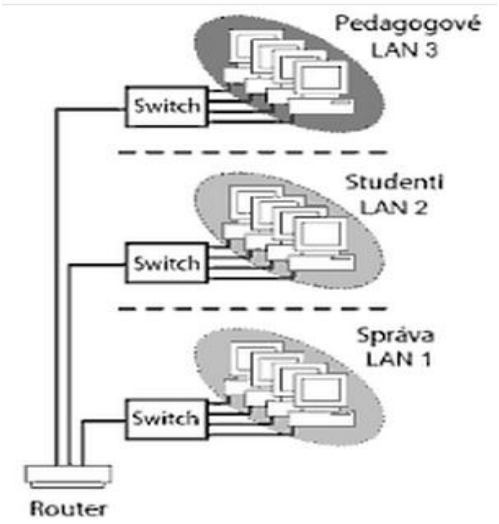
Bezdrátová síť – WIFI (Wireless Fidelity). Je určená k náhradě kabelového ethernetu bezdrátovým spojením v bezlicenčním pásmu, které je dostupné téměř v celém světě.

V odborné literatuře se může setkat s dalšími typy sítí (MAN – Metropolitní sítě, PAN – Osobní počítačové sítě) nebo s jiným způsobem dělení.(1)

1.11 Virtuální sítě LAN (VLANs)

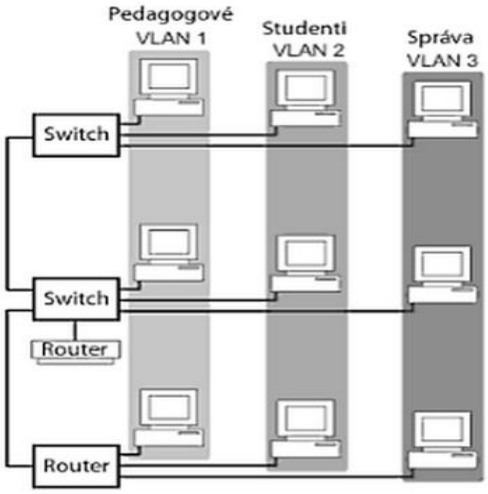
Switch přenáší datové rámce jedné účastnické stanice vždy na její příslušná výstupní připojení. Naproti tomu Brodacasts směřují na všechny připojené stanice a přenášejí se na všechna připojení. Síť, která je vybavena přepínači (switches), označuje jako doména Broadcast (Broadcast domain). U sítí s velkým počtem účastníků se může přejít na vysoký počet Broadcasts, které jsou distribuovány v celé síti. Tyto Broadcast si nárokují část pásem, která jsou volná a vytíží vyhodnocené připojení stanice. V síti připojené přepínači (Switched Network) si mohou v zásadě stanice vyměňovat zprávy v režimu každá s každou. Z důvodu bezpečnosti je to však omezeno a jen určitým uživatelským skupinám se dovolí, aby mezi sebou zájemně komunikovaly.

Např. na vysoké škole mohou být 3 skupiny: pedagogové, studenti a správa. Tyto skupiny musí být vzájemně odděleny, aby se zabránilo nepovolenému přístupu a aby se chránily uložené údaje o zasedáních, vědeckých radách a osobní data. Běžná bezpečnostní opatření, jako ochrana heslem, nejsou většinou dostačující a lze je úspěšně obcházet. Nákladným řešením je výstavba fyzicky oddělených sítí, jak je uvedeno na obr. 1-10.



Obr.1-10 Struktura sítě VLAN bez rozdělení do tří uživatelských skupin

Každá skupina má svůj vlastní switch a k němu příslušnou kabelovou síť. V případě organizačních změn, jakou je např. přesun přesun pracovníků, by se musela kabelová síť přizpůsobovat a rekonstruovat tak, aby se zachovalo připojení ke zvolenému přepínači(switch). Přepínač (switch) předává datové rámce jen mezi přípojkami stejné skupiny. Také Broadcasts se předávají jen počítačům, které jsou ve stejné skupině. Aby prostřednictvím několika přepínačů tento způsob zpracování fungoval, musí být rámce, které vedou od jednoho přepínače ke druhému, označeny. Tento způsob identifikace se nazývá Tagging – doslova značkování. Rámce, které vstupují na přepínač, jsou opatřeny skupinovým poznávacím identifikátorem. Při Broadcastu se takto označený rámec přivádí ke všem přepínačům. Přepínače (switche) odhalí identifikátor skupiny a doručí rámce na všechny připojené PC, které patří do jedné skupiny. Pro PC je tento postup transparentní, neboť změny v rámcích provádí vždy odesílající přepínač zpětně, vratným způsobem. Jestliže se přesto povolí komunikace mezi různými skupinami, musí se použít jako spojovacího prvku směrovače (routeru). Tím se mohou transportovat data mezi skupinami a současně s tím i cíleně filtrovat a vyřešit tok dat (firewall) a zabránit neoprávněnému přístupu (obr. 1-11). (3)



Obr.1-11 Struktura sítě VLAN s rozdělení do tří uživatelských skupin

1.12 MAN sítě

IEEE 802.6 je standard pro sítě *Metropolitan Area Network* (MAN). Jedná se o zdokonalení staršího standardu, který využíval technologii *Fiber Distributed Data Interface* (FDDI). Ten ztroskotal kvůli jeho drahé implementaci a chybějící kompatibilitě se současnými normami LANu. MAN využívá standard protokolu *Distributed Queue Dual Bus* (DQDB), který tvoří dvě protisměrné sběrnice. Tento standard však ztroskotal ze stejného důvodu jak FDDI. Většina sítí MAN v současnosti používá technologie Synchronous opitical network (SONET), tzv. digitální komunikaci za pomocí laseru nebo LED diod pomocí optických vláken nebo Asynchronous Transfer Mode (ATM), který byl dříve standard pro vysokorychlostní síťovou architekturu.(18)

1.13 PAN sítě

Osobní sítě, zvané PAN (*Personal Area Network*), jsou sítě s nejmenším rozlehlostí, jsou používané pro propojení osobních elektronických zařízení typu mobilní telefen, laptop nebo PDA. Osobní počítačové sítě si kladou za cíl co nejvyšší přenosovou rychlost (obvykle překračuje několik megabitů za sekundu), ale spíše odolnosti proti rušení, nízkou spotřebu elektrické energie nebo snadnou konfigurovatelnou. Mají velmi malý dosah, obvykle jen několik metrů. Nejčastěji je realizována pomocí technologie Bluetooth, (někdy WiFi), ZigBee nebo IrDA.(19)

1.14 WAN sítě

Rozsáhlé sítě, zvané též WAN (Wide Area Network), jsou sítě umožňující komunikaci na velké vzdálenosti. Bývají obvykle veřejné, ale existují i privátní WAN sítě. Jsou to sítě typicky pracující prostřednictvím komunikace se spojením, které nepoužívají sdílený prostředek. Přenosové rychlosti se velmi liší podle typu sítě. Začínají na desítkách kilobitů za sekundu, ale dosahují i rychlosti řádu několika gigabitů za sekundu. Příkladem takové sítě může být internet.(19)

1.14.1 Architektura

Client–Sever – jednotlivý klienti (PC) komunikují vždy s centrálním serverem či servery, prostřednictvím kterého komunikují i s jiným klienty (pokud je to potřeba). Server je samostatný počítač, který řídí předávání dat po sítí a umožňuje připojeným stanicím přístup k datům a k periferiím zapojených v sítí. Serverů může být více a mohou mít specifické významy, jako je např. databázový server, zabezpečovací server atd.

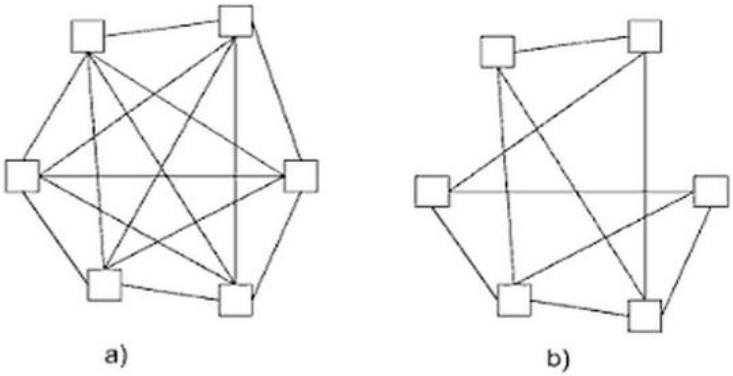
Peer-to-peer(rovný s rovným) neboli P2P. Je označení architektury počítačových sítí, kde spolu komunikují přímo klienti. Nejjednodušším příkladem je propojení dvou PC nebo PC a IP kamery.(1)

1.14.2 Základní topologie

Jednotlivá zařízení nebo účastníci, kteří se chtějí vyměňovat data v síti, jsou určitým způsobem geometricky vzájemně spojeni. Toto uspořádání se nazývá topologie sběrnice nebo sítě.(3)

1.14.2.1 Úplná nebo částečná polygonální síť

V úplně polygonální (neboli úplně propojené) síti se spojuje každý účastník přímo se všemi ostatními účastníky (obr. 1-12a). U částečné polygonální (též částečně propojené) sítě se spojují se všemi účastníky přímo jen někteří účastníci (obr. 1-12b).(3)

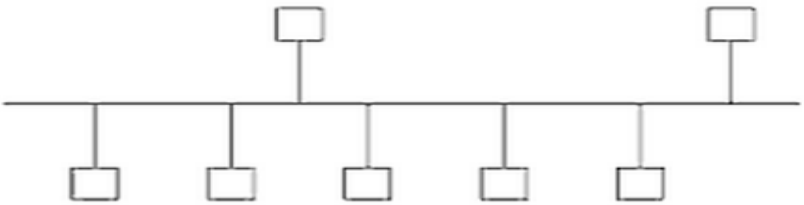


Obr. 1-12 Úplně propojená (a) a částečně propojená síť (b)

1.14.2.2 Topologie sběrnice (liniová)

U liniové topologie jsou jednotlivý účastníci připojeni krátkými odbočkami k přenosovému kanálu (sběrnici), obr. 1-13.(3)

Skládá se z jediného kabelu, nazývaného hlavní kabel (také páteř nebo segment), který v jedné řadě propojuje všechny počítačové sítě



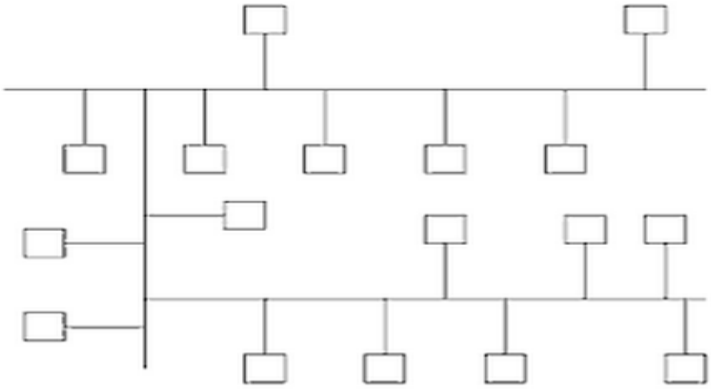
Obr. 1-13 Liniová (sběrnicová) topologie

K propojení se používá koaxiální kabel s impedancí 50Ω a BNC konektory. Na konce vedení musí být připojeny zakončovací odpory (terminátory) s impedancí 50Ω (obr. 1-14). (3)

Obr. 1-14 Jednotlivé vrstvy koaxiálního kabelu(7)

1.14.2.3 Topologie stromu

Jedná se o rozvinutí myšlenky konstrukce liniové topologie (obr. 1-15).(3)

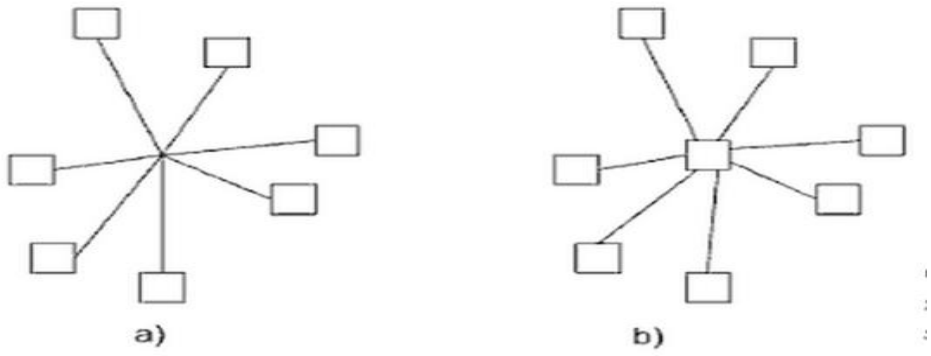


Obr. 1-15 Stromová topologie

U topologie stromu (obr. 1-11) nejsou na sběrnici připojeni jen účastníci, ale další sběrnice (linky). Takto mohou být zasíťováni účastníci na velkých plochách.(3)

1.14.2.4 Hvězdicová topologie

Při aplikaci hvězdicové topologie se přenosové kanály všech účastníků sbíhají do jednoho centrálního uzlu, nebo jsou společně propojeny do jedné centrální stanice. Centrální stanice se nazývá HUB nebo SWITCH (obr. 1-16). (3)



Obr. 1-16 Hvězdicová topologie s centrálním uzlem (a) a s centrální stanicí (b)

K propojení se používá UTP (Unshielded twisted pair), nestíněná kroucená dvojlinka zakončená konektory RJ 45 (obr. 1-17). (3)

Obr. 1-17 Konekror RJ 45(8)

1.14.3 Kabely, konektory a jejich zapojení

Dnes se zpravidla používá koaxiální kabel RG-58 s impedancí 50Ω. Montáž konektoru se provádí pomocí speciálních, tzv. stripovacích a krempovacích kleští.

1.14.4 Metody přístupu

Sběrnice a sítě umožňují všem účastníkům v prostředí síťové komunikace přímý přístup ke kanálu přenosu. Obecně řečeno, přenosový kanál může signály přijímat a dále zpracovávat. U vysílání však vzniká problém, že větší počet vysílaných signálů může přetížit kanál a navzájem by se mohly překrývat, rušit nebo smazat, pokud by byl přístup povolen více než jednomu účastníkovi. Proto byly vyvinuty metody, které umožňují, aby se při přenosu zdařil přístup ke kanálu bez kolizí.

Existují dvě možnosti jak regulovat přístup ke kanálu (na sběrnici nebo do sítě):

- přístup ke kanálu přidělím (řízený neboli deterministický přístup),
- přístup ke kanálu podle požadavku (náhodný neboli stochastický přístup).(3)

1.14.4.1 Přístup podle přidělení (rezervace)

U přidělovaného přístupu se v určitém časovém okamžiku k přístupu na kanál opravňuje pouze jeden jediný účastník. Přidělování přístupu ke kanálu je cyklické, tzn., že každý účastník obdrží uspořádanou řadu vysílajících oprávnění. To umožňuje také přesné

stanovení časového intervalu, po jehož uplynutí smí účastník znovu vysílat (proto deterministický přístup).

Oprávnění vysílače v případě přístupu přidělení:

- od účastníka s nejvyšší prioritou (Master) se převede na další účastníky (Slaves) – tzn. Metoda Master – Slave,
- nebo oprávnění se k vysílání předává v kruhu dále tzv. Token – „chodí pešek okolo“ metoda Token – Passing.

V protokolu BACnet se metoda Token-Passing kombinuje s metodou Master-Slave.(3)

1.14.4.2 Přístup podle požadavku

U této metody účastníci přistupují k přenosovému vedení (kanálu). Náhodně. Musí proto poznat, zdali je kanál volný, anebo obsazený. Když je kanál volný a několik účastníků chce současně zahájit přenos, musí se tento konflikt v přístupu vyřešit ve prospěch jednoho. Ti účastníci, jimž byl přenos odepřen, musí tento pokus později opakovat a o získání přístupu soutěžit s ostatními. Takto se nedá garantovat, zejména při vyšším vytížení kanálu, že se na určitého účastníka v stanoveném čase dostane; přístupová metoda není deterministická.

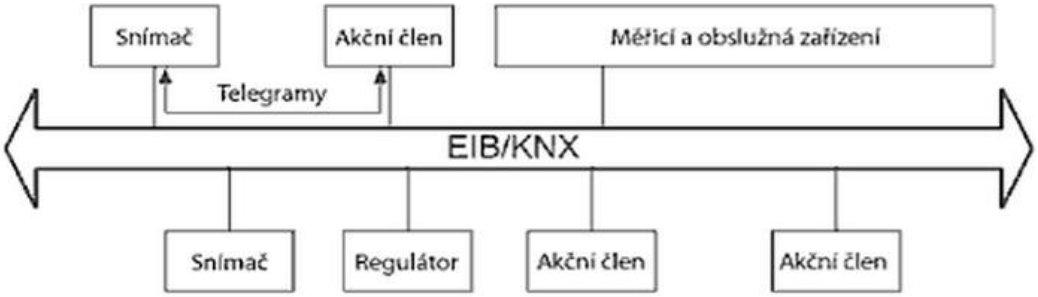
Známé postupy této kategorie jsou:

- CSM/CD (Carrier Sense Multiple Access/Collision Detection), kterého se např. používá u aplikace LON,
- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), který je využíván u KNX/EIB. (3)

2 ZÁKLADNÍ POŽADAVKY NA ZABEZPEČOVACÍ ZAŘÍZENÍ

2.1 Evropská instalační sběrnice KNX/EIB

Evropská instalační sběrnice KNX/EIB je celosvětový standard pro systémovou techniku budov. Používá se pro síťové informatické spojení zařízení (snímačů, akčních členů, regulačních a řídících zařízení, obslužných a měřících zařízení (viz obr. 2-1). Implementace KNX/EIB je přizpůsobena elektrotechnické instalaci, čímž jsou zajištěny funkce a automatizované procesy v budově.



Obr. 2-1 Informatické zasíťování zařízení systémové techniky budov sběrnicí KNX/EIB

Dat určená pro vzájemnou komunikaci se vkládají do datového telegramu a prostřednictvím instalační sběrnice se digitálně přenášejí. Sběrnici je možno realizovat různými fyzikálně – technickým způsobem. V případě KNX/TP je to kabel Twisted Pair, tj. kroucený pár metalických vodičů, u KNX.PL je to silový kabel a v případě KNX.RF se používá rádiového spojení. Lze taky použít přenos dat optickým kabelem. Výměna informací probíhá přímo mezi jednotlivými účastníky, kteří mají realizovat nějaké funkce.(3)

2.2 Použití KNX/EIB

Více pohodlí, bezpečnosti a větší hospodárnost – to jsou hlavní faktory stále širšího uplatnění elektroniky a průmyslové spojovací techniky v účelových budovách.

K realizaci automatizace a řízení mnohostranných funkcí budovy a to zejména pro :

- zajištění funkcí vstupu a výstupu,
- funkce zpracování dat,

- řídící funkce,
- obslužné funkce,

je v moderních budovách k dispozici množství:

- snímačů (např. pohybových, tlačítkových, osvětlení),
- akčních členů (spínacích, stmívacích, pro řízení pohonů),
- řídící a regulačních přístrojů,
- obslužných, měřících a sledovacích zařízení (přístroje vizualizace, např. kontrolní panely).(3)

2.3 Druhy sběrnicových přístrojů

Přístroje na sběrnici můžeme rozdělit do čtyř hlavních skupin:

- systémové přístroje, např. napájecí zdroj, akumulátory, liniové a oblastní spojky, liniové zesilovače, sběrnicové spojky rozhraní RS 232, resp. USB, IP rozhraní,
- snímače, např. tlačítkové snímače, tlačítkové ovladače a spínače, snímače pohybu, snímače rozbití skla,
- akční členy, např. spínací akční členy, ovladače, žaluziové nebo roletové akční členy,
- ostatní, např. logické moduly, kontrolní panel

Protože umístnění a možnosti zabudování těchto přístrojů závisí na lokalitě, lze je dostat v různých provedení, zejména pro instalace v krabicích pod omítku (zapuštěná montáž) nebo na omítku (nástěnná montáž), jako vestavné přístroje nebo přístroje, které se montují do rozvaděčů na nosnou lištu.(3)

2.4 Přenosová média a signály procházející po sběrnici

Pro přenos mezi účastnickými stanicemi mohou být využita různá média:

- Twisted Pair – kroucený pár (TP),
- Power Line – silové vedení (PL),

- rádiový přenos (RF),
- Ethernet (IP),
- optická vlákna – Optic Fibre(OF).

Binární informace musí být v závislosti na přenosovém médiu, přetransformovány zpět do vhodného fyzického signálu, např. do signálu napěťových, rádiových, světelných. To je úkolem přenosového modulu.(3)

2.4.1 Přenos přes kroucený pár

Kroucený pár – Twisted Pair (TP) se nejčastěji používá u novostaveb, protože se jedná o nákladové výhodnou variantu a položení nového rozvodu TP je jednoduché.

Certifikované jsou různé varianty provedení. Pro klasický TP je typické vedení YCYM 2 x 2 x 0,8. Má zelené opláštění PVC a skládá se ze dvou párů žil, jejichž vodiče mají průměr 0,8 mm, jsou ve dvojici zakroucené a odstíněné (kašírované hliníkovou fólií). Pár žil s červeným vodičem (+) a černým vodičem (-) se používá pro napájení účastníka energií a současně pro přenos dat. Pár žil se žlutým a bílým vodičem se používají jako rezervy, např. pro přídavné napájení účastníka

Vedení (TP) se může pokládat pod omítkou v suchém, vlhkém i mokrém prostředí. Platí pro něj stejné instalační podmínky jako pro vedení silnoproudu.(3)

2.4.2 Silové vedení (PL), rádiový přenos (RF), Ethernet (IP), kabely z optických vláken (OF)

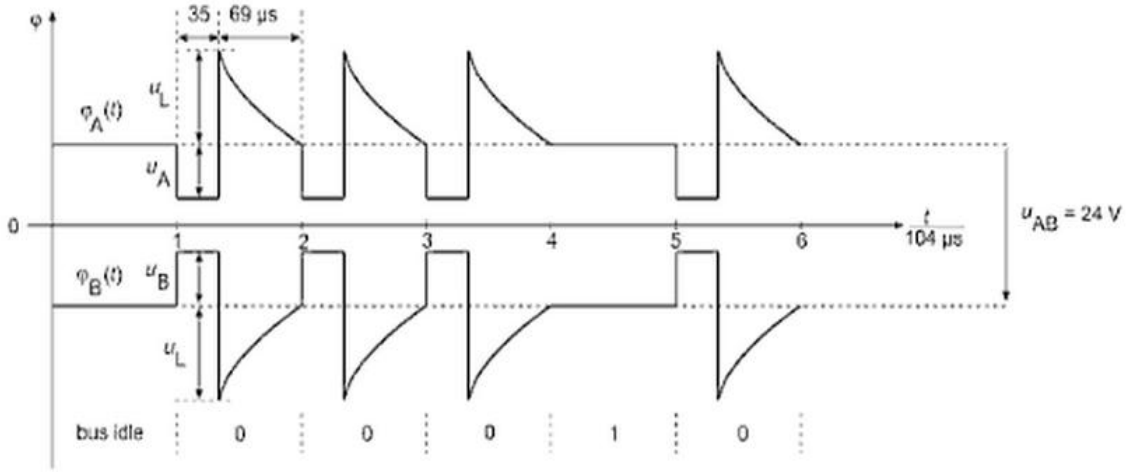
Pro určité aplikační podmínky se před TP dává přednost jiným přenosovým technikám:

- Výhodou silového vedení (PL) se projevuje zejména tehdy, když se stávající rozvodná síť musí využít pro přenos dat, kde se žádné samostatně oddělené vedení sběrnice nemůže položit. Datové signály se takto překrývají (superponují) sínusovým napětím napájecí stanice.
- U rádiového přenosu (RF) není potřeba pokládat žádné vedení, neboť přenos se děje rádiovým bezdrátovým spojem.
- Ethernet se využívá při napojení konfigurace na síť TCP/IP automatizace budov, např. při komunikaci s obsluhou a dohledem.

- Kabelů s optickými vlákny se využívá tam, kde jen nutné překonat větší vzdálenosti, především když se chceme vyhnout instalaci přístroje pro ochranu před výboji a přepětím tam, kde pokládané vedení zasahuje za hranice pláště budovy nebo jejího pozemku.(3)

2.5 Přenos sběrnicí TP (Twisted Pair)

Binární informace se transformuje do signálů elektrického napětí. K tomu se používají speciální přenosové moduly, např. TP-UART-IC. Signálem je rozdíl mezi napětím červeným žilovým vodičem (vedení A) a záporným černým vodičem (vedení B). Průběh napětí v čase můžeme změřit osciloskopem. Jeho první 3 bity jsou vždy nulové bity. Potom následuje např. kombinace bitů 1 0. Této posloupnosti bitu odpovídá průběh potencionálů na vodičích A a B, jak je znázorněno na obr. 2-2. Ve stavu kdy nenastává žádná aktivita na sběrnici (bus idle) nebo kdy je odesílán jedničkový bit, činí jmenovitý rozdíl potencionálů u_{AB} 24 V DC.



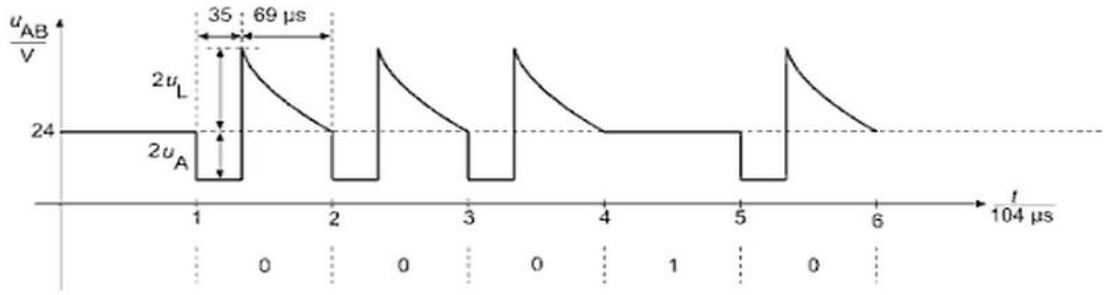
Obr.2-2 Průběh potencionálů vedení A a B

Platí následující vztahy

$0{,}25\ V < u_{A,}\ u_B < 5\ V$

$u_L = 1{,}7.\ u_A < 5\ V$

Na přijímači bude vyhodnocen jako rozdíl potencionálů $\varphi_A - \varphi_B = u_{AB}$ (obr. 2-3).



Obr. 2-3 Průběh napěťových signálů

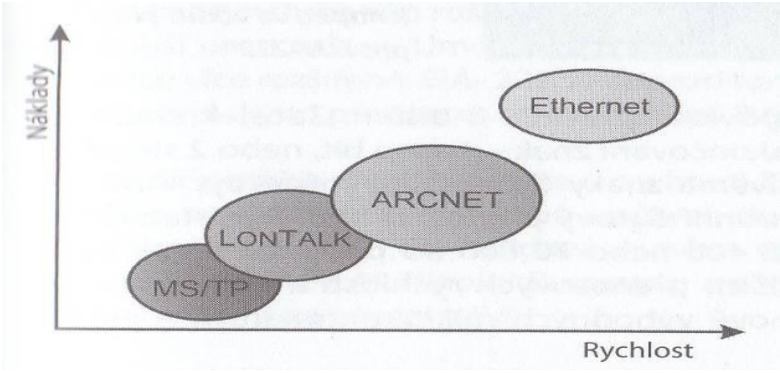
Průběh napětí znázorněný na obr. 2-3 je určitou idealizací. V závislosti na počtu účastníků, na vzdálenosti od zdroje napětí (úbytek napětí na vedení sběrnice, kapacita vedení) a v závislosti na vnějším rušení stability napětí vykazuje výsledný průběh podstatné odchylky od ideální formy. Moduly přijímače mohou však i tyto deformované a poškozené signály zpracovat, pokud se vejdou do stanoveného tolerančního pole. Prostřednictvím linkových spojek a liniových opakovačů se signály pro přesměrování v další linii, resp. v dalším liniovém segmentu generují, takže příjemce – i ve značné vzdálenosti od vysílače – může spolehlivě detekovat digitální informace obsažené v signálu.

Je-li pro přenos 1 bitu T = 104 µs, potom propustnost υ_{bit} lze vypočítat:

$$\nu_{\text{bit}} = \frac{1}{\text{T}} = \frac{1bit}{104\mu s} \approx 9615\frac{bit}{s} \approx 96\frac{kbit}{s} \quad (3)$$

2.6 Přenosová média, individuální vrstva a spojová vrstva

Přenos dat se může u BACnet realizovat prostřednictvím různých sítí. BACnet podporuje technologie LAN, jak je uvedeno na obr. 2-4, stejně jako provolbu přes telefonní síť.



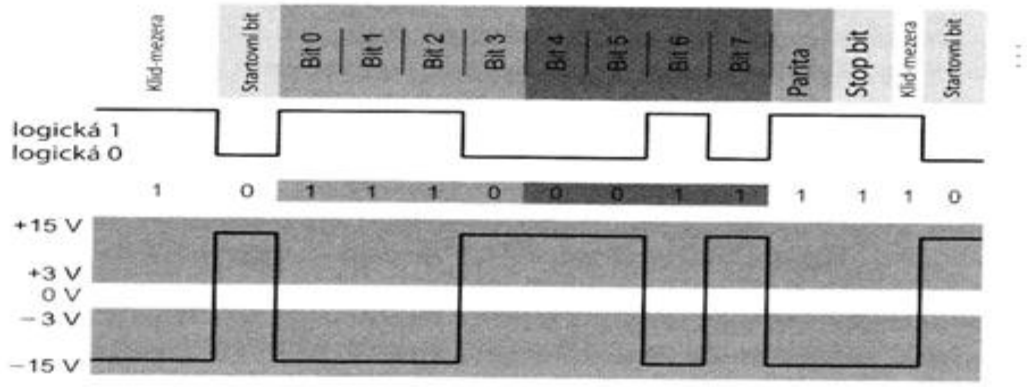
Obr. 2-4 Technologie LAN pro BACnet

Tyto technologie se odlišují svou výkonností, náklady a dostupností přenosových médií, které vedou od jednoduché kroucené dvojlinky přes koaxiální kabel až po vodiče z optických vláken. Při volbě některé z vhodných technologií LAN se řídíme podle následujících kritérií:

- Přenosová rychlost: zde musíme mít na zřeteli, že skutečná průchodnost dat je většinou menší než přenosová rychlost. Důvodem je transport dodatečných informací (adresy, chybová hlášení atd.), které se připojují prostřednictvím komunikačního kanálu protokolu k datovému poli a tím snižují datovou průchodnost.
- Reakční doba: reakční doba udává, jak dlouho trvá od přenosu příkazu do okamžiku provedení akce. Při deterministické technologie přenosu jako např. u Ethernet se tento časový úsek nedá dopředu předvídat, většinou je však zanedbatelně malý.
- Podle účastnických stanic,
- maximální délka vedení,
- náklady. (3)

2.6.1 Master-Slave/Token-Passing(MS/TP), EIA-485, EIA-232

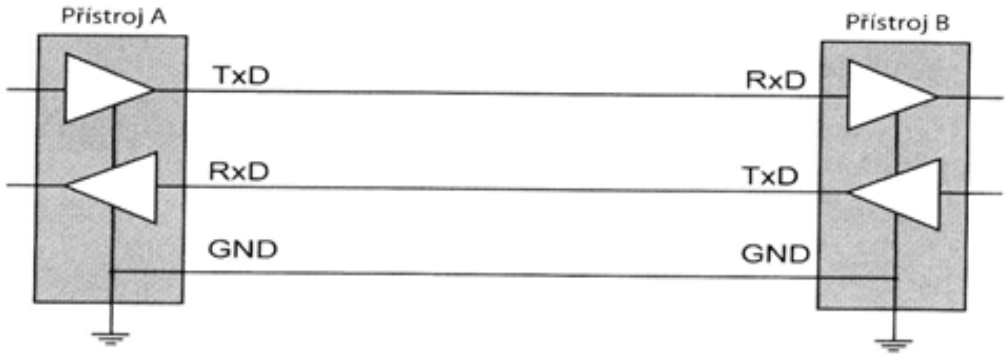
MS/TP nám poskytuje jednoduchou, ekonomicky výhodnou technologii přenosu. Je vhodný zejména pro menší řídící a regulační prvky s nižšími nároky na rychlost přenosu dat. Jako kabelu lze použít stíněné kroucené dvojlinky (UTP) s délkou až 1200 m. Individuální vrstva je založena na standardu EIA-485 (RS-485). Spojení RS-485 představuje sériový datový přenos, tj. bity se dostávají postupně jeden za druhým do přenosového vedení (obr. 2-3).



Obr.2-5 Asynchronní přenos znaků u RS 485 a RS 232. Přiřazení logických stavů k napětí ve vodiči platí jen u RS 232.

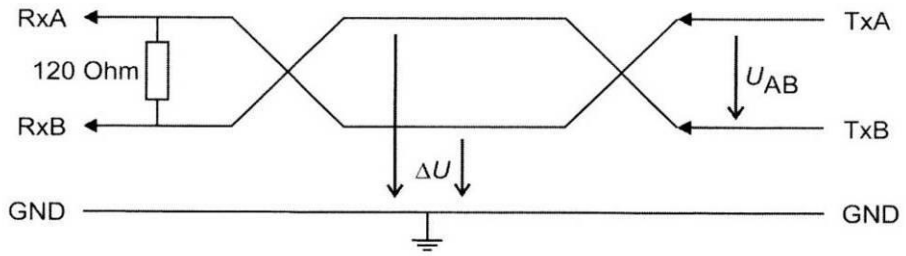
Přenos probíhá po znacích, Jeden znak odpovídá zpravidla 8 bitům. Začátek znaku se označí startovním bitem a na konci pole je zakončovací znak – 1 stop bit, nebo 2 stop bity. (1 stop bit u MS/TP). Časové rozpětí mezi dvěma znaky může být libovolné, tzn. asynchronní datový přenos. U SM/TP je standardní rychlost 9 600 Bd, ale může být i 19 200, 38 400, 76 800 nebo 115 200 Bd, podle toho, jak bude podporována výrobci zařízení. Z důvodů nižších přenosových rychlostí a jednoduchého protokolu je implementace možná i na cenově výhodných mikrokontrolérech – jednočipových počítačích.

Na rozdíl od rozhraní RS-232 známého z PC existují dva výrazné rozdíly: U RS-232 je masově využíváno napěťové rozhraní, tzn., že bity se zpodobňují hladinami napětí, přičemž napětí mezi -3V a -15V je logická jednička, kdežto napětí mezi +3V a +15V představuje logickou nulu. V nejjednodušším případě potřebujeme proto ke spojení mezi dvěma stanicemi při vodiče (obr 2-4).



Obr.2-6 RS 232 se 3 vodiči: TxD (Transit Data), RxD (Receive Data) a GND (Ground)

RS 485 je naproti tomu diferenciální napěťové rozhraní, u něhož se na straně přijímače vyhodnocují napěťové rozdíly (obr. 2-5).

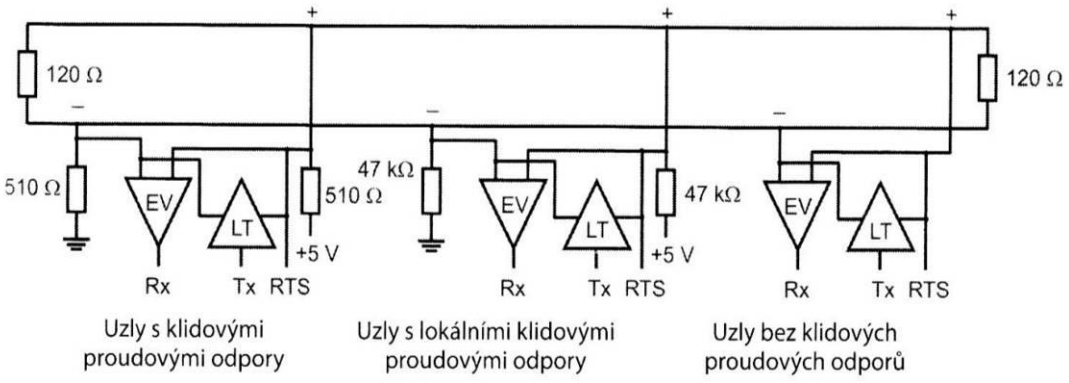


Obr. 2-7 RS 485 se 3 vodiči (poloduplex)

Vysílač vloží napětí U_{AB} = ±3 až 6V mezi vodiče A a B. Kladná hodnota napětí U_{AB} sa nazývá logická jednička, záporná napětí U_{AB} jako logická nula.

U velké délky vodičů a v blízkosti elektrických spotřebičů mohou na kabelu vznikat rušení, která na obou vodičích vedou k navýšení potenciálu ΔU. Napěťová odlišnost U_{AB} zůstává při odolnosti tzv. synchronním rušením pulsů neměnná. To je důvod, proč je rozhraní RS 485 odolnější proti rušení. Umožňuje delší rozvody a využití v průmyslové technice. RS 232 se naproti tomu využívá pro kratší vzdálenosti, většinou do 15 m, s typickými přenosovými rychlostmi 9600 Bd až 115 kBd.

Další odlišností je u rozhraní RS 232 možné napojení na rozhraní tzv. Point-to-Point, neboli plný duplex, který v obou směrech dovoluje současný přenos. U RS 485 je možný jen poloviční duplex, tzn. střídavá výměna vysílání v jednom nebo druhém směru. Proto nabízí RS 485 tzv. Multipoint Bussystem s připojením až 32 účastnických stanic na vedení jak je uvedenou na obr. 2-8.



Obr. 2-8 Síť RS 485 s větším počtem stanic v poloduplexním režimu provozu

Přitom musíme dbát na správné zakončení kabelů. K tomu je zapotřebí umístnit na konec kabelu ohmický odpor, který odpovídá vlnovému odporu vedení. Je to vyžadováno proto, aby se rušivé odrazy datových signálu na konci rozvodů eliminoval.

Když je vedení napájeno elektrickým signálem z vysílače, postupuje tento signál kabelem tzv. postupnou rychlostí (asi 2/3 rychlostí světla) dorazí-li signál na konec kabelu, bude se dokonale odrážet. To je důsledek zákona o zachování energie, protože energie signálu se nemůže ztratit. Odrážený signál se může překrývat s vysílaným signálem a vede k rušení u příjemce. Proto se konce rozvodů musí opatřit odporem, který přijatou energii signálu mění v teplo a zabraňuje tak odrazům. Odpor musí být zvolen tak, aby odpovídal charakteristické impedanci vodičů.

Charakteristická impedance je vlastnost vodiče nezávisle na jeho délce, která se udává jednotkou "Ohm" (Ω). Charakteristická impedance je vztah napětí a proudu elektromagnetické vlny, která dopravuje data vedením. Produktem napětí a proudu je signální energie. Jestliže ukončovací odpor odpovídá impedanci, pak se může přenášet energie bez odrazů a mění se v teplo.

U RS 485 se vedení počítá se systematickou náhodnou chybou neboli s odpory klidového proudu (obr. 2-7). Bez těchto odporů by se diferenciální napětí blížilo k nule, zatímco by žádný vysílač nebyl aktivní. Šumy vedení by mohlo snadno vést k tomu, že by diferenciální napětí kolísalo mezi kladnými a zápornými hodnotami. Připojené stanice by poté začaly mylně vysílat data. Proto je lepší, aby pro fázi klidu byla předávána pevná diference napětí na vedení přes odporovou síť (obr.2-6 rozdělovače napětí +5V - 510Ω ukončovací odpory s 120 Ω - 510 Ω - GND). Jednotlivé účastnické stanice mají povoleno lokální nastevení klidového proudu. Přijímané signály se přitom zesilují vstupním zesilovačem přijímače a vysílaná data se zesilují prostřednictvím vysílače.

Také na spojové vrstvě MS/TP se jednotlivé znaky spojují do rámců. Rámce mají své formáty; v tomto případě je používán následující formát (obr. 2-9).

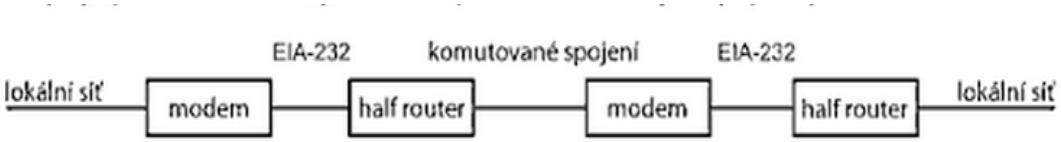
Obr. 2-9 Struktura rámce u MS/TP

Úvodní preambule zahajuje signalizaci rámce. Typ rámce udává, zda se jedná o vysílání dat anebo o řídící informace pro protokol Token-Passing. Adresa odesilatele (Source Address) a adresa příjemce (Destination Address) obsadí vždy po 1 oktetu. Adresa 255 je vyhrazena pro odesílání zprávy všem účastníkům (Broadcast). Zbylých 254 adres mají k dispozici připojené účastnické stanice. Potom následuje údaj o délce 2 oktetů pro datovou část, přičemž může mít přístupovou hodnotu mezi 0 až 501. Rovněž záhlaví rámce stejně jako datová část jsou jištěny vlastním CRC kontrolním součtem.

Spojová (linková) vrstva reguluje rovněž přístup k přenosovému médiu. Při aplikaci Token Passing se jedno oprávnění vysílat (Token) jedné stanice předává stanici druhé. Jakmile jedna stanice obdrží Token („dostane peška“), smí komunikovat s dalšími účastnickými stanicemi. V síti MS/TP se rozlišuje mezi stanicemi typu Master a Slave. Princip spočívá v tom, že jen Master může dostat Token a iniciovat výměnu dat. Stanice typu Slave naproti tomu čekají na dotaz a samy se předávání Token nezúčastní. Jako stanice Master mohou např. fungovat automatizační stanice, na které jsou připojena procesní, provozní a bezpečnostní zařízení (tj. snímače, akční členy) jako Slaves přes MS/TP. U více Masters se musí Token předávat v určitém přesně vymezeném časovém úseku. Po uplynutí čekací doby zase přijde Master na řadu. Proto se tento technologický postup přenosu označuje jako deterministický.(3)

2.6.2 Point-to-Point (PTP)

Dvě kompatibilní zařízení s (Half Router) si mohou spojení v protokolu Point-to-Point (PTP) vyměňovat na bázi RS 232 (obr. 2-10). Budovy, které jsou ve větší vzdálenosti od připojení na inernet, jsou dostupné komutovaným spojem přes modem.



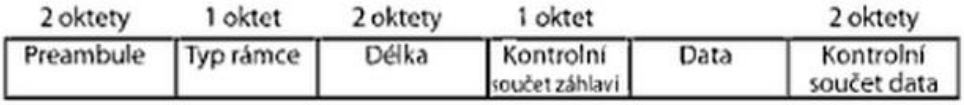
Obr. 2-10 Komutované spojení Point-to-Point se dvěma half routery

Zabývají se protokoly na spojové vrstvě a existujícím spojení vrstvy 1 umožňuje zajištěný přenos dat rámců. Spojení PTP sice umožňuje plný duplex, ale jsou k dispozici pouze dočasně a vykazují nízkou rychlost přenosu.

Zajišťovací mechanizmy jako např. dotazy na heslo zde není stanoveno. Mnohé modemy nabízejí možnost zpětného volání (callback). V případě, že je toto aktivováno, modem se po zavolání odpojí a volá přednastavené číslo zpět. Tím se zabrání tomu, aby neautorizovaný volající nezneužil jiným telefonickým napojením přístupu prostřednictvím modemu. Některé modemy umožňují automatický zpětný (potvrzovací) dotaz kombinovat s automatickým zpětným požadavkem na přístupové heslo.

Hned jak se fyzické spojení ustanoví, vymění se řídící rámce k navázání spojení ve vrstvě 2. Poté se mohou datové rámce přenášet, dokud řídící rámec nevyvolá přerušení spojení, nebo dokud se nepřeruší fyzické spoje. Formát rámce vychází u spojení Point-to-Point pochopitelně bez adres, protože se spojení uskutečňuje jen mezi dvěma stanicem.

Preambule signalizuje začátek rámce (obr. 2-11).



Obr.2-11 Struktura rámce u spojení typu Point-to-Point

Typ rámce udává, zdali se jedná o vysílání dat, nebo řídící informaci. Zvláštností protokolu PTP je, že každý datový rámec se jistí prostřednictvím řídícího rámce. U MS/TP je to v rámci délky datového pole a v záhlaví rámce, stejně jako i u dat se zajišťuje kontrolní součet CRC. (3)

2.7 Přenos přes sběrnici USB

USB (Universal Seriál Bus) je sériová sběrnice, umožňují připojit širokou paletu zařízení k osobnímu počítači. Pomocí USB lze připojit téměř každou periferii, klávesnicí, myší a tiskárnou počínaje a kamerami, čtecími zařízeními a pevnými disky konče. V současné době je nejrozšířenější specifikací USB 2.0. Nově ale již nastupuje USB 3.0. (10)

2.7.1 USB 2.0

Na trhu je i široká nabídka integrovaných obvodů pro použití s USB sběrnicí, od jednoúčelových převodníků (např. USB na RS 232) až po jednočipové mikrokontroléry se zabudovaným USB rozhraním. USB 2.0 specifikace využívá vrstvenou hvězdicovou topologii, kde je v centru každé hvězdice hub. K tomu může být připojen bud další hub (na

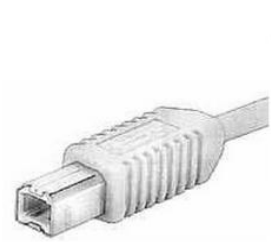
další úrovni) nebo koncové zařízení. USB sběrnice obsahuje jeden tzv. kořenový rozbočovač (Root Hub), který je považován za nejvyšší (první) úroveň a k němu jsou připojeny další huby a zařízení. Rozhraní mezi USB systémem a hostitelským počítačem je nazýváno hostitelský řadič (Host Controller). Tento radič může být implementován hardwarově nebo softwarově. Kořenový rozbočovač je integrován spolu s hostitelským řadičem do hostitelského systému a nabízí nejčastěji dva přípojné body. S ohledem na zpoždění signálu v kabelech a hubech povoluje specifikace maximálně sedm úrovní včetně kořenové vrstvy, tzn. mezi kořenovým rozbočovačem a koncovým zařízením může být zapojeno maximálně pět rozbočovačů. USB sběrnice používá tři rychlosti přenosu dat:

- Low speed – max. 1,5 MBit/s
- Full speed – max 12 MBit/s
- High speed – max 480 MBit/s

USB sběrnice využívá čtyři vodiče. Po dvou vodičích je přenášeno napájecí napětí a zem, a po dalších dvou (pro full/high speed se používá kroucený pár) jsou přenášena odlišně vlastní data. Díky tomu je i při vysokých přenosových rychlostech odolná proti šumu a rušení. (10)

Napájení je zde 5V a 100 mA, případně 500 mA v low/high power módu.

Obr.2-12 Konektor a zásuvka typu A



Obr.2-13 Konektor a zásuvka typu B

2.7.2 USB 3.0

Nová verze slibuje přenosové rychlosti 5 GBit/s (oproti 480 MBit/s u USB 2.0). USB 3.0 používá 8 vodičů a jiný typ konektoru. Pokud bude potřeba připojit zařízení USB 2.0 ke konektoru USB 3.0 na PC bude vše v pořádku, opačně však všechny nové konektory do staršího USB 2.0 připojit nepůjdou. Zpětná kompatibilita je zachována tím, že konektor USB 3.0 obsahuje zachovaný starý konektor USB 2.0, do kterého lze zařízení USB 2.0 i připojit. Obráceně to však již nepůjde u všech konektorů (tab. 2-1). (12)

Parametr	USB 3.0	USB 2.0
Přenosová rychlost	5 Gbit/s	480 Mbit/s
Rozhraní	dual-simplex, čtyři datové vodiče oddělené od USB 2.0	half-duplex, dva datové vodiče
Vodiče	4 pro SuperSpeed, 2 pro ostatní (+ 2 napájení, celkem 8)	2 pro low, full-speed i high speed (+ 2 napájení, celkem 4)
Transakční protokol sběrnice	řízený hostitelem (řadičem) asynchronní packetový tok je směrován	řízený hostitelem (řadičem) dotazovací packetový tok se vysílá na všechna zařízení
Power management	víceúrovňový (idle, sleep, suspend) PM pro připojení, zařízení i funkce	na úrovni odpojení a připojení portu PM pro zařízení
Napájení	jako USB 2.0 s možností 50% zvýšení pro nekonfigurovaná zařízení a 80% pro konfigurovaná	podpora low/high power (100 resp. 500 mA) zařízení
Detekce připojení	hardwarová detekce s přechodem do provozního stavu pro datovou komunikaci	hardwarové detekce připojení portu, softwarový ovladač přepne zařízení do stavu zapnuto (může začít datový přenos)
Typy dat. přenosu	jako USB 2.0 se SuperSpeed omezením (viz dále)	čtyři typy: control, bulk, interrupt a isochronous

Tab.2-1 Srovnání některých parametrů USB 3.0 a USB 2.0

2.8 Přenos přes Bluetooth

Bluetooth je lokální otevřený standard pro bezdrátovou komunikaci propojující dvě a více elektronických zařízení. Vytvořen byl v roce 1994 firmou Ericsson jako náhrada za sériové drátové rozhraní RS 232.

Technologie Bluetooth je definována standardem IEEE 802.15.1. Spadá do kategorie osobních počítačových sítí, tzv. PAN (Personal Area Network). Vyskytuje se v několika verzíchz nichž v současnosti nejvíce využívaná je verze 2.0 a je implementována ve většině zařízení. Nová verze rozhraní Bluetooth 4.0 (2011), u kterého je větší dosah (100 m), menší spotřeba elektrické energie a také podpora šifrování AES – 128.

Specifikace Bluetooth 2.0 EDR (Enhanced Data-Rate) zavádí novou modulační techniku, díky níž dosahuje větší vydrže baterií, protože samotné navázaní spojení i přenos probíhá v kratší době než u starších verzí (Bluetooth 1.2).

Class	Maximální povolený výkon		Dosah (přibližný)
	mW	dBm	
Class 1	100	20	~100 metrů
Class 2	2.5	4	~10 metrů
Class 3	1	0	~1 metr

Tab.2-2 Zařízení rozdělené podle výkonnosti

Verze	Rychlost přenosu dat	Maximální propustnost
Verze 1.2	1 Mbit/s	0.7 Mbit/s
Verze 2.0 + EDR	3 Mbit/s	1.4 Mbit/s
Verze 3.0 + HS	24 Mbit/s	
Verze 4.0	24 Mbit/s	

Tab.2-3 Přenosové rychlosti podle standardů

Bluetooth pracuje v pásmu 2,4 GHz (stejné jako Wi-Fi). K přenosu využívá metody FHSS(Frequency hopping sprej spektrum), kdy během jedné sekundy je provedeno 1600 skoku (přeladění) mezi 79 frekvencemi s rozestupem 1 MHz. To zvyšuje odolnost spojení proti rušení na stejné frekvenci. Výkonové úrovně (1 mW, 2,5 mW a 100 mW) s nimiž lze komunikovat do vzdálenosti cca 10-100 m. Udávané hodnoty platí pouze na volném prostoru. Pokud jsou mezi zařízeními překážky (např. zdi), dosah rychle klesá. Většinou nedochází ke skokové ztrátě spojení, ale postupně se zvyšuje počet chybně přenesených paketů. (11)

2.8.1 Protokol FRCOMM

Rádiofrekvenční komunikace (RFCOMM) je náhrada kabelového protokolu, který slouží k vytvoření virtuálního sériového datového toku. RFCOMM poskytuje binární přenos dat a emuluje EIA-232 (dříve RS-232) řídící signály ve vrstvě Bluetooth pásma. RFCOMM nabízí jednoduchý spolehlivý datový proud k uživateli, podobně jako TCP protokol. Používá se na mnoha telefonních profilech jako nosič pro AT příkazy, stejně jako transportní vrstva pro OBEX přes Bluetooth. Mnoho aplikací používá Bluetooth RFCOMM pro jeho širokou podporu a veřejné dostupné API na většině operačních

systémech. Kromě toho mhou aplikace, které používají sériový port pro komunikaci, použití RFCOMM. (11)

2.9 Sběrnice IEEE 1394

FireWire má dva základní standardy. Nejdůležitější vlastnosti sběrnice IEEE 1394 je v její původní variantě 1394a a v novější 1394b. Hlavními přednostmi sběrnice 1394 je použití v průmyslu. Přenosová rychlost dovoluje sbírat obrazovou informaci, kterou lze přenášet spolu se vstupy a výstupy a daty pro řízení (motion kontrol). Kamera zapojená do regulačního obvodu umožňuje řízení na základě vizuálně získaných informací. Synchronizace taktu jednolivých uzlů umožňuje velmi přesně řídit (časová nejistota je menší než 500 ps). Asynchronní přenos jako metoda zajištující informaci o úspěšném přenosu kritických nebo dat citlivých z hlediska bezpečnosti či důvodu neúspěchu přenosu. Nemá žádná omezení topologie sítě s komponentami podle specifikace 1394b. Možné jsou jak stromové, tak kruhové architektury. Všechny uzly jsou si rovnocenné (každý může komunikovat s každým). Na centrální řízení nejsou kladeny nereálné časové požadavky a zcela k němu postačuje běžné PC. Nevýhodou sběrnice 1394 je nedostatečná propustnost dat do kancelářských sítí (výhodné jen pro poměrně malé oblasti řídících úloh). V průmyslu přichází v úvahu pouze standard 1394b(důvodem je max.délka kabelu 4,5 m u standardu 1394a), pro který je na trhu zatím jen omezené množství obvodů(v posledním roce však došlo k výraznému zlepšení – firmy Oxford Semiconductor, Agere Systems). Při délce kabelu 100 m a rychlosti přenosu 100 Mb/s jsou u FireWire počet účastníků a popř. množství dal silně omezeny pevnou délkou cyklu 125 μs; Ethernet je v tomto případě mnohem mnohem flexibilnější a levnější. Při využití komponent reálného času pouze v malé míře je cenově výhodnější použití sběrnice Ethernet Powerlink. Někteří uživatelé jsou příliš fixováni na Ethernet a ke sběrnici IEEE 1394 zaujímají odmítavý postoj. (13)

2.9.1 Sběrnice IEEE 1394a alias FireWire 400

Rychlost přenosu 100, 200 a 400 MB/s (S100, S200 …), která se řídí podle nejpomalejšího přístroje. Používá čtyř nebo šesti žilový kabel (2x2 žíly pro TPA a TPB; 2x2 žíly pro TPA a TPB + 2 žíly pro napájení). Provedení kabelu je pouze stíněný kroucený pár vodičů (STP). Vzdálenost mezi sousedícím přístroji závisí na rychlosti sběrnice (např. 4,5 m při S400, 14 m při S200 atd.). Přenos TCP/IP přes 1394 je možný (u počítačů Mac jako

standard). Topologie je stromová, kruhové struktury jsou vyloučeny; koncová zařízení na sběrnici nevyžadují terminátory). Přenos dat je obousměrný, prostřednictvím paketů, izochronní mód k práci je v reálném čase a asynchronní mód je peer-to-peer. Délka sběrnice při zřetězení je maximálně 72 m (daisy chain). Počet uzlů v segmentu je až 63 (při řetězení do 16 na jedno místo řetězce). Počet segmentů v systému až 1023 (pospojovaných můstky). Řízení typu multimaster (1 až 63 řídících uzlů). Provozu je hot-plug (přístroje lze připojovat za chodu). Má vlastní automatickou identifikaci a adresaci přístrojů. Napájení po sběrnici 8 až 33V DC; 1,5 A, max. 48W. (13)

2.9.2 Sběrnice IEEE 1394b alias FireWire 800

Rychlost přenosu je 800, 1600 nebo 3200 Mb/s (S800, …). Využívá devítikilový kabel, nové konektory (2 žíly navíc: vedle TPx+ a TPx- vede také TPx zemnící a jeden kolík je nezapojen). Vedle krouceného páru (STP) lze použít také nestíněný kroucený pár (UTP), plastové optické vlákno, oplášťované polymerové vlákno (HCPF) nebo několikavidové vlákno. Vzdálenosti mezi sousedícími přístroji je podstatně větší, zavisí na kabelu (např. 100 m při S100 a UTP). Přenos TCP/IP je vlastnostmi blízké gigabitovému Ethernetu. Topologie je stromová, kruhové struktury jsou dovoleny. (13)

2.10 Ethernet

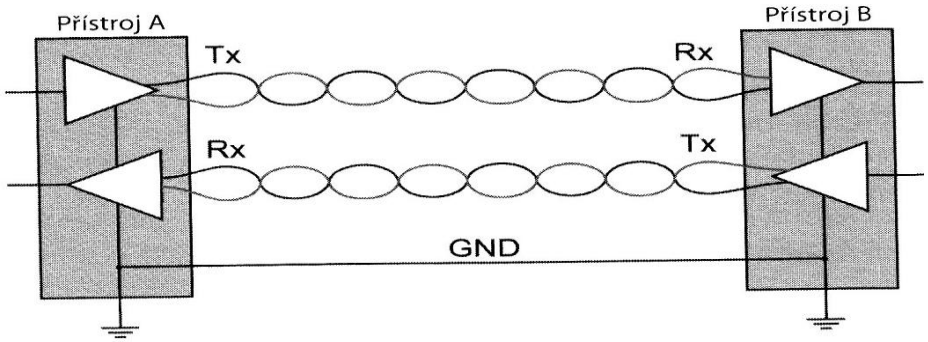
V případě Ethernetu se jedná o nejrozšířenější technologii LAN, jež byla původně zaměřena na komunikaci mezi jednotlivými kancelářemi a postupně se široce uplatnila v oblastech průmyslových aplikací a dálkových dopravních a komunikačních spojů. Kancelářské a průmyslové budovy jsou dnes Ethernetem průběžně zasíťovány, takže jeho využití v automatizaci budov je logickým důsledkem současného vývoje.

Ethernet zahrnuje pouze vrstvy 1 a 2 modelu OSI, vyššími protokoly jsou přednostně TCP/IP pro komunikaci mezi kancelářemi a pro automatizaci budov. Ethernet byl vyvinut již v 70. letech minulého století jako norma – Standard IEEE-802.3. V průběhu dalších let prošel Ethernet dalším rozvojem, což vedlo i k podstatnému několikanásobnému zvyšení přenosové rychlosti (10 Mbit/s, 100 Mbit/s, 1 Gbit/s, 10 Gbit/s) při stálém rozšiřování kompatibility. K tomu patří též zpřístupnění výkonných přenosových médií, jako jsou světlovaná vlákna, optické kabely atd. Také přenosové technologie, jako Wireless LAN, představují rozšíření oproti původnímu Ethernetu. (3)

2.10.1 Přenos koucenou dvojlinkou Twisted Pair

Twisted Pair

Pod pojmem Twiste Pair se rozumí měděný kabel s více zkroucenými páry vodičů, které vynikají jednoduchou instalací do zásuvek a nízkými náklady. V nejjednodušším případě potřebujeme dva páry (4 žíly) pro přenos signálu. Jeden pár slouží k vysílání (Tx), druhý k příjmu (Rx) (obr. 2-14).



Obr. 2-14 Zkroucené vodiče k přenosu dat (Twisted Pair)

Zkroucení páru vodičů redukuje možná rušení elektromagnetickými poli, které u sousedních vodících párů anebo v blízkosti kabelů působí. Dodatečně lze vybavit páry vodičů metalickým stíněním, anebo kabel může být stíněn celkově. Výběr vhodného kabelu závisí na požadavcích pro datový přenos. Zpravidla platí, že vyšší přenosové rychlosti digitálního signálu odpovídají vyššímu počtu obsažených frekvenčních komponent. To má za následek útlum a přeslechy mezi vodiči.

Jako útlum chápeme snížení energie signálu na cestě od odesilatele k příjemci. Příčinou jsou ohmické ztráty v metalickém vodiči a dielektrické ztráty v izolačním materiálu. Obojí druhy ztrát rostou s rostoucím kmitočtem, takže maximální povolená délka kabelů se snižuje v závislosti na rostoucí rychlosti přenosu.

Přeslechem rozumíme nežádoucí přenos signálu od jednoho páru vodičů k druhému, který může probíhat po celé délce kabelu. Příčinou jsou kapacitní a indukční vazby mezi sousedními páry při překrývání elektrických a magnetických polí. Také tento efekt vzrůstá s vyšší frekvencí, což vyžaduje odstínění pro každý jednotlivý pár vodičů. Útlum a přeslechy tak omezují maximální možnou kapacitu přenosu. (3)

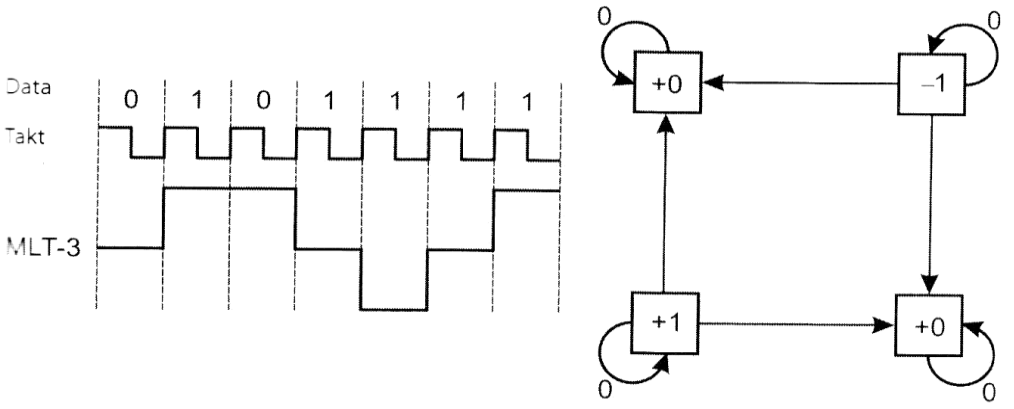
2.10.2 Varianty přenosu 100Base-TX, 1000Base-T

Hodnoty pro nejčastější aplikace Ethernetu jsou uvedeny v tab. 2-4.

Označení	Rychlost	Maximání délka vedení
100Base-FX	100 Mbit/s	100 m
1000Base-SX	1 Gbit/s	100 m

Tab.2-4 Varianty Ethernetu s Twisted Pair

100Base-Tx se často označuje jako „Rychlý Ethernet“ (Fast Ethernet), protože je desetkrát rychlejší než dříve obvyklý standardní 10Base-T-Standard. Enormního nárůstu rychlosti přenosu ve srovnání s 10Base-T bylo dosaženo zvláštním použitím speciální technologie přenosu, nazývané MLT-3 (Mulit Level Transmission). Jedná se o tříhodnotový přenos, tzn. že existují 3 možné symboly (-1,0.+1) nebo výstupní stavy vysílače (obr. 2-15).



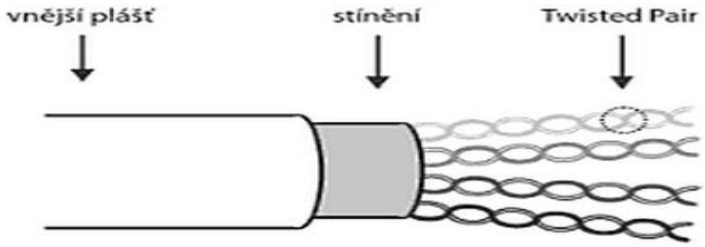
Obr. 2-15 Přenos MLT-3 (příklad signálu a stavový diagram)

U stavu logické 0 zůstává výstupní signál na předchozí hladině signálu, zatímco pro logické 1 se hladina signálu mění směrem nahoru nebo dolů podle stavového diagramu. Výhodou je, že napěťová hladina mění vždy jen málo (není to jednorázový skok od +1 na -1) a frekvence v signálu jsou relativně nízké. Nižší frekvence jsou výhodnější, neboť se jak útlum, tak přeslechy mezi sousedícími vodiči zmenšují. Proto můžeme u Fast Ethernetu pracovat bezpečně s délkou kabelů do 100 m.

Obvykle jsou kabely z osmi žil, z nichž vždy 4 se používají. (2 žíly pro Tx, 2 žíly pro Rx). Zbývající žíly se mohou využít jiným způsobem, např. k přenosu telefonního signálu (cable sparing). Gigabitový Ethernet využívá všech 8 žil a proto se od další možnosti využití upouští, protože je rozšířenější.

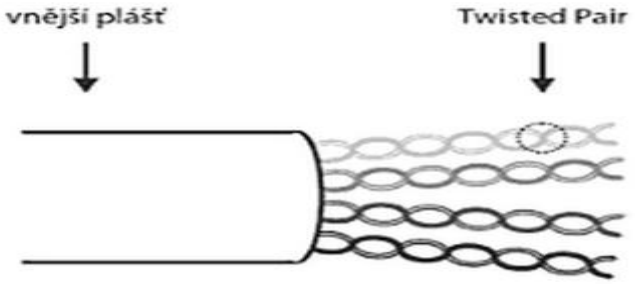
Při výběru kabelu je možno použít klasifikace podel EIA/TIA-568 (Electronic Industries Association/Telecommunication Industry Association). V této klasifikaci se popisují určité třídy aplikace a vlastnosti kabelů. Pro Fast Ethernet jsou vhodné kabely kategorie 5, které splňují kritéria minimálního útlumu, šumu a přeslechů.

Kabel s celkovým stíněním se označuje jako Screened Twisted Pair (ScTP)(obr.2-16).



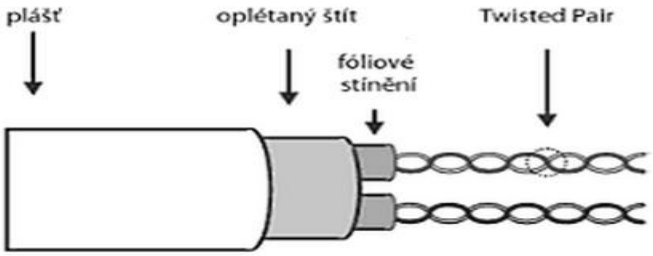
Obr. 2-16 Stíněný TP – Screened Twisted Pair

Celkové stínění redukuje jak rušení signály přicházejícími z vnějšího prostředí, tak i nežádoucí vyzařování energie signálu. Dalším typem jsou nestíněné kabely (Unshielded Twisted Pair - UTP obr. 2-17).



Obr.2-17 Nestíněný TP – Unshielded Twisted Pair

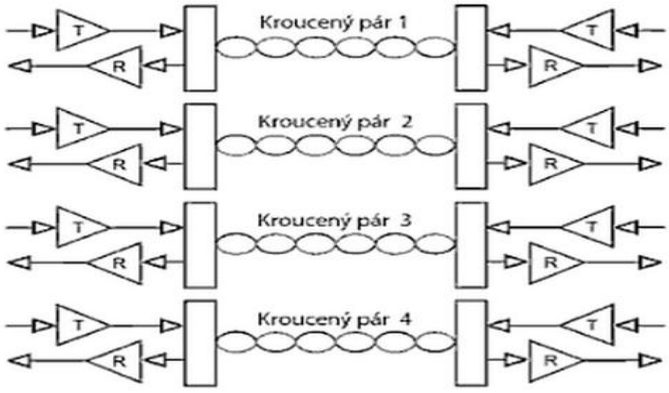
Výhoda UTP oproti ScTP je v nižší ceně a menším průměru, což usnadňuje pokládání vedení. Technicky nejlepší variantou pro kvalitní přenos je párový stíněný kabel s dodatečným celkovým opláštěním, označovaný STP (Shielded Twisted Pair, někdy SSTP jako Screened Shielded Twisted Pair – obr. 2-18).



Obr. 2-18 Screened Shielded Twisted Pair

Zde je ochrana nejen proti citlivosti proti rušení a šumu na signálech, které přicházení zvenčí, ale i proti vzájemnému rušení sousedících párů. Vzhledem k vyšším nákladům a obtížnější montáži konektorů se však tato varianta kabelů používá méně často.

V době rozvoje Ethernetu se při přechodu na vyšší rychlosti přenosu dat zvyšovaly i požadavky na používané kabely, což vedlo k vývoji několika kategorií a nejvíce se to odrazilo u kategorií 6 a 7. S 1000Base-T je ještě stále možné kabel kategorie 5, resp. 5e, použít pro přenos až 1 Gbit/s, ale pouze na vzdálenost do 100 m. Aby se omezilo frekvenční spektrum a tím se i šumy, útlum a přeslechy udržely v rozumných hranicích se používá čtyř párů žil současně a tím se redukuje přenosová rychlost na pár na 250 Mbit/s. Data protékají páry současně v obou směrech (bidirectional), takže se musí speciální technikou (Hybrid) opět rozdělit (obr. 2-19).



Obr. 2-19 Využití všech 4 kroucených párů vodičů u přenosu 1000Base-T

Současně se při 1000Base-T používá pěti symbolů (signálních stupňů) a tím se může rychlost kroku ještě dále zredukovat. Dodatečné zvýšení rychlosti nad 1 Gbit/s je možné pouze za použití lepších kabelů. Takto byl vypracován standard pro přenosovou rychlost 10 Gbit/s pro přenos po Twisted Pair.(3)

2.10.3 Kategorií kabelů v LAN podle výkonnosti

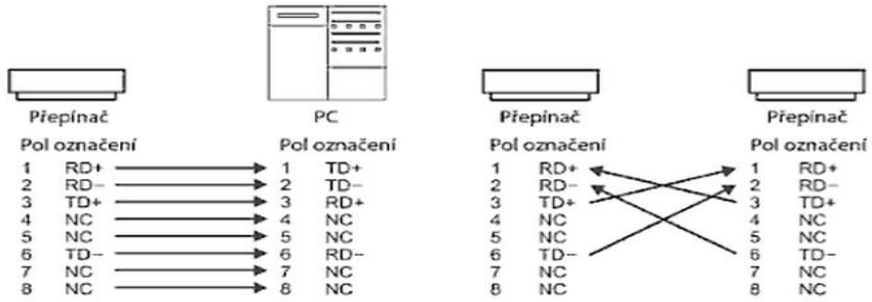
- Kategorie 5 (Cat. 5) – od roku 1995, nahrazena 5E, max. přenosová rychlost byla 100 MB/s (tzv. Fast Ethernet, protokol 100Base-T)
- Katerogie 5E (Cat. 5E) – vychází z kat. 5, šířka pásma 100 MHz, cenově dostupná a hodně rozšířená, max. přenosová rychlost 1GB/s (protokol 1000Base-T)
- Kategorie 6 (Cat. 6) – od roku 2002, šířka pásma až 250 MHz, spolehlivější než 5E, přenosová rychlost 1GB/s a více (protokoly 1000Base-TX, 10GBase-T)
- Kategorie 6A (Cat.6A) – od roku 2008, plnohodnotný přenos protokolu 10GBase-T na všechny vzdálenosti, rychlost 10GB/s v metalické kabeláži, šířka pásma 500 MHz,
- Kategorie 7 (Cat.7) – od roku 2002, schválený pouze kabel a ne pro spojovací hardware (zásuvky, patch panely atd.), šířka pásma 600 MHz,
- Kategorie 7A (Cat.7a) – rozšíření kategorie 6A a zdvojnásobení šířky pásma na 1000 MHz (15)

2.10.4 Auto-Negotiation, Auto-Sensing a Powe-over-Ethernet

Pro různé varianty přenosu se používá mnoho různých síťových karet a síťových komponent. Na druhé straně se stává, že se používají starší typy zařízení, které dovolují použít jen Standardu 10 Mbit/s 10Base-T. Aby se uživateli usnadnilo stále obtížnější vylaďování nutných standardů, byla vyvinuta technologie stanovení a generování parametrů konektivy; Auto-Negotion.

Po instalaci kabelového spoje mezi dvěma stanicemi se v pravidelných intervalech odešlou tzv. linkové pulsy (Link Pulse). Původně sloužily jen ke zjištění a potvrzení komunikačního partnera na protější straně spoje. Rozšíření na tzv. Normal Link Pulse, kdy se ve skupině vysílá více pulsů, umožnilo výměnu informací. Tím se mohou spojené účastnické stanice – každá podle svých možností – vyladit na optimální společné parametry přenosu (rychlost, plný duplex, poloduplex). Pokud je to požadováno, může se tento automatický postup přepsat v každém zařízení manuálním nastavením. Nové síťové komponenty často ovládají automatickou identifikaci a zohlednění typů kabelů (Auto-

Sensing). Přímo vedené nekroucené kabely (straight-through) se používají ke spojení mezi síťovými kartami a síťovými komponentami, jako např. Switch (obr. 2-20).



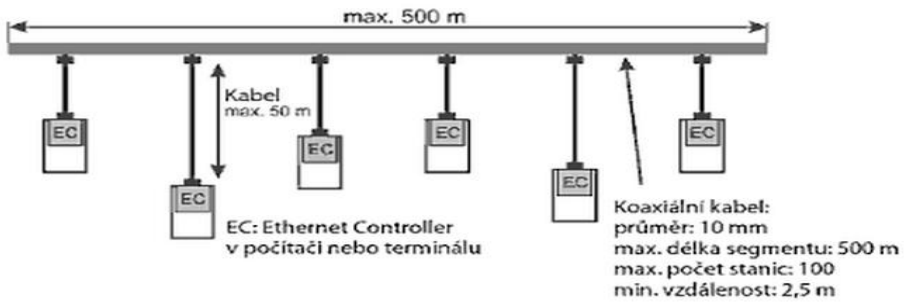
Obr. 2-20 Straight-through (nalevo) a Cross-over kabely (napravo)

Kolíky konektorů jsou se žilami spojeny v poměru 1:1. Díky tomu pak odesílají signál (TD+, TD-) vždy odpovídá příjimanému vstupnímu signálu (RD+, RD-) protější strany. Při spojení stanic stejného druhu – síťová karta k síťové kartě, přepínač k přepínači (Switch to Switch) je zapotřebí crossover kabel (Crossover Patch Cable), aby se mohl odesílatel vždy spojit s odpovídajícím příjemcem. Při aplikaci Auto-Sensing, vzhledem k automatickému nastavení, nehraje již použitý typ kabelu žádnou roli.

Kabelem Twisted Pair se může současně přivádět napájení pro připojené zařízení. Protože tenot postup, označovaný Power-over-Ethernet, nepotřebuje samostatné napájení, redukuje požadavky na kabely a potřebu místa. Umožňuje rovněž sepnutí a vypnutí na dálku. Komponenty sítě jako přepínače (Switches) se dodávají převážně s funkcionalitou Power-over-Ethernt a umožňuje připojit zařízení ve výkonovém rozsahu přibližně do 10 W. Přitom se může k napájení používat neobsazených žil (např. při aplikaci Fast Ethernet), nebo superponovat s datovými signály o stejném napětí. (3)

2.11 Síťové prvky opakovač (repeater), most (bridge), rozbočovač (hub) a přepínač (switch)

Původní varianta Ethenetu se stávala z koaxiálního kabelu, na který se připojovaly všechny stanice lokální sítě (obr. 2-21).



Obr.2-21 Původní varianta Ethernetu (10Base5) s koaxiálním kabelem

Účastnická stanice může vysílat svá data, pokud žádná jiná stanice neobsadila přenosové médium. Při menším vytížením vytížení sítě mohou nastavit nahodilé kolize, jestliže 2 stanice ve stejném okamžiku začnou přenášet data. Je jasné, že pak nastane vzájemné rušení a interference obou vysílání.

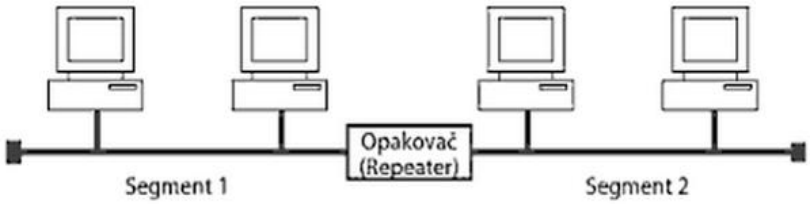
Síťové karty „odposlouchávají“ stále své vlastní vysílání, a ta je možno zjistit, kdy dochází ke kolizi a kdy je třeba přenos přerušit. Po náhodně zvoleném intervalu se předešlé kolidující rámce znovu přenášejí. Tento postup, označovaný jako CSMA/CD (Carrier Sense Mulitple Access/Collision Detection), funguje při menším vytížení sítě velmi dobře, při vyšším vytížení může větší počet kolizí vést k výpadku sítě.

Z toho důvodu se Ethernet a prvky, které k němu přísluší, vyvíjely tak, že dnešní kabelové propojené lokální sítě zpravidla již CSMA/CD nepoužívají, ale pracují na základě spojená Point-to-Point, v plném duplexním režimu na základě využití přepínačů (Switches).

Kromě toho přežívá postup CSMA u Wirelles LAN, kde je přenosovým médiem ovzduší, jako tzv. sdílené přenosové přestředí (Shared Medium) a je využíváno větším počtem stanic, takže kolize se mohou opět vyskytnout. (3)

2.11.1 Opakovač (Repeater)

Maximální geometrická rozloha síťových segmentů závisí kromě jiného na útlumu elektrického signálu na vedení. K zesílení se vestavuje mezi 2 segmenty opakovač – repeater. Tím se zvětší síť (obr. 2-22).



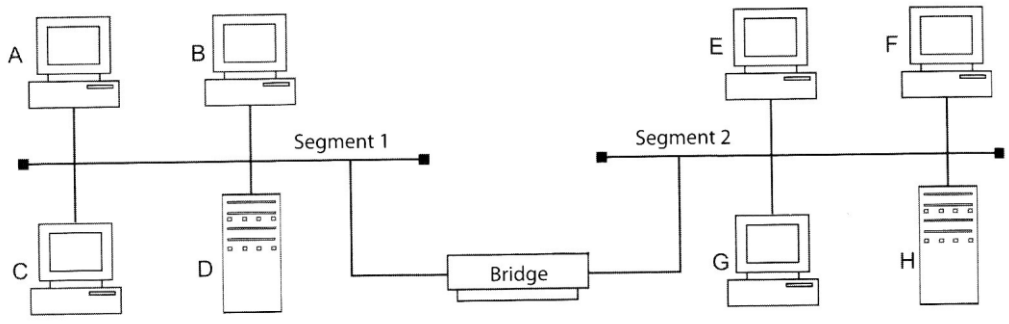
Obr.2-22 Segmenty a repeater

Jako opakovač (Repeater) se označuje taková komponenta vrstvy 1, která zpracovává pouze elektrické signály, ale nemůže vyhodnotit bity nebo obsah rámce. Nevýhodou tohoto řešení je zesílení každého signálu. Také výměna dat mezi dvěma stanicemi se ve stejném síťovém segmentu se přenáší dál, na všechny segmenty připojené na repeater, ačkoliv by to nebylo nutné.

To vede k nežádoucí zátěži segmentů datovým přenosem a omezuje tím maximální možný počet stanic v celé síti. Ne vždy musí vést ke kolizím mezi dvěma stanicemi ve stejném segmentu (Local Collision), ale může postihnout i jiné segmenty (Remonte Collision), protože repeater všechny příchozí signály předává dál. Proto se označují všechny segmenty spojené repeaterem jako kolizní domény. (3)

2.11.2 Most (Bridge)

K rozdělení sítě do menších kolizních domén slouží most (bridge), což je zařízení, které je modelu OSI začleněno do vrstvy 2. Most (bridge) spojuje dva síťové segmenty dohromady a rozhoduje o převedení došlých datových rámců do dalšího segmentu (obr. 2-23)



Obr. 2-23 Segmenty a jeden most (bridge)

Přenos se uskuteční jen tehdy, jestliže příjemce se nachází v jiném segmentu. Proto musí být most vybaven tabulkou adres, v níž jsou uvedeny adresy MAC připojených stanic

s příslušným přidělením do segmentu. Tato tabulka se při zapojení bridge v průběhu času automaticky naplní, bez zásahu administrátora zvenčí (tab. 2-5).

Akce počítače	Akce mostu (bridge)	seznam Segmentu 1	seznam Segmentu 2
A odesílá rámce do B	A se zaznamená do seznamu Segmentu 1, rámec se rovněž odešle do Segmentu 2	A	–
B odpovídá A	B se zaznamená do seznamu Segmentu 1, rámec se neodešle do Segmentu 2	A, B	–
B odesílá rámec do G	Rámec se vyšle také do Segmentu 2	A, B	–
G odpovídá B	G se zaznamená do seznamu Segmentu 2, rámec se rovněž odešle do Segmentu 1	A, B	G
F odesílá rámec do E	F se zaznamená do seznamu Segmentu 2, rámec se rovněž odešle do Segmentu 1	A, B	G, F
E odpovídá F	E se zaznamená do seznamu Segmentu 2, rámec se neodešle do Segmentu 1	A, B	G, F, E

Tab. 2-5 Struktura tabulky adres (Seznam Segmentu 1,2) v mostu (Bridge) po novém startu

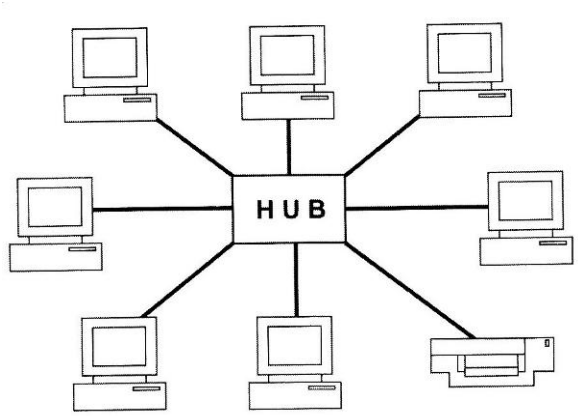
Jakmile datový rámec dorazí do bridge, zanesou se adresy MAC odesilatele a připojení (port), přes něž je napojen, do tabulky adres. Potom most testuje, zdali se adresa MAC příjemce již nachází v tabulce adres. Pokud ano, tak se datový rámec předá na další port, pokud se příjemce nachází v segmentu, který jen a tento port připojený. V opačném případě je datový rámec odmítnut. Pokud ještě žádný záznam adresyx neexistuje, pak se pro jistotu datový rámec předá také na jiný port.

Zvláštnost představují rámce Broadcast. Předávají se vždy z mostu dál, neboť jsou směrovány na všechny stanice v síti. Segmenty sítě, které jsou takto připojeny přes most, nazývají domény Broadcast (Broadcast Domains). (3)

2.11.3 Rozbočovač (Hub)

Původní sítě Ethernet s koaxiálními kabely byly buď poměrně poruchové (přerušení kabelů sběrnice ochromilo síťový segment), anebose značně prodražily při používání speciálního transceiveru pro větvení signálu ze sběrnice. Z toho důvodu byly vyvinuty hvězdicové sítě a koaxiální kabely byly nahrazeny výhodnější kroucenou dvojlinkou (Twisted Pair). Uprostřed sítě bylo nutné umístnit centrální síťový uzel – tzv. rozbočovač (hub).

Funkci rozbočovače (hub) je možno charakterizovat i pojmem Multipoint Repeater – tzn. „mnohonásobný opakovač“. Jedná se o zařízení vrstvy 1, které na jakýkoliv přípoj sítě vysílá zesílené signály a k dalším připojovacím portům. Signály jsou zesíleny a jsou dále vedeny (kopírovány) na všechny ostatní přípoje. Hub a s ním spojené počítače vytvářejí jednou velkou kolizní doménu (obr. 2-24).

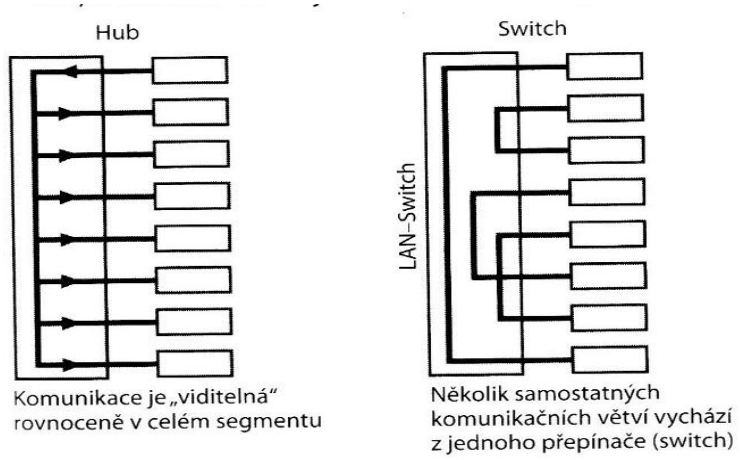


Obr. 2-24 Topologie s rozbočovačem (Hub)

Namísto počítače může být rozbočovač (hub) připojen na jiné rozbočovače (hubs), tak aby měl počítač další spojení volně k dispozici. Všechny připojené stanice musí sdílet šíři pásma, tj. při 100 Mbit/s a 100 účastnících při stejném, rovnocenném přidělování, připadne na každou účastnickou stanici 1 Mbit/s, což se ale z důvodů kolizí ještě sníží. (3)

2.11.4 Přepínač (Switch)

Podobně jako most (bridge) slouží přepínač (switch) k zvýšení výkonnosti aplikací Ethernet-LAN, u nichž se realizuje rozdělení na větší počet kolizních domén (obr.2-21).



Obr. 2-25 Srovnání mezi rozbočovačem (hub nalevo) a přepínačem (switch napravo)

Takto se množství dat v jednotlivých segmentech zredukuje a využitelné rozpětí se zvýší. Switch se může opět označit jako Multiport Bridge, tj. „vícenásobný most“ a v modelu OSI je přiřazen vrstvě 2. Přijímá na svých portech (přípojkách) vstupní rámce a přenáší je na odpovídající výstupy. Na rozdíl od hubu dosahuje switch cíleného přenosu, tj. prověřuje na

základě tabulky adres, na který výstup musí rámec dodat. Adresní tabulka je stejná jako u mostu (Bridge) a je v průběhu času automaticky doplňována.

Při použití switche s 10 přípojkami po 100 Mbit/s by to v ideálním případě umožňovalo při připojení 5 stanic současnou vzájemnou výměnu dat. Úhrnná rychlost přenosu dat by byla 100 Mbit/s x 5 = 500 Mbit/s, což je 5x rychlejší přenos dat ve srovnání s rozbočovačem (hubem). Pokud připojíme na jednom konektoru switche jen jeden počítač a žádný další hub, pak v tomto mikrosegmentu může být přepojen režim z poloduplexního na plně duplexní. Tím se ještě přenosové rychlosti zdvojnásobí. V tomto uvedeném příkladě by musel switch pracovat se standardní přenosovou rychlostí 1 Gbit/s, aby při plném vytížení nedocházelo ke ztrátám rámců.

V praxi se vyskytuje málokdy rovnocenné rozdělení přenášených datových objemů mezi přípojkami jednoho přepínače (switche). Nejčastěji je připojeno několik pracovních PC k jednomu serveru nebo i k více serverům. Pro PC na pracovním místě jsou k dispozici připojení s kapacitou 100 Mbit/s, zatímco server je připojen na switch s kapacitou 1 Gbit/s.

Přípoje jednoho přepínače (switche) jsou zpravidla kompatibilní směrem dolů. Dohoda o rychlosti a režimu provozu (plný duplex nebo poloduplex) probíhá automaticky (Auto Negotiation). V budovách bývají požadavky na přenosovou rychlost nižší a Ethernet s přenosovou rychlostí 10 Mbit/s by většinou stačil. Při smíšeném provozu s aplikacemi IT, VoIP a eventuelně se záznamem přenosu pohybu osob by se však velmi rychle dostal na horní hranici zátěže LAN. Řízení sítí (Network Managment) s dozorem nad jednotlivými komponentami a nad jejím vytížením je v tomto případě možno aplikovat, pokud budeme znát a respektovat úzká místa. Protože Ethernet není žádný deterministický protokol, v případě přetížení vydá v krátkém čase zprávu a datové rámce z přetížených komponent může odmítnout. Pak se mohou vyskytnout ojedinělé a obtížně identifikovatelné chyby. S ohledem na toho riziko je třeba síť Ethernt LAN projektovat vždy s nějakou rezervou. (3)

2.12 Rádiový bezdrátový přenos (Wireless –WLAN)

Většina sítí Ethernet aplikovaných v automatizaci budov je založen na spojení optickými vlákny. Wireless Local Area Network (WLAN) je někdy jedinou možností jak se vyhnout ukládání kabelů, např. v památkově chráněných historických budovách, nebo když jsou propojované budovy od sebe příliš daleko. Přenos WLAN je transparentní, tzn., že uživatel

většinou nepozná žádný rozdíl ve srovnání s propojením rozvodnou sítí. Spolehlivost, stejně jako ochrana proti rušení a odposlechu, jsou však u WLANu zásadně nižší. Wi-Fi je standard pro lokální sítě bezdrátové sítě (Wireless LAN, WLAN) a vychází ze specifikace IEEE 802. V tabulce 2-6 jsou uvedny známé standardní parametry podle IEEE (Institute of Electrical and Electronic Engineers).(3) (17) (14)

Označení	Rychlost	Frekvenční pásmo	Rok
802.11b	do 11 Mbit/s	2,4 GHz	1999
802.11g	do 54 Mbit/s	2,4 GHz	2002
802.11a	do 54 Mbit/s	5 GHz	2002
802.11n	do 540 Mbit/s	5 GHz	2007
802.11ac	do 1,3 Gbit/s	5 GHz	2012

Tab.2-6 Přehled standardů IEEE 802.11 WLAN

Původním cílem Wi-fi bylo zajišťovat vzájemné propojení přenosových zařízení a dále jejich připojování na LAN. S postupem času začala být využívána i k bezdrátovému připojení do sítě Internet v rámci rozsáhlejších lokalit a tzv. hotspotů . Úspěch Wi-Fi přineslo využívání bezlicenčního pásma 2,4 a 5 GHz. (20)

Bezdrátové sítí podléhají stejnému rozdělení jako sítě kabelové:

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)
- Personal Area Network (PAN)

2.12.1 Struktura bezdrátové sítě

Bezdrátová síť může být vybudována různými způsoby v závislosti na požadované funkci. Vždy hraje klíčovou roli identifikátor SSID (Service Set Indentifier), což je řetězec až 32 ACSII znaků, kterými se jednotlivé sítě rozlišují. SSID identifikátor je v pravidelných intervalech vysílán jako broadcast, takže všichni potencionální klienti se mohou snadno zobrazit dostupné bezdrátové sítě, ke kterým je možné se připojit.(20)

2.12.1.1 Ad-hoc sítě

V ad-hoc síti se spojují dva klienti, kteří jsou v rovnocenné pozici (peer-to-peer). Vzájemná identifikace probíhá pomocí SSID. Obě strany musí být v přímém rádiovém

dosahu, což je typické pro malou síť nebo příležitostné připojení, kdy jsou počítače ve vzdálenosti několika metrů.(20)

2.12.1.2 Infrastrukturní sítě

Typická infrastrukturní bezdrátová síť obsahuje jeden nebo více přístupových bodů (AP-Accesss Point), které vysílají svůj SSID. Klient si podle názvů sítě vybere a připojí se. Několik přístupových bodů může mít stejný SSID identifikátor a je plnou záležitostí klienta, ke které se připojí. Může se například přepojovat v závislosti na síle signálu a umožňovat tak klientovi volný pohyb ve větší síti (tzv. roaming).(20)

2.12.2 Zabezpečení sítě

Problém bezpečnosti bezdrátových sítí je, že jejich signál se šíří i mimo zabezpečený prostor bez ohledu na zdi budov, což si většina uživatelů neuvědomuje. Další problémem je, že se bezdrátová zařízení prodávají s nastavením bez zabezpečení, aby fungovala ihned po zapojení do zásuvky. Kdokoliv se tak může snadno připojit jen s pomocí směrové antény. Většina nejčastěji používaných zabezpečení bezdrátových sítí má jen omezenou účinnost a dá se snadno obejít. (20)

2.12.2.1 Zablokování vysílání SSID

Zablokování vysílání SSID sice porušuje standard, ale je nejjednodušším zabezpečením bezdrátové sítě pomocí jejího zdánlivého krytí. Klient síť nezobrazí v seznamu dostupných sítí, protože nepřijímají broadcasty se SSID. Při připojování klienta k přípojnému bodu SSID však přenášen v otevřené podobě a lze ho tak snadno zachytit. (20)

2.12.2.2 Kontrola MAC adresy

Přípojný bod bezdrátové sítě má k dispozici seznam MAC adres klientů, kteří se mohou připojit. (20)

2.12.2.3 WEP

Šifrování komunikace pomocí statických WEP klíčů (Wired Equivalent Privacy) symetrické šifry, které jsou ručně nastaveny na obou stranách bezdrátového připojení. Má

však nedostatky v protokolu. Klíč lze snadno získat pomocí specializovaných programů. (20)

2.12.2.4 WPA

WPA (Wi-Fi Protected Access) využívá zpětnou kompatibilitu WEP klíče, které jsou ale dynamicky bezpečným způsobem měněny. Autentizace přístupu do WPA sítě je prováděno pomocí PSK (Pre-Shared-Key – obě strany používají stejnou dostatečně dlouhou heslovou frázi) nebo RADIUS server (ověřování přihlašovacím jménem a heslem). (20)

2.12.2.5 WPA2

Novější WPA2 přináší kvalitnější šifrování (šifra AES), která však vyžaduje větší výpočetní výkon a proto WPA2 nelze používat na starších zařízeních. (20)

2.12.3 Nevýhody technologie bezdrátových sítí

- Kvalita spojení klesá při ztrátě přímé viditelnosti klienta na přístupový bod
- Omezený počet nepřekrývajících se kanálů způsobuje rušení komunikace u sousedních přístupových bodů.
- Připojení klienti se dělí o dostupnou šířku pásma, takže se jejich zvyšujícím se počtem klesá i datová dostupnost.
- Vyšší přenosové rychlosti se dosahuje typicky ve směru ke klientovi – pokud klient vysílá, snižuje se dosažitelná propustnost kolizemi, které vznikají na přístupovém bodu, přičemž jejich minimalizaci se snaží zajistit protokol CSMA/CA. (20)

2.13 Přenos optickými vlákny

Přenos dat v optických vláknech se uskutečňuje světelnými impulsy, přenášenými optickým světlovodem. Tato technologie je stále ještě dražší než je telekomunikační elektrický kabel, ale vykazuje tyto pozitivní vlastnosti:

Výhody v oblasti přenosu :

- nižší útlum signálu,
- širší pásmo a větší přenosové rychlosti,

- větší zajištění proti odposlechu oproti elektrickému komunikačnímu kabelu nebo rádiovému přenosu.

Výhody odolnosti oproti poruchám a vlivu okolí:

- odolnost proti zásahu blesku, proti vlivu rozvodu vysokého napětí,
- bezpečný přenos dat ve výbušném prostředí (bez nebezpečí vznícení nábojem),
- nedochází ke ztrátám vyzařováním signálu (vysoká elektromagnetická tolerance),
- galvanické oddělení prvků sítě (bez vyrovnávacích proudů daných rozdílem potencionálu).

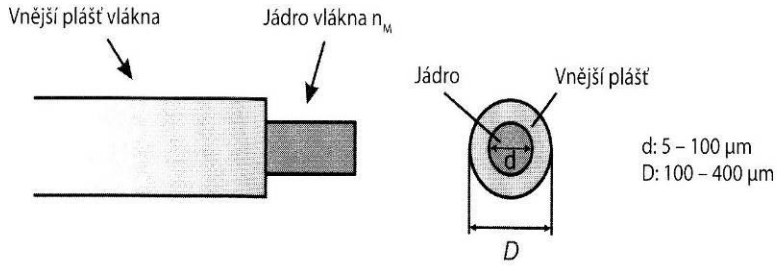
Mechanické výhody:

- menší průměr kabelu a nižší hmotnost (úspora místa, snazší položení kabelu),
- větší pokládací délky, větší vzdálenosti bez stanic,
- odolnost proti korozi.

Proti tomu jsou však nevýhody v podobě vyšších nákladů a náročnější montáže ve srovnání se spojením konektory. Kromě toho je důležité u skleněných vláken dodržen předepsané minimální poloměry ohybu, aby se předešlo eventuálnímu poškození světlovodů. (3)

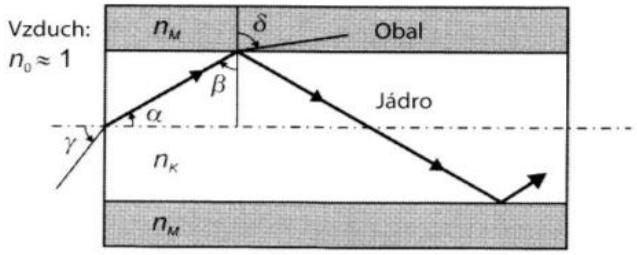
2.13.1 Konstrukce a struktura vlákna

Optické vlákno má uvnitř jádro z křemičitého skla (kysličník křemičitý, SiO_2), který je obklopen křemenným pláštěm (obr. 2-28). Jádro a plášť jsou různě legovány příměsí (cílená injektáž atomů příměsí do čistého kysličníku křemičitého), aby se dosáhlo požadovaného optického lomu n.



Obr.2-26 Konstrukce optického vlákna

Světelný paprsek se podle zákonů optiky na hranici mezi pláštěm a jádrem odráží. Index lomu jádra musí být větší než index lomu pláště. Světelný paprsek se může světlovodem v důsledku totální reflexe šířit (obr. 2-29). Úhel lomu se pak počítá na základě zákonu o lomu.



Obr.2-27 Vstupní vazba a šíření světelného signálu v optickém vlákně

Na ochranu citlivého skleněného vlákna o tloušťce lidského vlasu před mechanickým poškozením je vlákno pokryto dalším pláštěm s několika vrstvami plastových materiálů (např. Kevlarem). Optické vlákna se také vyrábějí z plastu. Ale horší optické vlastnosti těchto vláken nedovolují použití na delší trasy optické kabelové sítě, s výjimkou digitálního přenosu audio (CD/DVD – propojení k optickému přenosu audiozesilovačů). Optická vlákna z polymerů se mezitím začínají využívat pro spojení řídících zařízení a přístrojů v průmyslu a probíhá výzkum cenově dostupných vysokorychlostních systémů, které by měly nahradit DSL. (3)

2.13.2 Útlumové vlastnosti

Útlum je zmenšení intenzity světelného signálu na cestě mezi odesilatelem a příjemcem. Tento útlum by měl být co nejmenší, aby světelný výkon odesilatele a citlivost příjemce vystačily na co nejdelší přenosové trase. Útlum v optických vláknech má řadu příčin. Pod tzv. intenzitními ztrátami se rozumí Rayleighů rozptyl (rozptylové efekty) v důsledku nehomogenity materiálu, analogické s rozptylem světla na vodních kapkách v mlze) a infračervené absorpce. Extrinzitní ztráty vznikají v důsledku materiálových nečistot a příměsí, které rovněž vedou k efektu rozptylu a brání průchodu světla. Další ztráty vznikají důsledkem zakřivení vlákna, které nastává při pokládání optického kabelu (útlum v ohybu) a při prodlužování vedení (útlum při spojování a v konektorech). Kromě toho mohou větší ztráty vznikat při vstupní vazbě světla v tenkém vlákně. Útlum na trase optického vlákna se vyjadřuje v decibelech (dB) nebo vztažmo na délku trasy v dB/km.

Útlum D v dB se vyjádří vztahem:

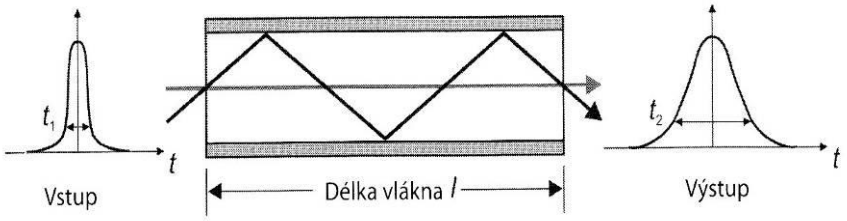
$$D = 10 \cdot \log \frac{P_E}{P_A}$$

Kde P_E je vstupní světelný výkon a P_A je výstupní světelný výkon.

Měrný útlum, tj. typická útlumová hodnota na délku trasy pro skleněná optická vlákna, se pohybuje v hodnotách mezi 0,5-3,0 dB/km. Protože útlumové mechanizmy v optických vláknech závisí n frekvenci, používá se světelné vlnové délky 850 nm, 1300 nm a 1550 nm, které vykazují nejnižší měrný útlum. (3)

2.13.3 Disperzní vlastnosti

Světlo procházející optickým vláknem se šíří světlovodem díky odrazům (obr.2-30). To je případ tzv. vícevidového vlákna (multimode fibre), které má poměrně velký průměr jádra (okolo 50 μm).



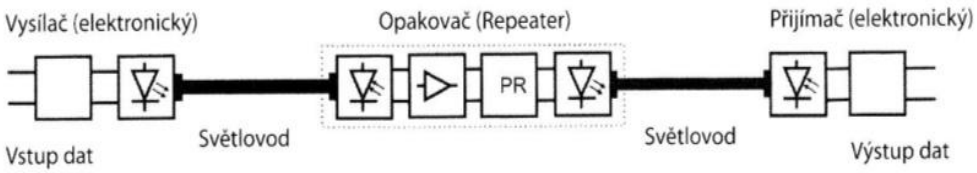
Obr.2-28 Cesta šíření ve vícevidovém vlákně a s tím související zvětšení šíře pulsu

Na základě rozdílných drah se určité části světelného impulsu dříve, jiné později, dostanou do místa příjmu. Vzájemnou interferencí vzniká tzv. rozšíření impulsu, které se označuje jako vícevidová disperze (rozptyl). Při přenosu digitálních signálů světelnými impulsy se dbá na to, aby jednotlivé bity nevysílaly příliš rychle za sebou. To by vedlo k přetížení na straně příjmu a rozpoznání logického stavu zprávy by ztížilo nebo dokonce znemožnilo. Rozšíření impulsu s rostoucí délkou přenosové trasy optického vlákna vzrůstá, takže se jde o tzv. produkty o délce omezené šířkou pásma. Vícevidové disperzi (rozptylu) můžeme zabránit snížením průměru jádra. Při průměru jádra několika μm se šíří světlo ve světlovodu téměř přímo z centra (centrální paprsek). Takováto vlákna se označují jako jednovidová, neboť mají jen jeden směr šíření a nedochází tím k žádné vidové disperzi. Jendovidová vlákna (single mode fibre, monomode fibre) vykazují tudíž lepší vlastnosti ve vztahu přenosové pásmo – vzdálenost – přenosová rychlost než mnohavidová optická

vlákna. Maximální přenosová rychlost je omezena dalším faktorem, materiálovou disperzí. Různé vlnové délky (barvy) světla se šíří ve skleněném vlákně různou rychlostí. Světelný impuls s určitou spektrální šíří (barevným rozsahem) se proto při průchodu vlastní části vlnové délky lomí, a tak se časově rozšiřuje (viz. obr.2-30, kde $t_2 > t_1$). To lze minimalizovat jen použitím takových světelných zdrojů, které vykazují barevnou koherenci, k čemuž se lze přiblížit u laseru (jako zdroje koherentního světla). (3)

2.13.4 Systém optického přenosu dat

Optický systém přenosu dat sestává vedle světlovodu z dalších komponent, uvedených na obr. 2-31.



Obr.2-29 Systém optického přenosu dat

Jako vysílače se používá buď polovodičového laseru, nebo světelné diody. V závislosti na elektrických datových signálech se řídí světelná intenzita. Laser se vyznačuje malou spektrální šíří (tím i nízkou materiálovou disperzí) a rovněž svazkováním, čímž zajišťuje dobrý průchod světla vláknem. Jako přijímačů se používá fotodiod, které světelné impulsy transformují opět na elektrické signály. Delší přenosové trasy vyžadují aplikaci zesilovací jednotky – opakovače (repeater), kde se světelný signál zpětně transformuje na elektrický signál, zesiluje se, upravuje se (PR – Pulse Regeneration) a zpětně se mění na světelný signál. U dlouhých optovlákenných tras se používá i čistě optických zesilovačů. V budoucnu se počítá se širším použitím dalších komponent (spínačů, filtrů, vazebních členů). (3)

2.13.5 Varianty přenosu

V Ethernetu se používá především variant uvedených v tab. 2-7, přičemž nejrozšířenější jsou varinaty s rychlostí 1 GBit/s.

Označení	Rychlost	Maximání délka vlákna
100Base-FX	100 Mbit/s	cca 400 m
1000Base-SX	1 Gbit/s	cca 500 m
1000Base-LX	1 Gbit/s	cca 5 km
10GBase-T	10 Gbit/s	cca 100 m
40GBase-LR4	40Gbit/s	nad 10 km
100GBase-ER4	100 Gbit/s	nad 40 km

Tab.2-7 Varianty přenosu optickým vláknem pro Ethernet

Doručení dat k příjemci a ve zpětném směru Tx, resp. Rx, vždy využívá vlastního samostatného optického vlákna. Oddělené cesty signálů Tx a Ry umožňuje režim plného duplexu. Na zakončení jsou zapotřebí dva odlišné konektory, které se označují zkratkami ST, reps. SC. U 1000Base-SX se pro vlnovou délku 850 nm využívá mnohovidových optických vláken. Průměr jádra může být 50 μm nebo 62,5 μm. 1000Base-LX je přechodem na jednovidová optická vlákna (průměr jádra je 10 μm), kde spojovací vzdálenosti jsou okolo 5 km a vlnová délka je 1300 nm. Nová 10GBase-T Ethernet využívá do vzdálenosti 55 m kabeláž kategorie 6. Při využití plné délky 100 m je nutné použít kabel 6a. 40GBase-LR4 využívá čtyř vlnových délek okolo 1310 nm pro přenos na vzdálenosti 10 a 40 km. 100GBase-ER4 se využívá na trásách, které jsou delší jak 2 km při využití deseti vlnových délek od 1523 do 1595 nm. (16)(3(14)

II. PRAKTICKÁ ČÁST

3 STUDIE DVOU ŘEŠENÍ

3.1 BOSCH - Divar

DIVAR je zkratka pro Digital Versatile Recorder. Zařízení vyrábí firma BOSCH a slouží k zabezpečení budov a jiných zařízení, kde je nutné zabezpečení ochrana. K zařízení můžeme připojit otočnou kameru, čtyři monitory a dvě klávesnice. K rozšíření kapacity jsou použita dvě disková pole typu LP, klávesnice jsou připojeny přes expandér a monitorové výstupy DIVARů do Video Manageru. Systém umožňuje zapojení až 4 těchto zařízení a tím se dostaneme k 64 vstupům na kamery, což postačuje k pokrytí i větších budov a jiných chráněných objektů. (22)

Obr.3-1 Propojení zařízení s kamerami, monitory, ovládacím panelem a uložištěm

3.1.1 Sledování obrazu

DIVAR Billix (obr. 7-2), je vybaven dvěma monitorovými výstupy: A a B. Způsob zobrazení závisí na nastavení sytému.

Obr. 3-2 DIVAR Billinx digitální universální rekordér

Monitor A

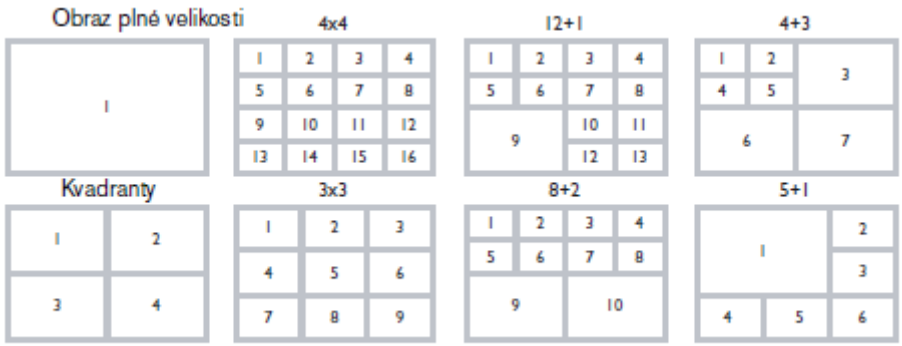
Monitor A je hlavní monitor. Je na něm obraz s plnou velikostí, kvadrantový nebo vícenásobný obraz, a to buď živý obraz z kamer nebo ze záznamu. Na tomto monitoru se zobrazují i stavové zprávy, poplachy, zjištěný pohyb a výstraha při ztrátě videosignálu. Dále se na něm zobrazí i systém menu.

Monitor B

Na monitoru B je jednoduchý obraz s plnou velikostí zvolené kamery nebo se na něm střída sekvence obrazů plné velikosti. Při vzniku poplachu nebo zjištění pohybu lze na monitoru B zobrazit obraz kamery s blikajícím indikátorem poplachu/akce. Pokud současně nastane více poplachů nebo akcí, budou se obrazy příslušných kamer na monitoru B postupně přepínat. (22)

3.1.2 Uspořádání obrazu

Všechna možná uspořádání monitoru jsou na obrázku (obr. 7-3). Některá vícenásobná zobrazení lze při nastavování jednotky zakázat. Vícenásobná zobrazení, která jsou k dispozici závisí na počtu připojených kamer.

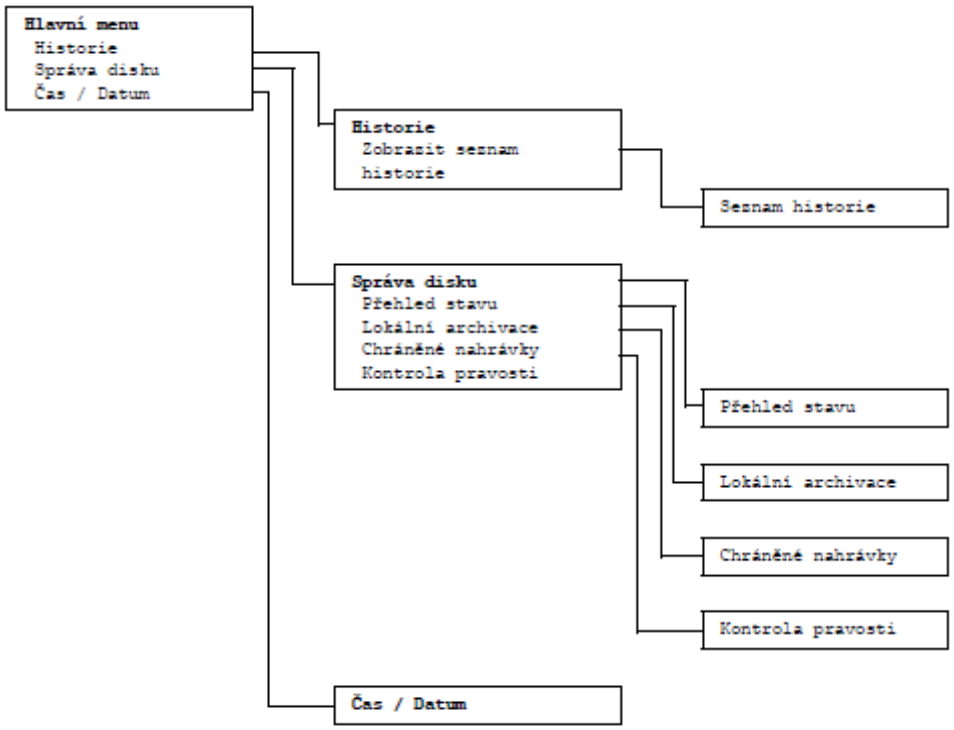


Obr. 3-3 Možnosti zobrazení kamer

Režim kvadrantového obrazu může mít 4 různé kvadranty (části obrazovky), které sem mohou postupně přepínat tak, aby se postupně zobrazilo všech 16 kamer. (22)

3.1.3 Režim živého obrazu, přehrávaní a vyhledávání

Režim živého obrazu je normální provozní režim jednotky, při kterém se sleduje živý obraz jednotlivých kamer. Může z něj přejít do režimu vyhledávání, přehrávání nebo do systémového menu (obr.7-4). Přístup k funkcím vyhledávání a přehrávání může být zabezpečen na heslo, aby nedocházelo k neoprávněnému užití dat. (22)



Obr. 3-4 Struktura menu

3.1.4 Spouštěcí události a poplachy

Způsob jakým jednotka právě pracuje, mohou změnit události různých typů. Jedná se o následující události:

- Signál jednotky, který se objeví na poplachovém vstupu jednotky.
- Zjištění pohybu v signálu kamery.
- Ztráta videosignálu některé z kamer.
- Výstraha vydaná jednotkou na základě vnitřního stavu.

Způsob, jakým bude jednotka na vznikající událost reagovat, závisí na tom, jak byla naprogramována.

Událost může spustit buď spustit reakci (spouštěcí událost, trigger) nebo vyvolat poplach. Spouštěcí událost ovlivní práci jednotky, ale nevyžaduje odezvu uživatele. Poplach může také ovlivnit práci jednotky, navíc se při něm obvykle aktivuje několik indikátorů a od uživatele se vyžaduje potvrzení poplachové situace.(22)

Jednotka může na událost reagovat jedním z následujících způsobů:

Poplachy

- Rozezní bzučák
- Zobrazí se stavová zpráva
- Zobrazí se ikona poplachu
- Okolí části obrazu Cameo může změnit barvu
- Bliká indikátor (AKC-přijmout, zvonek nebo pohybující se osoba)
- Aktivuje se výstupní relé

Poplachy a spouštěcí události

- Změní se zobrazovací režim monitorů
- Kamera, kterou lze ovládát se přemístí (otočí/nakloní) do předem definované polohy
- Změní se rychlost nahrávání

- Jednotka změní způsob, jakým pracuje, podle předem definovaných profilů.(22)

Události na pozadí

Spouštěcí události a poplachy mohou změnit úkoly běžící na pozadí, čehož si uživatel nemusí všimnout. Odezvy jednotky, které uživatel přímo nevidí, jsou např. změna rychlosti nahrávání, aktivace výstupního relé nebo zaznamenání událostí do deníku (log). Jednotku lze také nakonfigurovat tak, aby při aktivaci poplachové vstupu nahrávala videoklipy a automaticky zapnula jejich ochranu před smazáním. Spouštěcí událost může změnit způsob zobrazování kamer na monitorech bez nutnosti zásahu obsluhy.(22)

3.1.5 Sledování živého nebo přehrávaného obrazu přes internetový prohlížeč

Spuštěním internetového prohlížeče a zadáním síťové adresy IP jednotky Divar se lze připojit (např. http://192.168.1.2) k požadované jednotce. Adresa se však musí shodovat s IP adresou nastavenou v položce menu Systémová nastevení/Připojení/Nastavení síťové jednotky Divar. Nejvhodnějším prohlížečem je Internet Explorer verze 6.0 nebo vyší, který vyžaduje bezpečnostní nastavení ovládacích prvků ActiveX z jednotky Divar. Pro přihlášení se objeví stránka určená pro tuto činnost (obr. 3-5). (22)

Obr.3-5 Přihlašovací okno do aplikace DIVAR2

Po přihlášení se zobrazí okno s živým obrazem z kamer, kde lze:

- sledovat živý obraz
- přiřadit kamery plochám obrazovky cameo
- zvolit jiné uspořádání vícenásobného zobrazení

- přepínat obrazy v sekvenci
- pořizovat fotografie
- ovládat kamery (22)

Obr.3-6 Prostředí na ovládání kamer DIVAR2 od Bosche

3.1.6 Digitální klávesnice IntuiKey KBD-UNIVERSAL, KBD-DIGITAL a KBD-MUX

Víceúčelové digitální klávesnice řady IntuiKey jsou určeny k ovládání a programování jednotlivých zařízení průmyslové televize i rozsáhlých systémů z nich sestavených. Vybaveny jsou joystickem s proporcionálním řízením rychlosti natáčení, naklánění a zoomu a dvěma přehlednými LCD displeji s podsvícením. K zadávání povelů a dat slouží rovněž dvě tastatury - numerická a SoftKey - s podsvícenými tlačítky. Volitelná sada slouží k zabudování do 19-ti palcového stojanu (racku). Při lokální konfiguraci zajišťuje napájení klávesnice hlavní přepínač Allegiant nebo digitální videorekordér. Při konfiguraci se vzdáleným umístěním klávesnice zajišťuje napájení volitelný externí napájecí zdroj (prodává se samostatně). Klávesnice se zapojuje do systémů prostřednictvím přiloženého 3 m kabelu. Klávesnici jednoduše připojte a můžete začít pracovat. Žádné další programování není třeba. Digitální klávesnice IntuiKey je nabízena ve třech modelech

(KBD-Universal, KBD-Digital a KBD-Mux). Univerzální verzi je možné současně připojit k přepínači Allegiant a k digitálním videorekordérům Divar**.** Díky této možnosti odpadá nutnost použít více klávesnic. Verze KBD-Digital podporuje digitální videorekordéry Divar**.** Softwarová „SoftKey" tlačítka klávesnic IntuiKey nabízejí snadné ovládání pomocí systému menu. Tak mohou i noví operátoři snadno programovat a ovládat i ty nejrozsáhlejší systémy bez nutnosti pamatovat si systémové příkazy. IntuiKey nabízí funkci rychlé volby, která zajišťuje okamžitý přístup k nejčastěji používaným nabídkám a zobrazením. IntuiKey dále nabízí uživatelsky příjemnou strukturu menu pro programování všech pokročilých nastavení systému a kamer. Klávesnice podporuje více jazyků (obr. 3-7)**.** (22)

Obr.3-7 Digitální ovládací klávesnice k systému DIVAR od Bosche

3.2 Jablotron JA – 82V

JA-80V – komunikátor pro komunikace po počítačových sítích LAN (Ethernet) kombinaci s komunikátorem na pevnou telefonní linku. Umožňuje komunikaci na PCO po LAN a předává zprávy pomocí pevné linky. Také lze spravovat z aplikace GSMLink**.** Periferie mohou být zařazeny do 3 sekcí: A,B a C. Sekce se uplatňují buď při částečném hlídání: střeží A, střeží AB, střeží ABC (vhodné pro obytné prostory: A=odpolední hlídání, AB=noční hlídání a ABC=kompletní hlídání), nebo při rozdělení systému na 2 nezávislé části A a B s částí společnou C: hlídá A, hlídá B a pokud hlídá A i B hlídá i C (vhodné tam, kde sídlí dva nezávislí uživatelé – rodiny, firmy apod.). Ústředna má 2 poplachové

výstupy: IW = interní poplach a EW = externí poplach. Tyto poplachové signály jsou též vysílány pro bezdrátové sirény. V ústředně jsou 2 programovatelné výstupy PGX PGY s nastavitelnou funkcí. Stav PG výstupů je vyveden nejen na svorkách, ale je také vysílán pro bezdrátové moduly UC a AC. Systém lze ovládat pomocí přístupových kódů nebo karet (ústředna rozlišuje až 50 uživatelů). K ovládání lze také použít bezdrátové klíčenky a jeli ústředna vybavena vhodným komunikátorem, může být ovládána dálkově mobilním telefonem nebo z internetu. Přístupovým kódům (kartám) lze nastavit různé funkce (např. zajistí/odjistí, pouze zajistí, panik apod. Je-li systém rozdělen, lze určit, do které části domu má ten který kód přístup. Každý z padesáti uživatelů může mít nastaven čtyřciferným přístupový kód a přístupovou kartu. Ovládání je pak možné buď kartou nebo kódem a je-li požadována vyšší bezpečnost, lze zapnout potvrzování karty kódem(obr.3-6). (20)

Obr.3-8 Ústředna JA-82V

3.2.1 PC-01 bezdotyková RFID karta

PC-01 je bezdotyková RFID karta (standard EM UNIQUE 125 kHz). K systému lze přiřadit až 50 karet. Pro vyšší ochranu lze použití karty podmínit zadáním číselného kódu. Karty lze snadno potisknout. Přiřazuje se k ústředně naučením na klávesnici JA-81F, JA-81E, JA-80F, JA-80F, JA-80H nebo JA-80N(obr. 3-7). (20)

Obr. 3-9 RFID karta bezdotyková

3.2.2 Detektory

Slouží k prostorové detekci pohybu osob v interiéru budov, duální senzor pohybu a senzor rozbití skla (rozezná rozbití okna do vzdálenosti až 9m) a detekci požárního nebezpečí. Všechny detektory využívají digitální analýzu proti falešným poplachům.(20)

3.2.3 Bezpečnostní kamery EYE-02 GSM

EYE-02 je bezpečnostní a monitorovací kamera, která komunikuje bezdrátově prostřednictvím GSM sítě. Kombinuje v sobě detektory, které umožňují detekovat přítomnost narušitele:

- PIR pohybový detektor-detekuje pohyb pomocí změny teploty vlivem přítomnosti člověka v místnosti
- Zvukový detektor-Mikrofon detekuje, zda hluk nepřekročil stanovenou mez
- Detektor rozbití skla-rozeznává specifický zvuk rozbití okenního skla
- Detektor pohybu v obraze-kamera detekuje změny scény pravidelným pořizováním snímků a jejich porovnávání (20)

Obr. 3-10 Kamera EYE-O2

4 PROJEKT ZABEZPEČENÍ KANCELÁŘSKÉ BUDOVY

Při zabezpečení kancelářské budovy se klade hlavní důraz na jednoduchou instalaci, komfortní ovládání, bezporuchovost a snadný přístup k datům, které chceme zaznamenávat a ukládat pro další potřebu. Rozhodujícím faktorem je počet osob, které budou mít přístup do budovy a prostor, který je potřeba zabezpečit. Dnes při rozmachu výpočetní techniky se již vstupy a výstupy do budov, řeší pomocí čtecích karet. Umožňují nám nejen zaznamenávat příchod a odchod, ale lze také u nich nastavit různá oprávnění a přístupy do vymezených prostor. To se děje pomocí signálů (správně/chyba, 0/1), nebo se rozhoduje na základě informací z databází, které jsou uloženy na servrech a řízené mikropočítači. Odtud se v případě nežádoucí změny výstup přenáší na centrální pult ochrany (velín) na monitory a PC, které ovládají EZS, PZS a kamery. Data se ukládají na servrech a lze s nimi následně pracovat. V chráněných budovách navíc jak zabezpečení se využívá fyzická ochrana (Policie ČR, bezpečnostní agentury), které jsou přímo v budově, provádí pravidelnou kontrolu a řeší vzniklé situace. Při zjištění poplachu, neoprávněného vstupu se signál pak nemusí odesílat na policie, hasiče. V budovách chráněného typu se využívá veškerých dnešních dostupných technologií od kamer, detektorů pohybu, požáru, tepla, perimetrů (okolí budovy) posílené o fyzickou ostrahu. Tyhle budovy jsou potom velmi dobře zajištěny proti neoprávněnému stupu cizích osob. Náklady však na takové zabezpečení (kamery, monitory, uložiště dat, přenos dat, detektory, policie) jdou do obrovských čísel a můžou si je dovolit pouze velké firmy nebo stát (důležité ministerstva).

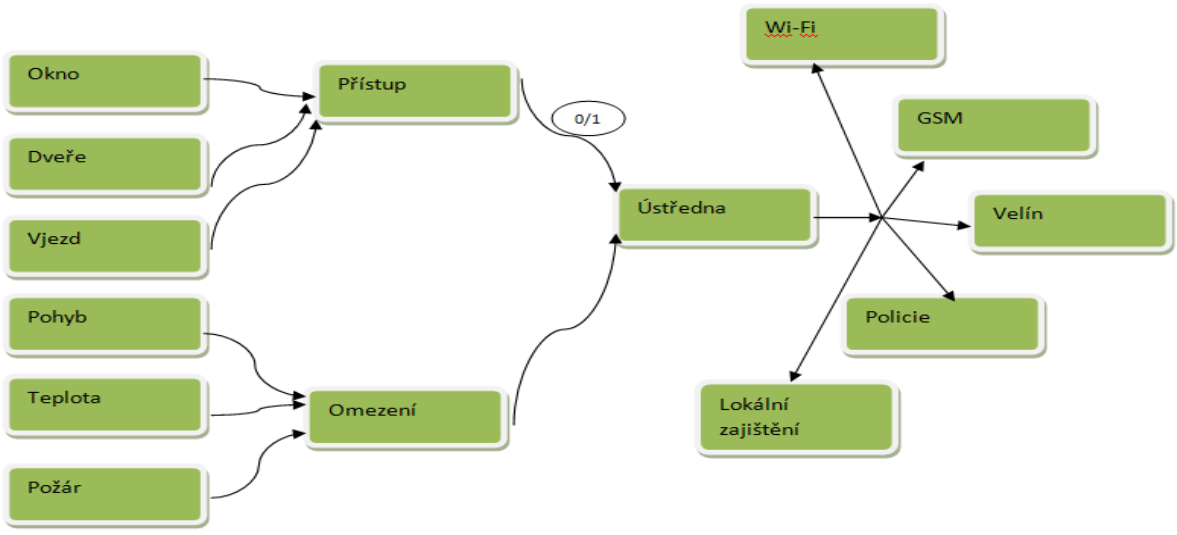


Schéma 4-1 Obecné schéma

4.1 Vstupní lokální schéma

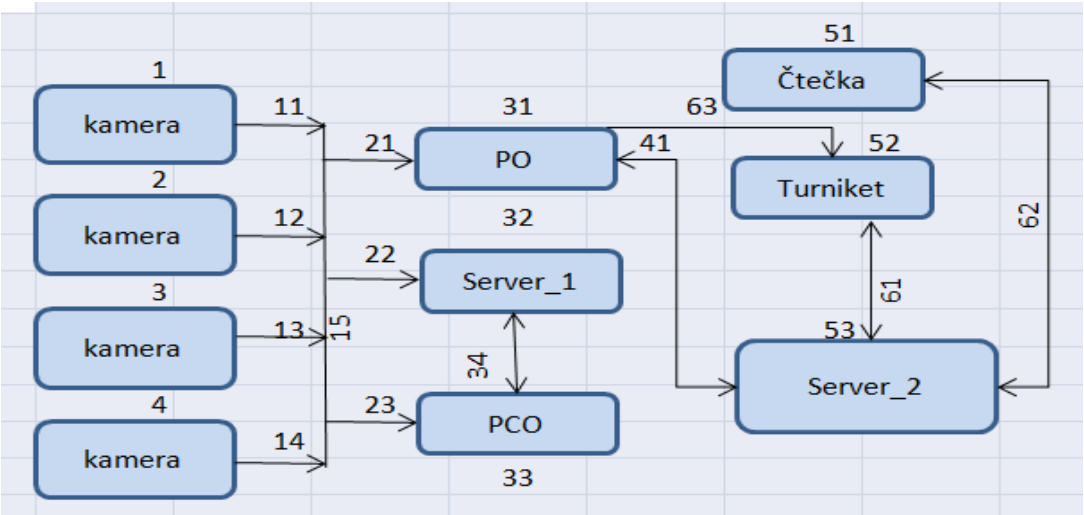


Schéma 4-2 Lokální vstup

Při vstupu do budovy v prostor snímají kamery (1-4), které obraz přenáší přes sběrnici (11-14) a koaxiální kabel (21) na pult ochrany (31 PO), kde se na monitoru zobrazují dané kamery, které můžeme zobrazit jednotlivě nebo pomocí kvadrantového selektoru 4 na jednom monitoru. Pult ovládá např. policista. Na Server_1 se přenos provádí přes kroucený kabel (TP) nebo optický kabel (22), kde se na uložiště ukládá záznam ze všech kamer (až na několik měsíců podle kapacity uložiště). Na pult centrální ochrany (33 PCO) se kamery přes koaxiální kabel (23) přenáší rovněž. Server_1 a PCO jsou propojeny TP (34). Z PCO kde sedí ochranná služba, lze ovládat kamery, a pracovat se záznamy ze všech kamer pomocí zařízení a programu DIVAR (kap. 3). K PO je ještě připojen pomocí TP (41) Server_2, kde je databáze pro vstup osob. Na Server_2 je připojeno čtecí zařízení na karty (62) přes (USB, TP), která vyhodnocuje po přiložení karty, zda je osoba oprávněna pro vstup. Při platném vstupu se odešle signál na PO(41), kde na PC v programu BEWATOR (Siemens) se na monitoru zobrazí fotografie osoby v zeleném rámečku (OK). Dále server vyšle signál pro turniket (61), že se může otevřít. V případě neplatného vstupu se na monitoru na PO nezobrazí fotografie osoby, ale pouze prázdný červený rámeček a turniket se neotevře. Turniket lez také vládat fyzicky tlačítky z PO (63), kde je fyzicky přítomna ochranná služba.

Mezi vstupy do budovy řadíme dveře, okna a vjezdy. Každé okno na plášti budovy, které lze otevřít se opatřuje dotykovým senzorem, který detekuje kdy je okno otevřené, nebo senzor proti rozbití skla. U dveří se používá zámek nebo dotykový senzor. Pro zvýšení bezpečnosti vstupu se vstupy a výstupy opatřují čtecím zařízením na karty doplněné o klávesnici pro zadání kódu. Jako nejvyšší zabezpečení lze ke všem těmto prvkům přidat ještě fyzickou ostrahu objektu, kterou provádí buď bezpečnostní agentura nebo přímo policie ČR. U takových budov jsou na vstupu ještě používány bezpečnostní rámy, které detekují nebezpečné předměty při vstupu a předměty jsou odebírány dotyčným osobám, dokud jsou v budově. Při velkém počtu osob v budově se vstup monitoruje pomocí vstupních bezdotykových RFID, jejichž snímáním se identifikuje v systému (Siemenes Bewar), který má na monitoru spolu s fotografií dotyčné osoby ostraha k dispozici a tím se velmi výrazně eliminuje vstup nežádoucích osob do objektu. Vše je umocněno vstupem přes turniket, který neoprávněné osoby nevpustí dovnitř, ostraze se neplatný vstup zobrazí na monitoru a může operativně zamezit vstupu do budovy i při použití fyzické síly. Vše je snímána dostatečným množstvím kamer, které jsou přepojeny na centrální pult ostrahy (CPO). Zde mají dokonalý přehled o dění uvnitř budovy a o pohybu osob. V kancelářských budovách je většina vstupu opatřena čtecím zařízením na karty, kde se definují práva jednotlivým uživatelům. Při takovém zabezpečení se eliminují neoprávněné vstupy osob do prostor, které jim nejsou určeny.

4.2 Dispoziční schéma přenosu

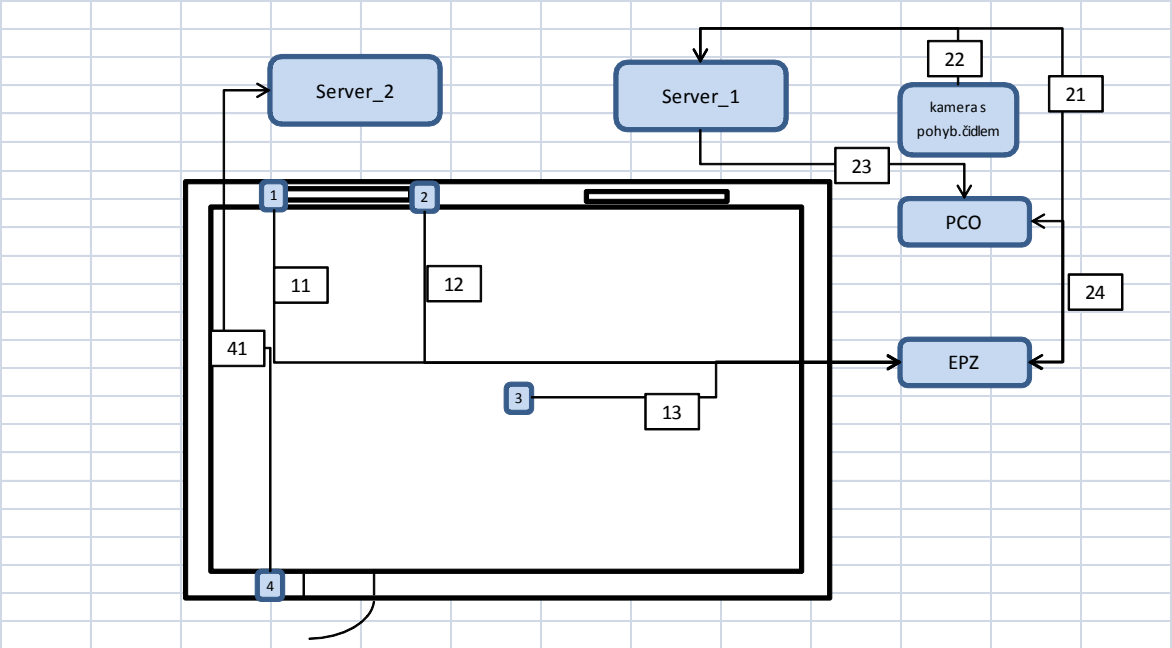


Schéma 4-3 Dispoziční schéma přenosu

Při ochraně vstupu do místnosti a přenosu signálů z detektorů může být následující. Z čidla kontaktu oken (1), čidla rozbití skla (2) a protipožárního čidla (3) se signály směřují do přes sběrnici (11,12,13) elektronického požárního zabezpečení (EPZ), který je propojeno na Server_1(21) a PCO (24) přes sběrnici a kameru s pohybovým čidlem (22). Ze Server_1 může PCO přes TP (23) pomocí specializovaného softwaru vidět pomocí dispozičního přenosu, v které konkrétní části budovy a čidlo vyslalo signál. U dveří bývá zpravidla pro zabezpečení čtecím zařízením na karty (4) opatřena klávesnicí pro zadání kódu, čímž se zvyšuje zabezpečení. Signál ze čtecího zařízení přes (TP,USB) (41) vede na Server_2, kde se v databázi vyhodnotí oprávněnost vstupu osoby.

ZÁVĚR

Se systémy přenosu dat ze zabezpečovacích se dnes setkáváme velmi často při vstupu do bank, kancelářských budov a větších podniků. Tyto systémy pro přenos uchování dat jsou výhodnou investicí pro rozsáhlé objekty s přístupem pro stovky osob. Umožňují kontrolu osob v objektu, poskytují informace o jejich pohybu a ukládají informace v reálném čase. To přispívá k ochraně budov před nepovelenými vstupy a požáry i režimovými opatřeními. Přenos se však vyskytuje i v jiných systémech např. EZS či CCTV. Práci jsem popsal systémy přenosu a funkci jednotlivých prvků. Obecně jsem popsal přenosové média, typy sítí a prvky přenosu mezi sběrnice a uložišti dat. Cílem bylo popsat přenos dat ze zabezpečovacích zařízení (čtecí zařízení, požární signalizace, detektory ajn.) a formulovat požadavky na tyto systémy. Problematika této oblasti je velmi rozsáhlá. Při tvorbě této práce jsem se snažil, aby se čtenář seznámil s danou problematikou a pochopil, jakým způsobem se přenos probíhá a jaké jsou možnosti.

ZÁVĚR V ANGLIČTINĚ

To data transmission systems of security are now very often encountered when entering banks, office buildings and large enterprises. These systems for the transmission of data storage are good investments for large buildings with access to hundreds of people. Allows control of persons in the building, provide information on their movements and store information in real time. This helps to protect buildings from fire and unauthorized inputs and lifestyle changes. The transfer is not found in other systems such as intrusion detection and CCTV. The work I have described transmission systems and the function of individual elements. Generally, I described the transmission media, types of network elements and transfer between bus and data storage. The aim was to describe the transfer of data from security devices (readers, fire alarms, detectors asn.) And formulate the requirements for such systems. Problems of this area is very extensive. In creating this work I have tried to make the reader familiar with the issues and understand how the transfer takes place and what are the options.

SEZNAM POUŽITÉ LITERATURY

(1) KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 2. S.l.: Cricetus, 2003, 351 s. ISBN 80-902-9382-4.

(2) KREJČIŘÍK, Alexandr. *SMS*: *střežení a ovládání objektů pomocí mobilu a SMS : GSM pagery a alarmy : princip použití, návody, příklady*. 1. vyd. Praha: BEN - technická literatura, 2004, 303 s. ISBN 80-730-0082-2.

(3) MERZ, Hermann, Thomas HANSEMANN a Christof HÜBNER. *Automatizované systémy budov*: *sdělovací systémy KNX/EIB, LON a BACnet*. 1. vyd. Praha: Grada, 2008, 261 s. ISBN 978-80-247-2367-9.

(4) Schneider Electric CZ, I/NET Seven zabezpečovací a přístupový systém. Praha: Schneider Electric CZ, 2005

(5) KONÍČEK, Tomáš, Stanislav KŘEČEK a Pavel KOCÁBEK. *Městské kamerové dohlížecí systémy*. Praha: Odbor prevence kriminality Ministerstva vnitra ČR, 2002, 87 s., [8] s. obr. příl. Prevence se musí vyplatit. ISBN 80-731-2009-7.

(6) UHLÁŘ, Jan. *Technická ochrana objektů*. Vyd. 1. Praha: Vydavatelství PA ČR, 2006, 246 s. ISBN 80-7251-235-8.

(7) Vrstvy koaxiálního kabelu. [online]. [cit. 2012-06-03]. Dostupné z: http://site.the.cz/index.php?id=26

(8) RJ 45. [online]. [cit. 2012-06-04]. Dostupné z: http://www.tomshardware.com/reviews/pc-interfaces-101,1177-9.html

(9) Zabezpečení proti narušení. [online]. [cit. 2012-06-02]. Dostupné z: http://www.technicom.cz/komplexni-reseni- zabezpeceni-proti-naruseni.html

(10) HW [online]. 2005 [cit. 2012-05-22]. USB 2.0. Dostupné z: http://www.hw.cz/Rozhrani/ART1232-USB-2.0---dil-1.html

(11) Wikipedia [online] 2012 [cit. 2012-5-29] Přenos přes Bluetooth. Dostupné z: http://cs.wikipedia.org/wiki/Bluetooth

(12) HW [online]. 2008 [cit. 2012-05-19] USB 3.0. Dostupné z: http://www.hw.cz/teorie-a-praxe/dokumentace/vysla-specifikace-usb- 30.html

(13) Automa [online]. 2006 [cit. 2007-01-01] SBĚRNICE IEEE1394. Dostupné z: http://www.odbornecasopisy.cz/index.php?id_document=34406

(14) 100GBase Ethernet. [online]. [cit. 2012-06-01]. Dostupné z: http://en.wikipedia.org/wiki/100_Gigabit_Ethernet

(15) Ethernet. [online]. [cit. 2012-05-07]. Dostupné z: http://cs.wikipedia.org/wiki/Ethernet#Optick.C3.A9_vl.C3.A1kno

(16) Sítě. [online]. [cit. 2012-06-07]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Gigabitovych-Wi-Fi-siti-80211ac-se-dockame-jeste-v-letosnim-roce-1-2512012

(17) WLAN. [online]. [cit. 2012-06-07]. Dostupné z: http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite.html

(18) MAN. [online]. [cit. 2012-06-07]. Dostupné z: http://cs.wikipedia.org/wiki/IEEE_802.6

(19) Wikipedia [online] 2012 [cit. 2012-5-30] PAN sítě. Dostupné z: http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5

(20) Jablotron [online]. 2012 [cit. 2012-06-01] Jablotron JA-82K. Dostupné z: http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/oasis+868mhz/ustredny/ja82k+ustredna+zabezpecovaciho+systemu+oasis/

(21) Siemens [online]. 2012 [cit. 2012-06-01] Bewator Entro. Dostupné z: http://www.siemens.cz/siemjetstorage/files/44520_BewatorEntro5$cz.pdf

(22) DIVAR2. [online]. [cit. 2012-06-07]. Dostupné z: http://www.bosch-securitysystems.cz/produkt-detail.php?sel_prod=670

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PZTS	Poplachový zabezpečovací a tísňový systém
EZS	elektrická zabezpečovací signalizace
CCTV	Closed Circuit TV – uzavřený televizní okruh
DDC	Direct Digital Control
EIB	European Installation Bus
BACnet	Bulding Automation and Control Network
MS/TP	Master-Slave/Token-Passing
Bit	Binary Digit
Bd	Baud
HDD	Hard Digital Disk
CRC	Cyclic Redundancy Check - cyklická redundantní kontrola
NRZ	Non-Return-to Zero
DMC	Differential Manchaster Code
OSI	Open Systems Standardization – otevřené systémy
ISO	Interanzional Organization for Standardization - Mezinárodní organizace pro normalizaci
UDP	Data Unit Prototocol - datové jednotky protokolu
LAN	Local Area Network – lokální síť
WAN	Wide Area Network – rozsáhlá síť
Wi-Fi	Wireless Fidelity – bezdrátová síť
PAN	Personal Area Network – osobní síť
MAN	Metropolitan Area Network – Metropolitní síť
FDDI	Fiber Distributed Data Interface
DQDB	Distributed Queue Dual Bus

SONET	Synchronous opitical network
ATM	Asynchronous Transfer Mode
PC	Personal Computer – osobní počítač
P2P	Peer-to-Peer – rovný s rovným
UTP	Unshielded twisted pair - nestíněná kroucená dvojlinka
TCP	Transfer Control Protocol
IP	Internet Protokol
USB	Universal Seriál Bus

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH