Využití inteligentního systému INELS v BP

Utilization of intelligent system INELS in the security industry

Stanislav Zavadil

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

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

Jméno a příjmení:	**Stanislav ZAVADIL**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Využití inteligentního systému INELS v BP**

Zásady pro vypracování:

1. **Seznamte se s problematikou inteligentních systémů v BP.**
2. **Uveďte jednotlivé části, které obsahuje systém INELS.**
3. **Popište bezpečnostní technologie využívané v inteligentních budovách se zaměřením na systém INELS.**
4. **Uveďte nové trendy v této oblasti.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Valeš, Miroslav. Inteligentní dům. 2. vyd.: ERA, 2008. 136 s. ISBN 978-80-7366-137-3.**
2. **Merz, Hermann, Hansemann, Thomas, HUBNER, Christof. Automatizované systémy budov. Vaclav Bartoš. 1. Vyd. Praha : Grada Publishing, a.s., 2008. 264 s. ISBN 978-80-247-2367-9**
3. **Zálešák, Martin,. Technika prostředí v oboru Integrované systémy v budovách = Environmental technology in the field of integrated systems in buildings : teze habilitační práce /. Ve Zlíně : Univerzita Tomáše Bati, 2009. 42 s. : ISBN 978-80-7318-834-4 (brož.).**
4. **Křeček, Stanislav. Příručka zabezpečovací techniky. 2. autoriz. vyd.: Cricetus, 2002. 350 s. ISBN 80-902938-2-4.**
5. **Ivanka, Ján,. Systemizace bezpečnostního průmyslu I /. 3. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 123 s. : ISBN 978-80-7318-850-4 (brož.).**
6. **Ivanka, Ján,. Systemizace bezpečnostního průmyslu II /. Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 86 s. : ISBN 978-80-7318-863-4 (brož.).**

Vedoucí bakalářské práce: **Ing. Petr Navrátil, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Práce pojednává o úvodu do problematiky inteligentních systémů v bezpečnostním průmyslu, ve kterém jsou uvedeny jednotlivé topologie sítí, komunikační sběrnice nebo typy komunikačních médií. Následně je zde charakteristika systému INELS s jeho prvky. Hlavním cílem práce je zjištění využitelnosti inteligentního systému INELS, jeho technologické a technické vybavení se zaměřením na bezpečnostní průmysl.

Klíčová slova: Referenční model OSI, LonWorks, KNX/EIB, INELS, CIB.

ABSTRACT

Work deals with an introduction on Intelligent Systems in the security industry which provides various network topologies, communication bus or types of communication media. Subsequently there is a characteristic of the INELS with his components. The main task is to determine usability of intelligent system INELS and his technological and technical equipment with a focus on the security industry.

Keywords: The OSI Reference Model, LonWorks, KNX/EIB, INELS, CIB.

Tímto bych chtěl poděkovat vedoucímu mé práce Ing. Petru Navrátilovi, Ph.D. za poskytnuté odborné rady a konzultace.

Rád bych také poděkoval své rodině a přítelkyni, kteří mě ve studiu na vysoké škole podporovali a dokázali pochopit mou zaneprázdněnost.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Vývoj inteligentních budov začal kolem 80. let. Od tohoto roku se systémy dále vyvíjely podle technických a technologických možností a požadavků na ně samotné. Inteligentní systémy byly realizovány především v rozsáhlých objektech a budovách. Teprve několik let zpátky zaznamenaly systémy inteligentních budov velký pokrok a vývoj ve všech směrech.

Pod pojmem inteligentní budova si můžeme představit objekt, který je plně automatizovaný a dokáže sám na základě svých podnětů a informací ze senzorů vyhodnotit danou situaci a následně provést úkon. Inteligentní systémy budov jsou navrhovány tak, aby usnadňovaly jinak komplikované realizace elektroinstalací a integrovaly v sobě veškeré moderní technologie, jako jsou řízení vnitřních klimatických podmínek, vytápění, osvětlení, kamerové systémy, bezpečnostní a požární systémy a také systémy kontroly vstupů. Veškeré tyto systémy mohou být ovládány a konfigurovány prostřednictvím centrální jednotky, která je srdcem celé elektroinstalace a řídí veškerý tok informací na sběrnici. Samozřejmostí pro funkční komunikaci je důležitý výběr prvků systému tak, aby dokázaly vzájemně komunikovat (pracovaly se stejným komunikačním protokolem).

Inteligentní systémy budov se začínají realizovat ve velké míře v rodinných domech, kde nabízejí svým uživatelům nejen funkčnost, ale také komfort a bezpečnost. Přístup do celého systému je přes grafické prostředí, ve kterém můžeme jednoduše ovládat celý objekt. Není vůbec důležité, jestli se nacházíme uvnitř objektu nebo u počítače ve své kanceláři, protože přístup na web server centrální jednotky máme odkudkoli.

Důležitým aspektem inteligentních systémů je komunikace, která může být realizována prostřednictvím ethernetu, bezdrátového spojení, silovým vedením nebo sběrnicovým systémem. Propojení mezi jednotlivými prvky systému je realizované přenosovým médiem. Samotné propojení se musí řídit pravidly dané topologie zapojení sítě.

Bakalářská práce by měla sloužit pro přiblížení problematiky inteligentních systémů budov a využití v praxi převážně zaměřené na bezpečnostní technologie systému INELS.

1 INTELIGENTNÍ SYSTÉMY V BP

Do bezpečnostního průmyslu všeobecně spadá velmi široké spektrum služeb a výrobků k ochraně zdraví, života, a majetku. Inteligentní systémy budov dokážou být v dnešní době velmi schopné a užitečné. Pokud mluvíme o využití inteligentních systémů v bezpečnostním průmyslu, tak tím můžeme chápat sjednocení, vzájemnou komunikaci, vyhodnocení a výsledné jednání, které je založeno na inteligentním rozhodnutí celého systému do kterého spadají jednotlivé podsystémy, jako jsou kamerové systémy (CCTV), elektronická zabezpečovací signalizace (I&HAS), elektronická požární signalizace (EPS), přístupové a kontrolní systémy (ACCES), systém řídící osvětlení a měření energií apod.

Samotná zařízení jako taková většinou nemůžeme nazývat jako inteligentní. Jejich inteligenci můžeme chápat do jisté míry podle množství volitelných funkcí, kterými disponují a nastavitelnost těchto funkcí. Hlavní výhodou inteligentních systémů je přístup a správa celého objektu jedním uživatelským rozhraním. Hlavními přínosy integrovaných systémů řízení budov, jsou:

- úspora energií a provozních nákladů,
- vizualizace a přehled o všech systémech z jednoho místa,
- vyšší stupeň zabezpečení např. vyloučením reakcí na plané poplachy,
- okamžitá kontrola spotřeby energií, záznam historie a analýza špiček,
- komfortnější pracovní prostředí,
- spolehlivost napájení a kontinuita provozu,
- zajištění komunikace. [1][2]

Inteligentní systémy budov jsou navrženy tak, aby dokázali v jediném okamžiku vyhodnotit vzniklou situaci a provést následnou operaci, která vede k upozornění, omezení nebo zrušení daného problému. Pokud bychom se bavili všeobecně o inteligentních systémech, tak zde můžeme například uvést reakci zatažení předokenních rolet v závislosti na svitu slunce. Jelikož práce pojednává o bezpečnostním průmyslu, tak se zaměříme na reakce vzniklé při ochraně zdraví, života, a majetku.

Všechny inteligentní systémy jsou uzpůsobeny tak, aby využily dostupných nebo přídavných prvků systému a informovali o vzniklých příčinách hrozícího nebezpečí. Tato informovanost může být realizována několika způsoby. Základním způsobem, jehož komunikačním prvkem je síťová karta integrovaná na základní desce řídící jednotky celého

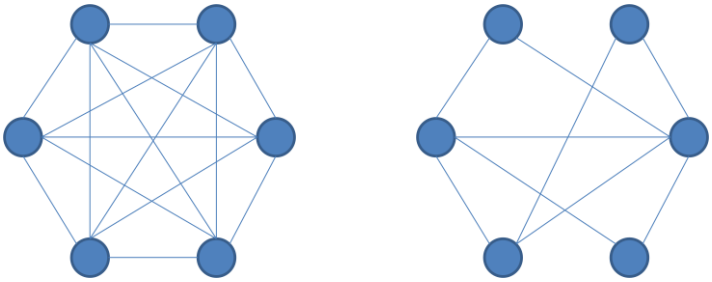
systému, je přenos poplachových zpráv a informací pomocí internetu. Další možností je použití modulu GSM (Global System for Mobile Communications), který nám v případě poplachu nebo vzniklého problému zašle na mobilní telefon nebo na přednastavené telefonní číslo pultu centralizované ochrany zprávu, která bude obsahovat informace o stavu systému nebo druhu vyvolaného poplachu. Stále jedním s nejspolehlivějších a nejbezpečnějších přenosových cest je volba jednotné telefonní sítě. U tohoto přenosu je nejmenší pravděpodobnost výpadku nebo narušení pachatelem. Pokud se jedná o zasílání krátkých textových zpráv (SMS), doručení této zprávy není se 100% jistotou. Zpráva SMS může dojít se zpožděním nebo vůbec. Zejména se jedná o případy zasílání SMS do jiné operátorské sítě. Přenos informačních a poplachových zpráv přes internet je také značně nespolehlivý. Může dojít k výpadku serveru, který nás úplně odřízne nebo částečné rušení signálu bezdrátovým připojením k síti internet. Toto omezení nebo úplné rušení zabrání v nahlášení samotného poplachu.

1.1 TOPOLOGIE SYSTÉMŮ

Jedním z důležitých pojmů z oblasti sběrnic je topologie sítě. Jedná se o fyzické připojení jednotlivých členů tak, aby mezi s sebou správně komunikovaly. Takové připojení do sítě musí být realizováno podle daných pravidel, abychom se vyhnuli chybám a vzájemnému rušení, které můžou vzniknout ve chvíli, kdy se v zapojení vyskytne více informací najednou. Tuto problematiku řeší spojový protokol kanálu. [2]

1.1.1 Polygonální topologie

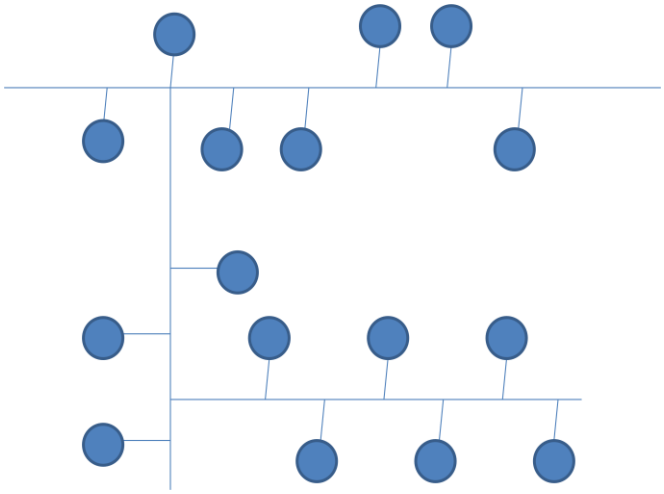
Tyto sítě se vyznačují tím, že každý účastník sítě je propojen se všemi ostatními účastníky. U částečné polygonální sítě se na všechny účastníky připojují jen někteří. Polygonální síť je velice spolehlivá, protože při odpojení jednoho uzlu může zbytek dále komunikovat navzájem prostřednictví jednoho nebo více zprostředkujících uzlů. Značnou nevýhodou polygonální topologie je velké vynaložení finančních prostředků na nákup kabelů, které slouží k pospojování mezi jednotlivými členy systému.



Obr. 1. Polygonální síť (úplně a částečně propojená)

1.1.2 Stromová topologie

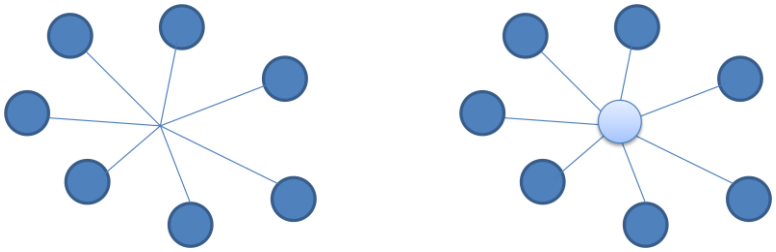
Stromová topologie je rozvinutí sběrnicové topologie, kde nejsou připojeny pouze funkční jednotky systému, ale také další sběrnice (linky). Pomocí této topologie jsou možné realizovat rozsáhlejší plochy elektroinstalací.



Obr. 2. Znázornění stromové topologie

1.1.3 Hvězdicová topologie

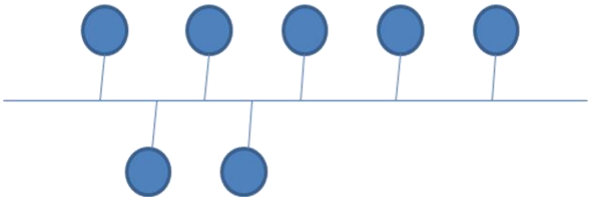
Hvězdicová topologie je založena na sjednocení všech uzlů do jednoho centrálního. Tím, že je každý uzel spojen s centrálním, je značně menší pravděpodobnost výpadku celé sítě. Při fyzickém přerušení kabelu, dojde pouze k odpojení jednoho zařízen a ostatní budou nadále fungovat. Komunikace mezi jednotlivými zařízení je realizována přes hlavní uzel (rozbočovač). Pokud dojde k poruše hlavního rozbočovače, dojde k výpadku celé sítě.



Obr. 3. Hvězdicová topologie bez centrální stanice, s centrální stanicí

1.1.4 Sběrnicová (liniová) topologie

Je jedním z nejvíce používaných sítí v automatizaci budov (inteligentní budovy). Spojení je realizováno jediným přenosovým médiem (sběrnicí), ke které se připojují jednotlivé hardwarové složky systému. Výhodou při realizaci sběrnicové topologie oproti topologii polygonální jsou mnohem menší pořizovací náklady na kabeláž. V tomto případě vedeme jeden hlavní kabel, na který připojujeme jednotlivé členy.



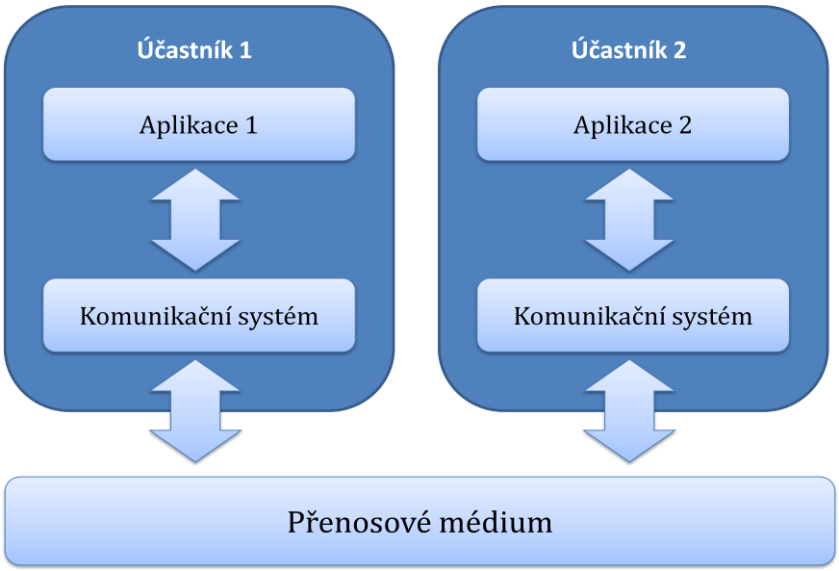
Obr. 4. Liniová (sběrnicová) topologie

1.2 KOMUNIKACE V SYSTÉMU

Komunikačním prvkem v integrovaných systémech jsou sběrnice, tedy použití otevřeného komunikačního standardu. V praxi se nejvíce osvědčily standardy, jako jsou LonWorks a KNX/EIB. Každý velký výrobce zaměřený na domovní zařízení a systémy používá jiný druh datové sběrnice. Datová síť celého systému obsahuje velké množství informací, které jsou pro nás v určitý okamžik nepodstatné. Systém musí být perfektně naprogramovaný, aby dokázal zpracovávat podstatné informace od senzorů a stavy akčních členů k analyzování situace a následnému vyhodnocení, které může mít podobu rozsvícení světla v návaznosti na PIR detektor nebo vyhlášení poplachu způsobeného hlásičem požáru.

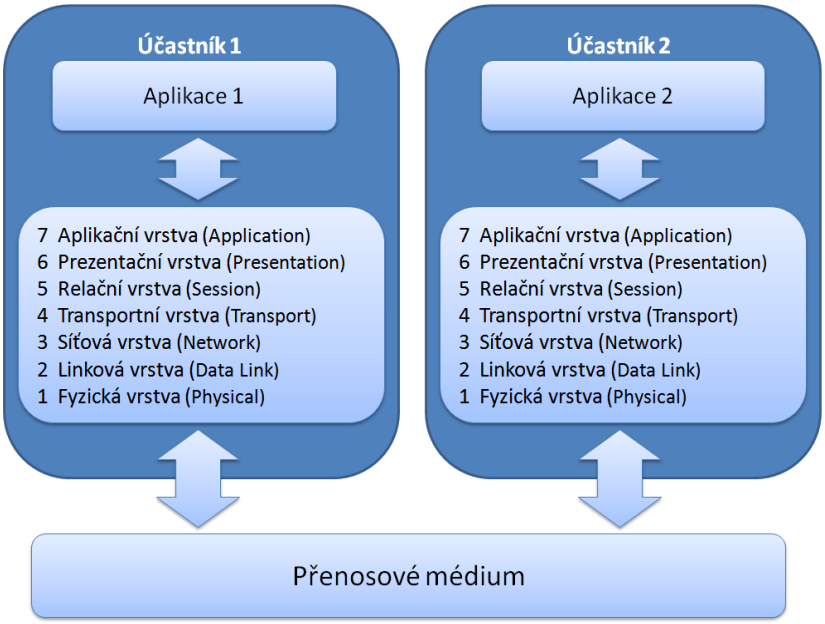
REFERENČNÍ MODEL ISO/OSI

Referenční model ISO/OSI je upraven mezinárodním standardem ISO 7498 (Information processing systems), kde popisuje vytváření vrstvených protokolů (pravidla o provádění komunikace). Dále je v normě uveden i popis všech úkolů, které se nacházejí v jednotlivých vrstvách protokolu. Základní funkcí každého otevřeného komunikačního standardu je zajištění přenosu dat z jednoho aplikačního procesu k procesu dalšímu.



Obr. 5. Komunikace mezi dvěma účastníky

Aby došlo ke správnému navázání komunikace a následné výměně dat mezi účastníky, musí být na obou stranách implementován stejný komunikační systém, který je složen z hardwaru a softwaru. Není nutnostní u sběrnicových systémů využívat všech sedm vrstev. Například sběrnicový systém KNX/EIB využívá vrstvy 1,2,3,4,7.[2]



Obr. 6. Sedmivrstvý referenční model OSI

1.3 PŘENOSOVÁ MÉDIA

- **Kroucený pár (TP)** – jedná se o metalické vodiče, které mají ve standardu KNX dvě definované provedení. Jejich vlastnosti jsou podobné a funkce identické. Napájení a přenos dat je veden po jednom krouceném páru (asynchronní přenos dat poloduplexním systémem).
  - **TP0** - převzaté ze standardu BatiBus - komunikační rychlost krouceného páru je 4.8 kbit/s, přístup na sběrnici CSMA/CA[1],
  - **TP1** - převzaté ze standardu EIB - komunikační rychlost krouceného páru 9.6 kbit/s, přístup na sběrnici CSMA/CA.
- **Napájecí po síťovém vedení (Power line)** - jedná se opět o metalické vodiče, které můžou být v rámci KNX provedeny ve dvou verzích, které mají stejné vlastnosti v podobě kódování komunikace SFSK (Spread frequency shift keying). Přenos dat je řešen asynchronním poloduplexním systémem.
  - **PL110** - převzaté ze standardu EIB - komunikační rychlost 1200 bit/s, nosná přenosová frekvence 110 kHz, přístup na sběrnici CSMA,

[1] CSMA s předcházením kolizím, Carrier Sense Multiple Access With Collision

- **PL132** - převzaté ze standardu EHS - komunikační rychlost 2400 bit/s, nosná přenosová frekvence 132 kHz, přístup na sběrnici CSMA.

- **Radiový přenos (RF) - bezdrátový** - standard KNX umožňuje bezdrátovou komunikace na frekvenci 868 MHz. Přenos dat může být jednosměrný, poloduplexní nebo obousměrný s rychlostí 32 kbit/s s kódovaným systémem FKS (Frequency Shift Keying) a metodou přístupu CSMA. Na likové úrovni jsou média specifikována standardem CEN TC294 z důvodu možného spojení různých hardwarových platforem. RF přenos pak splňuje doporučení ERC/REC 70-03 pro zařízení krátkého dosahu (Short Range Device) a Evropský standard ETS 300-220.
- **Infračervený přenos (IR) -** tento přenos byl plně převzat ze standardu EIB,
- **Ostatní –** je možné, také využít média, jejíž komunikace je založena na IP protokolu jako jsou Ethernet IEEE 802.2, WiFi /Wireless LAN (IEEE 802.11), Bluetooth, nebo FireWire (IEEE 1394). K takové komunikaci se využívá tzv. ANubis mód (Advanced Network for Unified Building Integration & Services).

1.4 SBĚRNICE LONWORKS

Sběrnice LonWorks byla v letech 1989 až 1992 americkou firmou Echelon Corporation, která při vývoji spolupracovala s firmami Toshiba a Motorola. Tento protokol má velkou výhodu v tom, že vlastní všech sedm vrstev referenčního modelu ISO/OSI. Těchto sedm vrstev můžeme rozdělit na jednu, která je programovatelná vývojáři a zbylých šest, které jsou obsaženy ve firmware (neuron-čip). Sběrnice LonWorsk se u nás na evropském trhu prosadila až v oboru automatizaci budov. Společnost Echelon Corporation pro výstavbu sítí LonWorks nabízí velké množství softwarových i hardwarových komponent. Jelikož technologii přijalo spoustu firem, tak není jedinou společností dodávající tyto komponenty na trh. [4]

1.4.1 Základní charakteristika LONKWORKS

Základem je protokol LonTalk, na které funguje celá síť. Funkce protokolu nám nabízí využití například při posílání potvrzovaných nebo nepotvrzovaných zpráv, periodické zasílání zpráv, mechanismus dotaz-odpověď, ale také hromadné rozesílání zpráv nebo pouze určité skupině. Další výhoda je implementace tzv. stavových proměnných, které si můžeme představit jako „přímé“ spojení dvou členů. Tato funkce lze využít při párování dvou členů, jako jsou výkonný člen a snímač. Přenos mezi těmato

zařízeními lze nakonfigurovat tak, aby daný snímač automaticky posílal informace ve formě paketů s měřenou hodnotou. Mezi charakteristické rysy sítě můžeme zařadit následující funkce:

- řízení a automatizace budov,
- řízení domácích spotřebičů,
- sledování spotřeby energií – vodoměry, spotřebiče tepla, odečet elektroměrů a plynoměrů,
- telekomunikace, přenosu zvuku,
- dálkové řízení libovolných procesů,
- bezpečnostní a požární zařízení,
- měření a Regulace (MaR),
- HMI (Human-Machine Interface) – zpracování přenesených dat od akčních členů, senzorů a klávesnic s následným zobrazením přímo na displeji,
- ovládání akčních členů - topná tělesa, motory, sirény apod.,
- nízké instalační nároky – pro instalaci a zprovoznění sítě můžeme využít stávající přenosová média domovních rozvodů televize, internetu, ale i napájecí sítě 230/400V,
- vysoká spolehlivost a zabezpečení sítě - speciální ověřovací algoritmus,
- dobrá flexibilita,
- kvalitní diagnostické možnosti - díky inteligentním uzlům sítě (Node),
- případné jednoduché programování – jako správce máme přístup k celému systému, takže si můžeme napsat svůj vlastní program na jeho funkce,
- 2 až 32000 zařízení připojených v síti,
- architektura peer-to-peer (P2P),
- komunikace Master / Slave,
- rozhraní pro RS-232, RS-485, ISA, VME, PCI.

1.4.2 Vlastnosti sítě LONWORKS

Sběrnice LonWorks využívá přímé komunikace mezi jednotlivými uzly systému (peer-to-peer). Hlavní priorita je přiřazena systému zasílání zpráv. Hlavním prvkem a základem celé sběrnice LonWorks je inteligentní uzel (Node). V tomto uzlu, který se nazývá Neuron chip, běží komunikační protokol LontTalk. Celý tento uzel je založen

na speciálních mikrokotrolérech. V uzlu jsou obsaženy samozřejmě i prky jako je tranceiveru[2], napájecí zdroj, externí paměť a další, které uzel potřebuje pro svou činnost. Velkou výhodou je nezávislost celého uzlu na přenosovém médiu. Toto přizpůsobení je realizované prostřednictvím tranceiveru, který dokáže zpracovávat přenášené pakety jak z párových vodičů, radiového přenosu, optických vláken, koaxiálního kabelu, radiový a infračervený přenos ale také elektrickým vedením 230/400V AC. Transceiver je umístěn na základní desce plošných spojů a pro každé stávající nebo nové přenosové médium jsou k dispozici různé transceivery.

Další výhodou je použití architektury peer-to-peer pro řízení přenosu a směrování paketů. Tato výhoda se dá například uplatnit v kombinaci s externí pamětí (I/O buffery) v Neuron chipu, aby se v případě nutnosti mohly pozastavit méně důležité zprávy, které se budou následně ukládat v paměti a dát přednost těm s vyšší prioritou.

1.4.3 Protokol LONTALK

Tento protokol, který byl navržen v roce 1989 firmou Echelon a standardizován jako EIA 709.1 Standard normou EN 14908, definuje přístup na sběrnici a řízení přenosu paketu (messages) po existující síti. Síťový protokol LonTalk byl navržen dle ISO OSI referenčního modelu (*Obr. 7*). To umožňuje, běžícím programům na aplikačním procesoru (CPU) komunikovat s aplikací běžící na jiném uzlu tvořeného Neuronovým chipem kdekoliv ve stejné síti. Služby protokolu, které jsou vyvolávány programy a objekty pracující na aplikační hladině OSI modelu. [5]

[2] Transceiver je zařízení, které integruje funkci vysílače (Transmitter) a příjmače (Receiver).

Obr. 7. Referenčního model OSI

1. FYZICKÁ VRSTVA OSI MODELU (PHYSICAL OSI LAYER)

Fyzická vrstva slouží pro příjem paketů po fyzickém komunikačním médiu. Protokol LonTalk umožňuje přenos po libovolném médiu, pro který existuje tranceiver. Ten je přímo napojen na piny Neuron chipu. Příklady médií pro přenos paketů:

- **kódování Manchester** - je způsob zakódování dat po krouceném páru vodičů izolovaných oddělovacím transformátorem a přenosovou rychlostí 78kbps až 1.25Mbps,
- **síťové vedení 230V** - současně se přenáší data, tak i datové informace (pakety). Komunikace po takovém napětí se řídí v Evropě standardem CENELEC (Evropský výbor pro elektrotechnickou normalizaci),
- **optické kabely** - v podobě dvou vláknového přenosu (jedno vlákno slouží pro přenos informací tam, druhé zpět) nebo jednovláknový přenosy (oba směry se šíří po jednom vláknu),
- **radiový přenos** - využívané pásmo pro radiový přenos je 49MHz, 400 - 450MHz, 900MHz, 1,2GHz nebo 2,4GHz s rozprostřeným spektrem,
- **infračervený přenos** - vhodný pro přenosové aplikace,
- **koaxiální kabel** - použití koaxiálního kabelu je vhodné pro vysokou rychlost přenosu.

Musíme brát v úvahu i fakt použití více druhů médií v jedné síti. Tuto možnost protokol LonTalk plně podporuje. Pokud bychom měli senzory ve vzdálené budově, můžeme využít síťové vedení pro přenos informace z objektu. V řídící stanici si pro místní přístroje zvolíme například zkroucený pár. Zároveň jsou podporovány vícenásobné kanály

pro komunikaci s možností připojení až 32385 uzlů. V tomto případě může být každá síť tvořena z jednoho nebo více kanálů, které podporují různé komunikační média. Pokud je síť složena z více kanálů, je třeba mezi ně vložit routery.

2. LINKOVÁ VRSTVA OSI MODELU (DATA LINK OSI LAYER)

Pro přístup se zde využívá metoda přenášení paketů CSMA/CA. Neuron chipy všech uzlů v celé sítí neustále monitorují komunikační kanál. Pokud na síti probíhá komunikace, nemají k ní uzly přístup. Jakmile je kanál volný, zašlou informaci a na konec informace přidají synchronizační bit. Po ukončené komunikaci každý uzel odpočítává tzv. Prioryty time slots. Je to čas, který můžou mít jednotlivé uzly jiný, podle stupně důležitosti. Pokud máme uzel s nastavenou vysokou prioritou, tak má přístupový čas menší než ten s nízkou prioritou. Odpočítávaný čas mu dřív vyprší a tím se dostane dřív na komunikační kanál, kde může zaslat pakety. Každý uzel má pro tento případ paměť (buffery), kde uchovává zpožděné informace, které stojí ve frontě na zaslání.

3. SÍŤOVÁ VRSTVA OSI MODELU (NETWORK OSI LAYER)

Linková vrstva data připravovala a odesílala a síťová vrstva zodpovídá za správné doručení dat (paketů) cílovému uzlu, popřípadě více uzlům. Pro správné identifikování uzlů se využívá 3 – úrovňové adresace.

4. TRANSPORTNÍ VRSTVA OSI MODELU (TRANSPORT OSI LAYER)

Zajišťuje spolehlivé doručení paketů s následnou zpětnou vazbou o správnosti doručení do cílového uzlu. Tato vrstva také ničí duplikátně vyslané pakety. Mezi hlavní funkce vrstvy patří čtyři základní služby:

- služba potvrzování došlého paketu či zprávy,
- služba zasílání zpráv typu broadcast,
- služba žádost / odpověď,
- služba nepotvrzeného zasílání zpráv.

5. RELAČNÍ VRSTVA OSI MODELU (SESSION OSI LAYER)

Pokud vysíláme data (pakety), tak požadujeme zpracování dat a následnou reakcí na zaslané informace. Tato vrstva protokolu LonTalk definuje standardní kódy zpráv pro síťový management a diagnostiku (diagnostika sítě a případné opravy). Tyto zprávy potom usnadňují instalaci a celé řízení sítě, kde tyto zprávy slouží pro konfiguraci a nastavení

Neuron chipu (obsah paměti EEPROM). Relační vrstva má také své bezpečnostní prvky pro ověřování zpráv. Ověřovací protokol, který umožňuje příjemci zprávy zjistit, zdali odesílatel je oprávněn tuto zprávu odeslat. Každý uzel má 48 – bitový ověřovací klíč, takže si může příjemce zprávy zkontrolovat, jestli se jeho klíč s přijatým shoduje a následně zprávu zamítnout nebo přijmout.

6. PREZENTAČNÍ HLADINA OSI MODELU (PRESENTATION OSI LAYER)

Slouží pro vyměňování informací mezi jednotlivými aplikacemi v rámci celé sítě. Došlý paket interpretuje jako:

- síťovou proměnnou
- cizí rámec
- explicitní zprávu

Aplikační data se většinou vyměňují prostřednictvím síťových proměnných, které zjednodušují vývoj a instalování systému. Tyto proměnné tvoří třídu zprávy, ve které jsou data označena jako Neuron C proměnná a tak je s nimi i zacházeno. Proměnné se řadí do skupin podle fyzikálního významu, včetně jednotek. Takto přenášené proměnné mají jasně stanovené, jakou informaci přenáší a jak s ní má druhá strana zacházet. Protokol LonTalk definuje několik standardních typů síťových proměnných (SNVT), které tvoří předdefinovanou skupinu která má přidělené fyzikální jednotky, jako jsou volty, ampéry, °C, sekundy apod.

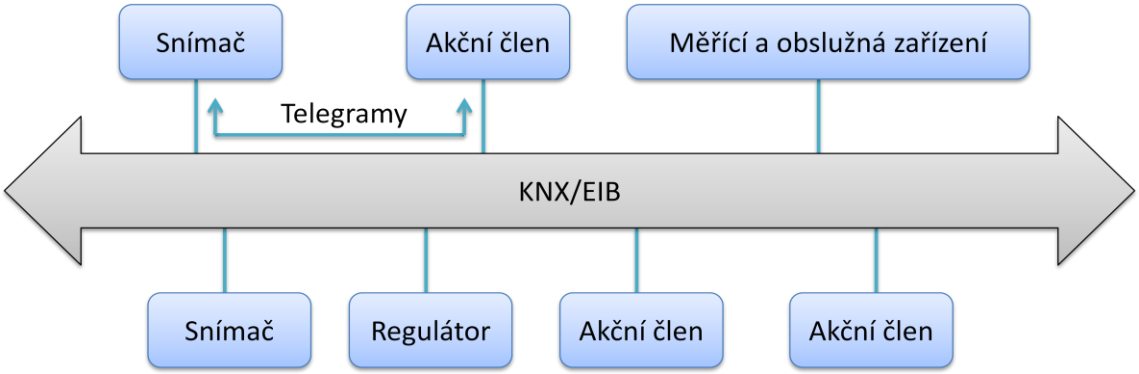
7. APLIKAČNÍ VRSTVA OSI MODELU (APPLICATION OSI LAYER)

Aplikační vrstva je jednou z hlavních, ve které běží samotný aplikační program, který definuje používané typy síťových proměnných, kódy explicitních zpráv apod. Obě strany, které pracují s proměnnou, by měly mít stejné aplikace, aby pracovaly a prezentovaly například stejné fyzikální jednotky. Výrobce většinou dává ke svým produktům seznam proměnných, které zařízení využívá.

1.5 SBĚRNICE KNX/EIB

Instalační sběrnice KNX/EIB je celosvětový uznávaný Evropský standard, který se v systémové technice a automatizaci budov používá pro síťové spojení řídících a regulačních zařízení, snímačů, akčních členů, obslužných a měřících zařízení. Instalaci

sběrnice KNX/EIB je možné provádět velice podobně jako instalaci sběrnice LonWors. To znamená, pomoci krouceného kabelu, silových vodičů, radiového přenosu, ale i optickými kabely. Výměna informací na této sběrnici probíhá přímo mezi jednotlivými členy, které realizují zadané funkce.



Obr. 8. Příklad blokového schématu sítě KNX/EIB

Standard KNX/EIB byl v roce 2003 ratifikován technickou komisí CENELEC, která ho začlenila do Evropské normy EN 50090 (Home and Building Electronic Systems). V polovině roku 2006 byla větší část normy převzata do norem ISO/IEC. To znamená, že zařízení různých výrobců, které jsou zkonstruovány pro sběrnicové systémy KNX/EIB musí mezi sebou komunikovat. Tyto zařízení jsou označena logem KNX a některé mají možnost napájení přímo ze sběrnice. Samozřejmostí je dodržení topologie sítě a protokolových standardů. [6]

1.5.1 Základní charakteristika KNX/EIB

Charakteristické rysy standardní konfigurace:

- **přenos dat** - různá rychlost přenosu 1,2; 2,4; 4,8; 9,6 nebo 32 kb/s (závislosti na použitém komunikačním médiu),
- **maximální velikost sítě –** do 1000 m, s maximální vzdáleností mezi zařízeními do 700m,
- **možnost adresace v síti** - přes 65 tisíc jednotek, až 256 v každé podsíti,
- **datové pakety** - volitelná délka 14 nebo 248 bajtů,
- **segmentace** - slouží pro vytváření rámců z větších bloků dat,
- **peer-to-peer** - komunikace s možností režimu Multicast a Broadcast,
- **přenosové standardy** - na 1. a 2. (Fyzické a Linkové) vrstvě OSI modelu.

1.5.2 Použití sběrnice

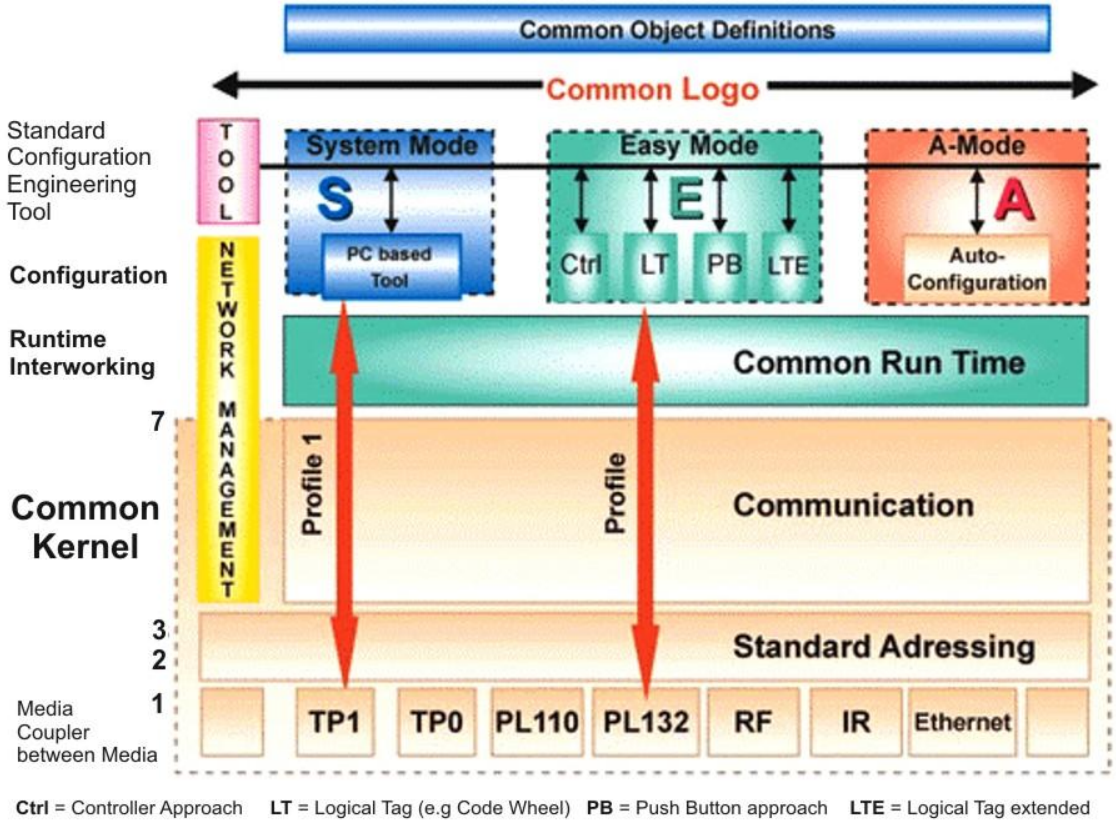
- řízení a automatizace budov,
- protipožární ochrana,
- zabezpečovací zařízení,
- dálkové řízení libovolných procesů,
- měření a Regulace (MaR),
- HMI (Human-Machine Interface) - zpracování přenesených dat od akčních členů, senzorů a klávesnic s následným zobrazením přímo na displeji,
- ovládání akčních členů - topná tělesa, motory, sirény apod.

1.5.3 Struktura komunikace KNX

Struktura sběrnice KNX se velice podobá OSI modelu. Jediným rozdílem je fakt, že nevyužívá všechny vrstvy. Pro její funkce stačí vrstvy 1,2,3,4,7. Pro dobré znázornění je zde vyobrazen model sběrnice, který je složen z bloků a komponent formulující síťovou komunikaci a rozhraní aplikace (*Obr. 9).*

1.5.4 Hlavní prvky sítě KNX

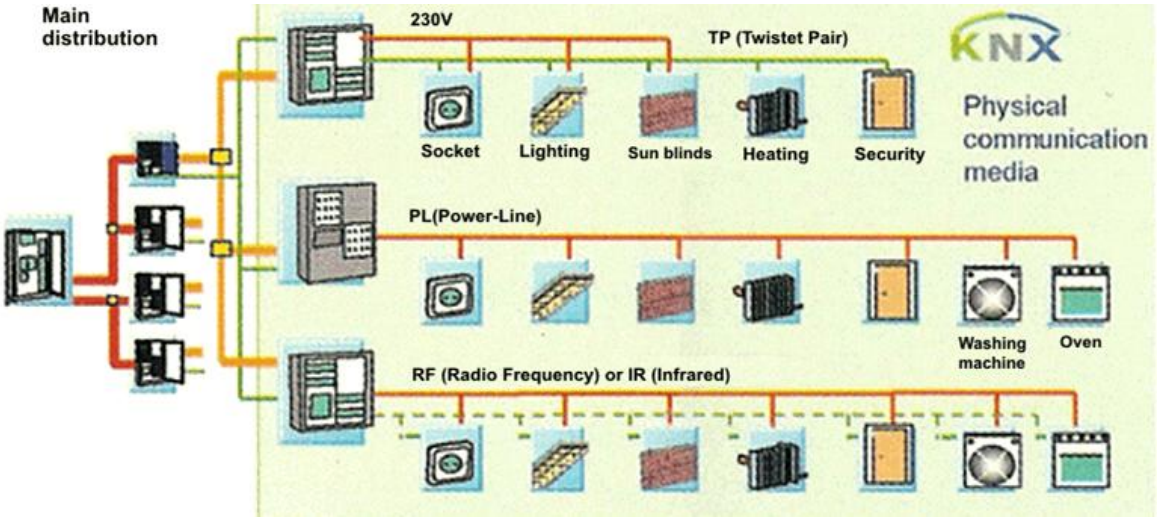
- **Common Object Definitions** - propojené distribuční aplikované modely pro zpracování a přizpůsobení různých úloh z oblasti automatizace budov.
- **Configuration Tools** – zde se jedná o tzv. konfigurační mód struktury KNX a přesné řízení všech síťových zdrojů a části distribuovaných aplikací, které můžou běžet na různých uzlech sítě.
- **Communication** (KNX Common Kernel) – jedná se o komunikační systém, sloužící pro správu přenosu dat po fyzickém médiu a protokolování zpráv. Další funkcí je podpora a vyřizování všech komunikačních požadavků pro řízení instalace, konfigurace systému a také řízení požadavků distribuovaných aplikací.
- **Média coupler** – je konkrétní hardwarový výstup (rozhraní), jeho prostřednictvím se připojuje zařízení na zvolený typ komunikačního média (TP1,TP0, PL110, PL132, RF, IR, Ethernet).



Obr. 9. Struktura KNX (čísla 1,2,3 a 7 znamenají číslo vrstvy OSI modelu) [6]

1. FYZICKÁ A LINKOVÁ VRSTVA

První vrstva KNX z pohledu volby fyzické vrstvy je nezávislá a umožňuje zvolit z několika známých standardů a dokonce je i kombinovat. Linková vrstva poskytuje konkrétnímu zařízení řízení přístupu na médium a základní řízení navázání vzájemné komunikace. Její provedení a funkce je přímo závislá na médiu, připojeného k jednotce.



Obr. 10. Příklad možností volby fyzického komunikačního média [6]

2. SÍŤOVÁ A TRANSPORTNÍ VRSTVA

Síťová vrstva provádí rozdělování rámců a řízení jejich směrování v celé síti. Transportní vrstva naopak vytváří komunikační propojení mezi uzly a řídí vyslání a příjem dat mezi nimi.

Struktura sítě - adresovací systém

V systému KNX může vzájemně komunikovat až 65 536 zařízení / uzlů pomocí 16bitového adresování. Celá síť KNX se skládá ze tří úrovní. První úroveň (nejvyšší úroveň) je centrální / páteřní, která má 15 hlavních linií (střední úroveň). Na každou z podsítí může být napojeno dalších 15 linií (nejnižší úroveň). Tímto struktura umožňuje připojit až 256 zařízení na jednu linku. Všech 256 zařízení bude zahrnuto do jedné skupiny zvané zóna (v celém systému 15 zón podle nejvyšší úrovně). Je ovšem nutné, do systému připojit oddělovač zón a linií, protože bez tohoto zařízení by byla struktura sítě omezena pouze na jednu linii. KNX umožňuje i integraci podsítě přes IP protokol. Pokud zvolíme komunikaci po napájecím vedení, provede se separování sousedních domén 16bitovou doménovou adresou. Počet připojených zařízení je ovlivněn instalační formou (typy transceiverů, přenášených médií, kapacita napájecího vedení). Dále to mohou být faktory, které ovlivňují zařízení z jejich okolí (elektromagnetické rušení). Pro segmentaci sítě a propojení linek typu krouceného páru s jinými médii můžeme použít přenosové mosty, opakovače, směšovače, paketové filtry a ochranné firewally.

Transportní vrstva může vytvořit 4 typy komunikačních propojení mezi komunikujícími uzly:

- jeden uzel komunikuje s mnoha dalšími (multicast),
- jeden uzel se všemi připojenými a komunikujícími uzly (broadcast),
- jeden uzel komunikuje s jedním uzlem (point-to-point).

3. KOMUNIKAČNÍ KNX RÁMEC (KNX FRAME)

Přenášení dat v síti je realizované prostřednictvím KNX rámce, který zajišťuje přenos všech potřebných informací zajišťujících správnou komunikaci zařízení a jednotek na sběrnici. Přenášená data mohou mít délku až 22 bajtů (*Obr. 11*). Cílová adresa je dána speciálním polem, které zároveň definuje délku rámce a čítání přeskoků. Standardní rámec může nést až 14 bajtů. Pokud bychom potřebovali přenášet větší objem dat, je možné provést segmentaci a tím rozšířit celý rámec až na 248 bajtů dat. Tento princip je kompatibilní se sběrnicí EIB. Velkou výhodou je poslední pole rámce (Frame Check), který slouží pro kontrolní součet pro zabezpečení přenosu dat a jejich konzistenci.

octet 0	1	2	3	4	5	6		7	8	N - 1	N ≤ 22
Control Field	Source Address		Destination Address		Address Type; NPCI length	TP CI	AP CI	data /APCI	data		Frame Check

Obr. 11. KNX rámec pro komunikaci a přenos sítí

7. APLIKAČNÍ VRSTVA

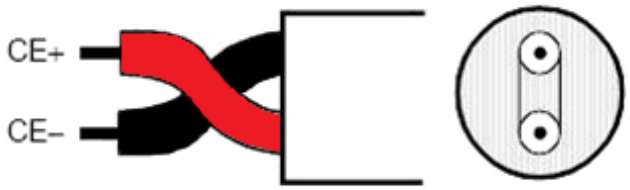
Touto vrstvou je realizováno množství služeb a aplikačních procesů, které se od sebe liší použitím typu komunikace transportní a nižší vrstvy. Služby související se vzájemnou komunikací mezi dvěma uzly (point-to-point) a komunikace uzlu se všemi připojenými (broadcast). Tyto komunikace slouží pro správu sítě. Třetí možností, která slouží pro provozní operace je komunikace s více uzly najednou (multicast). Velkou výhodou KNX je přizpůsobení zařízení, které se na síť připojují. Není nutností používat specifické zařízení nebo mikroprocesory.

VOLBA A PŘIPOJENÍ KABELŮ SBĚRNICE KNX

V síti KNX máme 4 možnosti komunikačních médií. Pro propojení zařízení a modulů prostřednictvím KNX, existujet 4 typy komunikačních médií (více o jednotlivých typech v kapitole 1.3): [6]

- **kroucený pár vodičů (TP)** - stále nejpoužívanější volba,
- **napájecí po síťovém vedení (PL)** – většinou se používají jen v nejnutnějším případě,
- **infračervený přenos (IR)**,
- **radiový přenos (RF)**.

V dnešní době mezi nejpoužívanější komunikační médium sloužící pro přenos informací mezi jednotlivými prvky v síti KNX/EIB a také pro napájení vstupních elektronických částí (liniových spojek), popřípadě připojených přístrojů a snímačů. Z důvodu indukčních rušivých vlivů se požaduje stínění kabelů. Vodič připojený ke kladnému pólu napájení je značený červenou barvou, vodič připojený k zápornému pólu je značen barvou černou (*Obr. 12*).



Obr. 12. Struktura základního kabelu TP1 pro KNX/EIB [7]

Pro napájení a komunikace postačuje jeden pár vodičů, ale je předepsáno používat kabelu, ve kterém je kromě černého a červeného párů, také pár bílí a žlutý (*Obr. 13*). Druhý pár je určen jako rezerva pro případ poškození některého s vodičů sběrnice. Sběrnicové kabely je možné klást v blízkosti silového vedení nízkého napětí, bez vzájemného rušení. Pro instalaci je také možné použít speciální ploché kabely, které lze propojit konektory. Tato možnost se využívá v objektech, kde často dochází ke změnám technologie provozu. Ploché kabely obsahují jak sběrnicové vedení sítě KNX/EIB, tak vedení silové a díky konektorům je daná část sběrnice velmi flexibilní.

Obr. 13. Kabel JYSTY 2x2x0,8 pro systémovou sběrnici KNX/EIB [8]

Při návrhu systému KNX/EIB je velice důležité dodržet podmínky vzdáleností. Čím větší vzdálenost komunikačních vodičů máme, tím větší úbytek napětí vzniká. Proto je nutné dodržet tyto podmínky pro instalaci.

První důležitou podmínkou je maximální délka jedné linie nebo jedné samostatně napájené větve, která nesmí být delší než 1000m s maximálním připojení 64 prvků. Při rozmístění prvků v jedné linii musí být jejich rozestup nejvíce 600m. Další podmínkou je vzdálenost od napájecího zdroje vedení, která je stanovena na maximální délku 300m. Pokud bychom potřebovali zapojit do sítě jedné linie dva zdroje napětí, musíme omezit průchod vyrovnávacím proudům dostatečným odporem sběrnice. Zdroje od sebe mají být vzdáleny minimálně 200m.Dodržení těchto podmínek je zárukou spolehlivé komunikace.

2 ČÁSTI SYSTÉMU INELS

Systém se skládá z celé řady akčních členů (aktorů) a senzorů, které tvoří ve výsledku funkční komplet. Vzhledem k velkému množství těchto jednotek bychom se v této kapitole zaměřili pouze na jednotky nutné k hlavním funkcím systému a jednotky zařazené do bezpečnostního průmyslu.

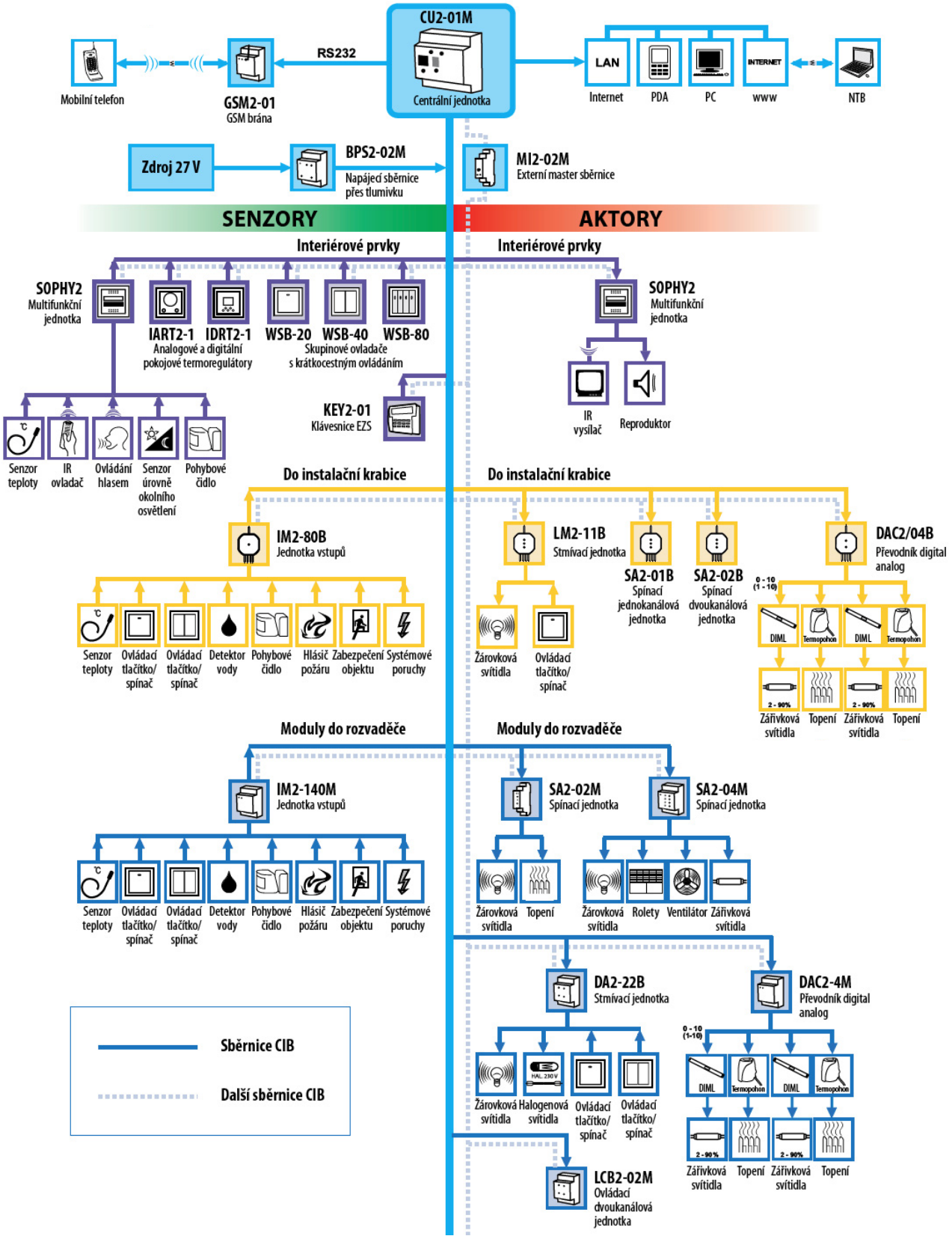
2.1 SBĚRNICE CIB

Sběrnice Common Installation Bus (CIB) byla vyvinuta společností Teco, a. s. Charakteristických rysem sběrnice je dvouvodičová soustava, která slouží jak pro napájení jednotlivých akčních členů a senzorů, tak i jako datová síť celého systému. Přenos dat je založen na modulaci napájecího napětí, přičemž toto spojení umožňuje rychlou komunikaci v celém systému.

Velkou výhodou celé sběrnice CIB je již zmíněný počet vedených kabelů a jejich připojení ke koncovému senzoru nebo akčnímu členu. Nutností připojení na sběrnici je pouze dodržení správné polarity vodičů (CIB+, CIB-). Systém má podobu stromové topologie, ale zapojení je libovolné, kromě zapojení do kruhu. Maximálně počet prvků, které se dají zapojit na jednu větev je 32 s tím, že centrální jednotka má tyto větve dvě.

Jako každý takový systém je i tento vybaven záložním zdroje energie pro případ výpadku a poruše napájení. CIB sběrnice má napájecí hodnotu 24 V DC, ale doporučuje se napětí 27 V DC z důvodu stálého nabíjení akumulátorů (2 × 12 V). Pokud dojde k výpadku energie ze sítě, tak bude fungovat veškerá komunikace, I&HAS a EPS na sběrnici. Naopak fungovat nebudou prvky, které pro svůj provoz vyžadují napájení ze sítě 230 V AC (osvětlení, elektrické zásuvky, vzduchotechnika, rolety, apod.).

Člověk dokáže vnímat okamžitou reakci pod 300 ms. Odezva sběrnicového systému CIB při maximálním počtu osazených jednotek na všech připojených větvích je pod 150 ms. Taková reakce je například pro regulaci topení zbytečná. Taková rychlost oceníme v případě přepnutí vypínače a následní rozsvícení nebo při přenosu dat z aktivovaného PIR (Passive infrared sensor) detektoru na základě zaznamenaného pohybu.



Obr. 14. Topologie CIB sběrnice s aplikací na systém INELS [13]

Adresace jednotek v síti je realizovaná prostřednictvím šestnáctibitové adresy, vyjádřené jako čtyři hexadecimální číslice uvedené na krytu jednotky. Po naistalování celého systému se programátor připojí do centrální jednotky prostřednictvím kabelu RJ-45, kde mu software automaticky načte všechny elektronické adresy připojených jednotek. V tabulce je vyplněna adresa jednotky, které programátor přiřadí jméno podle projektu a dále se pracuje už jen s tímto názvem.

Pokud by systém vyhodnotil jakékoli odpojení jednotek od sběrnice, tak samozřejmě může dojít k vyhlášení poplachu a přenosu informací na PCO. [10]

2.2 SOFTWARE PRO PRÁCI SE SYSTÉMEM

Mosaic

Je integrované vývojové prostředí, které umožňuje vytvářet aplikační programy pro PLC TECOMAT. Prostředí umožňuje programování v jazyce instrukcí (mnemokód), systémy s 32 bitovými procesory lze programovat také v jazycích podle IEC EN 61131-3 (Programmable controllers - Part 3: Programming languages). Součástí prostředí MOSAIC je i řada nástrojů usnadňujících vývoj a ladění aplikací.

Reliance

Je moderní SCADA/HMI systém určený pro monitorování a ovládání průmyslových technologií. Reliance je vyvíjena na základě dlouholetých zkušeností s budováním rozsáhlých aplikací a k jejímu zdokonalování přispívají i neustálé podněty ze strany zákazníků. Výsledkem je bohatě škálovatelný, bezpečný a robustní systém, optimalizovaný i pro velmi rozsáhlé aplikace.

IDM

Nový parametrizační SW v nabídce firmy Teco a.s. je určen pro snadné a rychlé nasazení moderního elektroinstalačního systému INELS. Je určen pro ty, kteří potřebují rychle nasadit systém a očekávají od něj pouze standardní funkce, obvyklé v systémech řízení budov, od řízení osvětlení, vytápění, klimatizace přes řízení spotřeby až po celkový dohled nad budovou, alarmová hlášení a základní komunikaci přes PC, respektive přes mobilní telefony.

Pro ty, kteří potřebují volně programovatelný systém, kdy je vyžadována speciální funkce nebo složitější integrace jiných subsystémů, jako například výtahů, parkovacích systémů, hotelových informačních a navigačních systémů, zůstává vždy k dispozici

programovací prostředí MOSAIC a centrální jednotka FOXTROT, se kterou jsou aktory a senzory elektroinstalace INELS plně kompatibilní. [12]

2.3 CENTRÁLNÍ JEDNOTKA

V dnešní době máme na výběr do pozice centrální jednotky ze dvou možností. První možností je výběr centrální jednotky CU2-01M, která byla navrhnuta přímo pro systém INELS. Její použití je určeno spíše pro řízení a bezpečnost v menších objektech jako jsou rodinné domy a menší objekty. Druhou možností je využití programovacích modulů Tecomat Foxtrot (CP - 10xx) firmy Teco, a. s. Obě tyto jednotky pracují na bázi programovatelných logických automatů PLC (Programmable Logic Controller) a již zmíněné CIB sběrnici. Základním rozdílem mezi jednotkami je možnosti připojení akčních členů, senzorů, funkcí jednotek a protokolem s kterým pracují. Obě tyto možnosti mají spoustu identických funkcí. Jednou z hlavních ze strany uživatele je ovládání a monitorování celého systému přes integrovaný WEB server prostřednictvím sítě internet. Programování centrálních jednotek CU2-01M a jednotek Tecomat Foxtrot (CP - 10xx) je možné v prostředí Mosaic. V současné době, jsou čtyři programovací jazyky prostředí Mosaic. Dva grafické – LD, FBD a dva textové – ST, IL (*Obr. 15*). [10]

Kodifikované označení v angličtině		Označení obvyklé v němčině		Vhodný název v češtině
zkratka	**název**	**zkratka**	**název**	
LD	Ladder Diagram	KOP	Kontaktplan	reléové schéma
FBD	Function Block Diagram	FUP	Funktionplan	jazyk funkčních bloků
IL	Instruction List	AWL	Anweisungsliste	jazyk mnemokódů
ST	Structured Text	ST	Strukturierter Text	strukturovaný text
SFC	Sequential Function Chart	AS	Ablaufsprache	jazyk sekvenčního programování

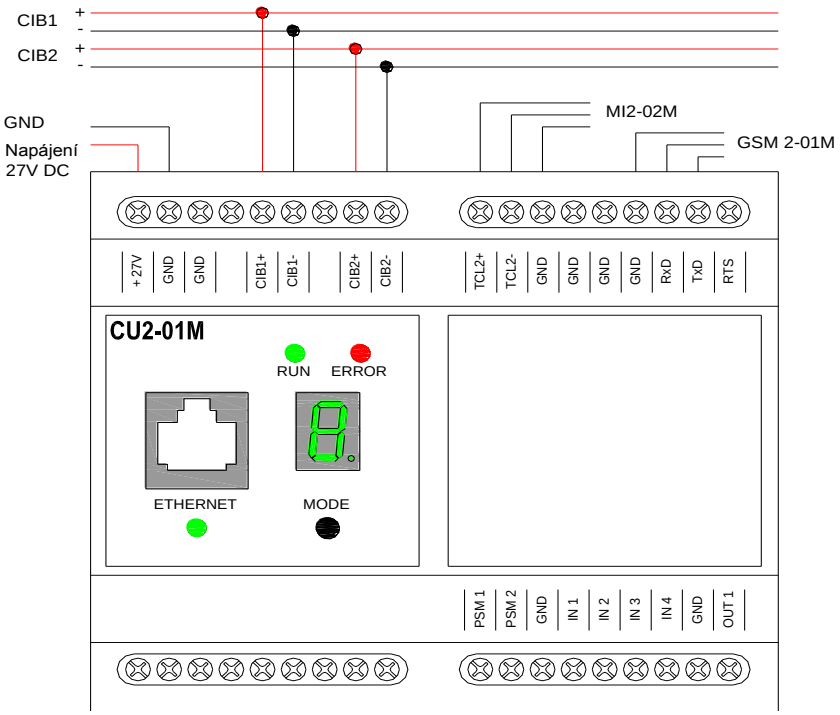
Obr. 15. Jazyky pro programování řídicích jednotek specifikované v normě IEC EN 61131-3 [11]

2.3.1 Centrální jednotka CU2-01M

Je mozkem celého inteligentního systému INELS, která podporuje protokoly TCP/IP, UDP/ IP, HTTP a jako systémová sběrnice je zde použito rozhraní RS485 (TCL2, 345kbit/s). Tato centrální jednotka vykonává široké spektrum funkcí, které zajišťují komfort a bezpečnost v daném objektu. CU2-01M je orientován do řízení obytných domů i větších objektů s důrazem na rychlé nastaveni – parametrizaci [3].

Nejběžnější funkce pro parametrizaci jsou ovládání teploty pro každou místnost, vypnout/zapnout osvětleni (ihned, se zpožděním), krátký/dlouhý stisk tlačítka, stmívání, zpracováni alarmů, odesílání a vyhodnocování SMS zprav (GSM2-01M), zadávání korekce požadované teploty, osvětleni ve skupinách a ovládání výstupních relé.

Nastavení jednotky CU2-01M je velmi jednoduché přes uživatelské prostředí programu INELS IDM, který je určitě pro operační systém Microsoft Windows. Pro volné programovaní, je zde prostředí Mosaic. Tato jednotka umožňuje připojení až 192 akčních členů a senzorů (64 přímo na CU2-01M + 128 na masterech MI2-02M).



Obr. 16. Centrální jednotka CU2-01M [12]

[3] Parametrizace je přiřazení funkcí jednotlivým členům, které provádíme bez větších znalostí programování.

2.3.2 Centrální jednotky TECOMAT FOXTROT (CP - 10xx)

Pokud bychom potřebovali více jednotek a funkcí, je možné jako mozek celého systému zvolit centrální jednotky Tecomat Foxtrot (CP - 10xx). Tyto jednotky jsou navrženy pro rozsáhlé objekty a automatizační haly. Nabízí i kromě rozhraní RS485 také RS232. Přes zmiňované rozhraní lze připojit k jednotce široké spektrum zařízení, které bezproblémově budou s celým systémem pracovat. Všechno záleží na konfiguraci řídícího programu centrální jednotky, podle kterého pracuje.

Centrální jednotky Tecomat Foxtrot jsou volně programovatelné modulární PLC, které se programují v prostředí Mosaic, kompatibilním s normou IEC EN 61131-3. Umožňuje připojit až 288 jednotek na sběrnici CIB. V současné době jsou nabízeny čtyři typy modulů, CP-1004, CP-1005. Další dva, CP-1014, CP-1015, CP-1016 jsou vybaveny navíc čtyřřádkovým displejem a šesti tlačítky (CP-1016 má tlačítek sedm). Každý tento modul má interní master CIB na který je možno připojit přímo 32 jednotek. Tyto centrální jednotky je možné rozšířit o dalších osm větví CIB.

Pro dálkový dohled a přístup do systému je využíváno připojení k místní síti a internetu, přes ethernetový port 100 Mb/s, nebo také zasílání SMS zpráv, pomocí připojeného GSM modulu GSM2-01 do kterého může být vložena SIM karta libovolného operátora. Ethernetový port je nejen určen pro parametrizaci, ale jeho prostřednictvím jsou přístupná také vnitřní data pro pohodlnou vizualizaci na PC, např. v programu Reliance 4.

2.4 EXTERNÍ MASTER MODUL MI2-02M

Externí modul MI2-02M umožňuje rozšíření počtu připojených jednotek do systému založeném na sběrnici CIB. Na zařízení je možné připojit až 64 jednotek, přičemž k základní jednotce CU2-01M je možné připojení pomocí komunikační sběrnice TCL2 dvou externích modulů, přičemž každý z nich přidá o 64 připojovaných prvků více. Připojení externích master modulů má výhodu i ve zvětšení rozsahu celé sítě, protože master modul můžeme umístit až do vzdálenosti 300 m od centrální jednotky a pokud bychom použili optický kabel, tak se nám vzdálenost zvětší na 1,7 km se stejnou rychlostí odezvy.

Výsledný počet jednotek v celém systému za použití 2 externích modulů a jedné centrální jednotky je 192. Tento modul je napájený přímo ze sběrnice CIB. [13]

2.5 ODDĚLOVACÍ MODULY BPS2-01M/02M

Tento modul zabezpečuje napájení dvou větví sběrnice CIB. V podstatě jeho činnost spočívá v oddělení zdroje napájení od vlastní komunikace na sběrnici CIB. Přímo na tento modul se připojuje záložní akumulátor 24V DC, který se neustále dobíjí jmenovitým napětím 27V DC. Modul je napojen na centrální jednotku, která dále napájí všechny akční členy a senzory v celé sběrnicové síti. Výstupy s modulu BPS2-02M jsou elektronicky chráněny proti přepětí a indikace připojení je znázorněna na čelním panelu pomocí LED (Light-Emitting Diode).

2.6 JEDNOTKY BINÁRNÍCH VSTUPŮ IM2-20B/40B/80B

Tato jednotka je pro nás z hlediska bezpečnostního průmyslu velice důležitá, protože nám slouží jako prostředník mezi sběrnicí CIB, tudíž centrální jednotkou a samotným zařízením, které používá na výstupu bezpotenciálový kontakt. V našem případě se jedná o spínače, přepínače, tlačítka, PIR detektory, požární hlásiče, plynové detektory apod. Na tyto jednotky lze připojit 2, 4 nebo 8 zařízení. Jednotku je možné díky malým rozměrům zabudovat do instalační krabice ve zdi. Pokud bychom potřebovali více připojených zařízení, tak můžeme zvolit modul IM2-140M, který je přizpůsoben montáži na DIN lištu v ústředně a umožňuje připojení až 14 zařízení s bezkontaktním výstupem. V jednotce je napěťový měnič, který 27 V DC promění na 12 V DC. Veškeré reakce na stavy přijaté tímto modulem můžeme parametrizovat v IDM nebo přímo programovat v prostředí Mosaic.

2.7 MULTIFUNKČNÍ JEDNOTKA SOPHY 2/2L

Jednotka SOPHY 2 má v sobě zabudovaný hlasový procesor podle kterého dokáže rozpoznat až 4 různé hlasy uživatelů. Každý tento uživatel má k dispozici 4 příkazy a následně 4 podpříkazy. Jednotka SOPHY2 v sobě obsahuje:

- snímač lidského hlasu,
- teplotní senzor,
- senzor intenzity okolního osvětlení,
- přijímač infračerveného (IR) signálu,
- vysílač infračerveného (IR) signálu,
- 1 dvoustavové tlačítko,

- 4 univerzální vstupy ovládané bezpotenciálovým kontaktem - na základě těchto vstupů (senzorů) lze pak ovládat různé akční členy zahrnuté v systému,
- reproduktor.

Informace ze senzorů můžou být užitečné i například při zabezpečení objektu. Pokud je systém v režimu střežení, tak kromě standardních jednotek pro zajištění bezpečnosti v objektu může složit i tato jednotka pro vyhodnocení poplachu prostřednictvím svých senzorů. [13]

2.8 SPÍNACÍ JEDNOTKY SA2

Spínací jednotky SA2-01B/02B/02M/04M/012M jsou určeny pro spínání od jednoho až po dvanáct spotřebičů (zátěží) jako jsou žárovky, motory, termoelektrické hlavice, topné rohože, atd. V centrální jednotce máme nastavenou adresu tohoto modulu s číslem výstupu, který chceme sepnout. Spínání je realizované prostřednictvím relé s bezpotenciálovým kontaktem. Maximální zatížitelnost kontaktu je 8 A/2000 VA/AC1.

2.9 GSM BRÁNA GSM2-01

GSM brána je určena pro příjem a odesílání zpráv SMS do a z centrální jednotky. Centrální jednotka může zprávy přijímat v podobě povelů, na které následně umí reagovat podle nastaveného programu. Pokud dojde k poplachu vyvolaným systémem I&HAS nebo EPS dojde k zaslání poplachové zprávy na PCO. GSM modul se připojuje přes rozhraní RS232 přímo k centrální jednotce a pracuje v pásmech 900/1800 Mhz.

Prostřednictvím software IDM může GSM modul obsluhovat 32 telefonních čísel, 48 odchozích zpráv o max. délce 20 znaků a 32 příchozích SMS o max. délce 20 znaků. Dále je možné nastavit 32 aktivních příchozích SMS o max. délce 20 znaků.

2.10 BEZPEČNOSTNÍ PRVKY SYSTÉMU

Systému INELS v sobě integruje I&HAS a připojení požárních hlásičů EPS na sběrnici CIB prostřednictvím modulů IM2-20B/40B/80B. Při narušení střeženého prostoru dojde k vyhlášení poplachu, který se prostřednictvím GSM brány nebo internetu zasílá na pult centralizované ochrany PCO a popřípadě i majiteli domu. Vyvolání poplachu nemusí mít za následek pouze informování pultu centralizované ochrany. V centrální jednotce lze nastavit provádění akcí, které by následovaly po narušení střeženého objektu.

Například je možné nastavit vytažení nebo shrnutí okenních rolet, rozsvícení všech světel v objektu nebo otevření vstupní brány. Taková nastavení jsou hodně individuální. [13]

2.10.1 Nástěnná čtečka karet WMR2-11

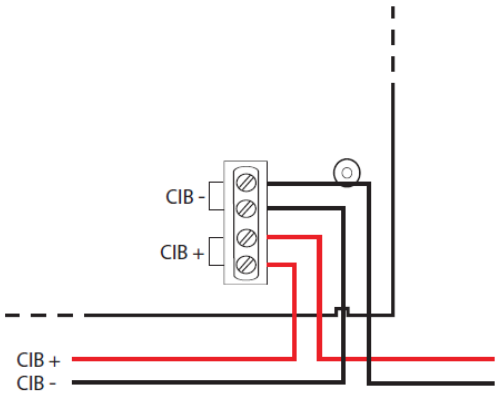
WMR2-11 je RFID zařízení, které je určeno pro čipové karety, klíčenky a podobná zařízení, které využívají RFID technologii. Modul podporuje RFID media s nosnou frekvencí 125 kHz a s IC type Unique 64 bits Ask Manchester (standard ID karet).

Centrální jednotka může být napojena na systém kontroly vstupu (ACCESS), přes komunikační rozhraní RS-485 nebo RS-232 a propojit tento systém s jednotkami WMR2-11 a následně vytvářet databázi pracovníků, jejich docházku a pohyb v celém objektu. Je možné také vytvořit grafickou vizualizaci v programu Reliance 4, díky které můžeme sledovat danou osobu a zjistit, kde se momentálně nachází.

Čtečky karet jsou koncipovány, tak aby zapadly do celého systémového designu, takže jsou velice podobné nástěnným vypínačům.

2.10.2 Zabezpečovací klávesnice KEY2-01

Klávesnice se připojuje přímo na CIB sběrnici systému INELS a jejím prostřednictvím ovládáme bezpečnostní systém v objektu. Přes klávesnici můžeme kontrolovat i osvětlení v objektu, vytápění, ale i jiné akční členy nebo senzory, které si v centrální jednotce nastavíme. KEY2-01 integruje čtečku RFID karet a čipů, takže po vstupu do objektu stačí přiložit kartu ke klávesnici a systém se odstřeží.



Obr. 17. Připojení KEY2-01 k sběrnici CIB [13]

2.10.3 Požární hlásič SD-280

Jedná se o kombinovaný optický kouřový hlásič. Tento požární hlásič při své aktivaci pošle signál do ústředny a zároveň je vybaven sirénou a červeným signálním světlem pro lokální varování. Jeho napájení je realizované prostřednictvím sběrnice CIB a zálohovaných napájecích zdrojů typu A nebo B dle ČSN EN 50131-6[4] Výstupní signál z poplachového hlásiče je ve formě reléového výstupu, který se připojuje k binárnímu modulu.

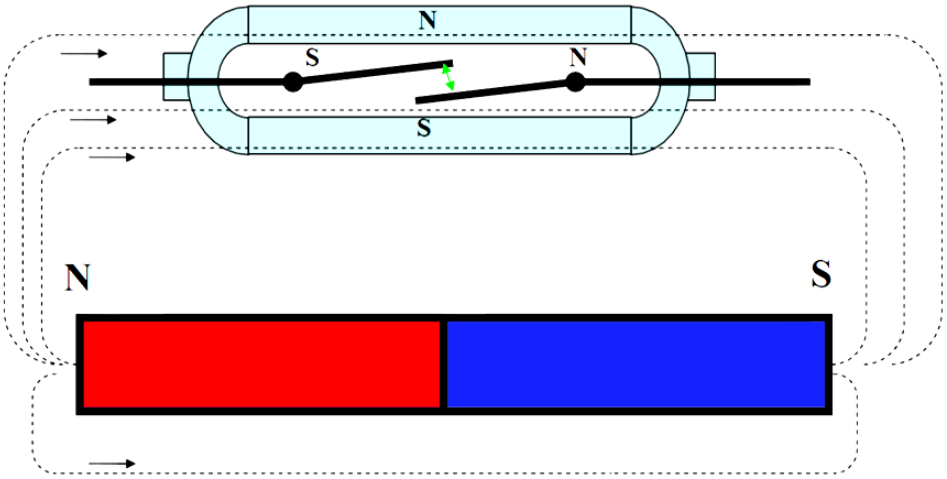
Optický hlásič kouře je citlivý na větší částice (hustý dým) a pracuje na principu rozptýleného světla. Z důvodu reakce na větší částice je v hlásiči vestavěn i detektor teplot. Mozkem celého hlásiče je mikroprocesor, který provádí analýzu měřených veličin a tím snižuje vyvolání falešných poplachů.

2.10.4 Magnetický kontakt

Magnetické kontakty jsou složeny ze dvou částí. První část je umístěna na okenním nebo dveřním rámu napevno. Tato část je tvořena jazýčkovým kontaktem ve skleněné trubičce s ochrannou atmosférou. Jazýčkový kontakt je nejčastěji vyráběn z permanentního magnetu.

Pokud jsou dveře nebo okno zavřené, permanentní magnet působí svým magnetickým polem na jazýčkové kontakty z feromagnetického materiálu a ty jsou spojené (sepnuté). Pokud je systém aktivován, následně dojde k otevření dveří nebo okna (vzdálení permanentního magnetu od trubičky s jazýčkovými kontakty), jazýčky spojeného kontaktu se ve chvíli vzdálení rozepnou a tím se vyhlásí poplach.

[4] ČSN EN 50131-6 - Poplachové systémy - Elektrické zabezpečovací systémy - Část 6: Napájecí zdroje



Obr. 18. Magnetický kontakt

2.10.5 Detektory pohybu

K systému INELS může být připojen libovolný detektor prostřednictvím modulu binárních vstupů IM2-20B/40B/80B. Pro zabezpečení objektu můžeme připojit zařízení, které slouží pro ochranu:

- **plášťovou** – magnetické kontakty, detektory na ochranu prosklených ploch, mechanické kontakty, vibrační senzor, rozpěrné tyče,
- **prostorovou** – pasivní infračervená (dále jen PIR), ultrazvukové, mikrovlnné a kombinované detektory,
- **předmětovou** - otřesové a kapacitní senzory, detektory na ochranu závěsných předmětů,
- **perimetrickou** - mikrofonické kabely a infračervené závory a bariéry, mikrovlnné bariéry a štěrbinové kabely, zemní tlakové hadice. [14]

2.10.6 CCTV

Pokud realizujeme inteligentní elektroinstalaci, je dobré do tohoto systému zahrnout i uzavřený televizní okruh CCTV. Systém INELS, respektive centrální jednotka dokáže zpracovávat signál z IP kamer prostřednictvím své síťové karty a připojení ve stejné síti. S tímto obrazem umí dále pracovat. Jednou z možností je uchovávání obrázků z jedné nebo více IP (Internet Protocol) kamer najednou. Je možné data ukládat přímo v centrální jednotce, která disponuje slotem pro SD (Security Digital) karty s pamětí až 32GB. Pokud bychom chtěli kameru ovládat, tak máme dvě možnosti. První možnost je ovládání přímo přes protokoly TCP/IP, UDP/IP nebo pomocí rozhraní RS232 a RS485.

Okamžitá vizualizace je možná na WEB serveru centrální jednotky, HMI operátorském panelu nebo přímo na televizi.

Při instalaci systému si můžeme zvolit tzv. INELS multimedia. Je to zařízení sdružující televizní anténu, satelit, internet, CCTV a samotný systém INELS. Výsledný signál se zobrazí na HMI panelu (*Obr. 19),* televizi (*Obr. 20)* nebo obrazovce počítače.

Obr. 19. IP kamera na HMI panelu [12]

Obr. 20. INELS multimedia [12]

2.10.7 ACCESS

Systém kontroly a řízení vstupu do chráněných prostor s možností sledování a vyhodnocení docházky. Tento systém je vhodné kombinovat se systémem CCTV a I&HAS. K systému INELS je možné připojit tento systém pro kontrolu a řízení vstupů, pokud je zařízení vybaveno správným komunikačním rozhraním jako je například RS-485 nebo Ethernet. Pokud ano, je možné propojit centrální jednotku a tudíž i kompletní systém se systémem kontroly a řízení vstupů. Pro přístup k datům získané systémem ACCESS stačí přejít na web server centrální jednotky nebo na vzdálený web server, se kterým centrální jednotka komunikuje a zasílá do něho veškeré informace. Vzdálený web server je nutný, pokud by mělo do centrální jednotky vstupovat více osob najednou. Po zadání ověřovacích údajů se dostaneme k celému systému tak, jak nám byl naprogramován.

3 BEZPEČNOSTNÍ TECHNOLOGIE SYSTÉMU INELS

3.1 TECHNOLOGIE RFID

Radiofrekvenční identifikace (RFID) je jeden z mnoha způsobů spolehlivé identifikace uživatele. RFID transpondér (nosič kódované informace) se skládá z antény, čipu, popřípadě i baterie. Komunikace mezi transpondérem a čtecím zařízením probíhá bezdrátově a bez přímé viditelnosti. Každý transpondér, respektive jeho čip nese identifikační číslo (neměnné po celou dobu životnosti), které může být za jistých podmínek unikátní. [15][16]

RFID transpondéry

Transpondéry můžeme rozdělit podle způsobu komunikace a podle typu paměti na aktivní, pasivní a semiaktivní. Aktivní mají v sobě baterii, která dovoluje neustále vysílat periodický signál do okolí. Pasivní z důvodu absence baterie samy vysílat nemohou. Čtečky neustále do okolí vysílají periodický signál. Pokud se pasivní RFID transpondér nachází v prostoru signálu, zachytí ho, impulzem nabije kondenzátor, který slouží jako momentální zdroj napájení a následně vyšle signál do okolí, který zachytí RFID čtečka. Semiaktivní transpondéry mají v sobě baterii stejně jako transpondéry aktivní, ale slouží pouze na prodloužení vzdálenosti mezi čtečkou a transpondérem.

Dosah signálu transpondérů je závislý na použité frekvenci:

- **nízkofrekvenční přenos** - (LF; 125 a 135 kHz) tento přenos se vyznačuje dosahem do 0,5 m a malou rychlostí komunikace. Jejich použití je vhodné ve vlhkém prostředí, čtení umožňují přes kapalinu a částečně i přes kov. Na této frekvenci pracují i RFID zařízení systému INELS.
- **vysokofrekvenční přenos** - (HF; 13,56 MHz) dosah do 1m, vyšší komunikační rychlost. Nevýhodou je menší vzdálenost čtení přes kapalinu nebo kov než u nízkofrekvenčních přenosů. Nejpoužívanější a nejlevnější.
- **ultravysokofrekvenční přenos** - (UHF; 860 až 960 MHz) velkou výhodou je vzdálenost do 3m a velká rychlost komunikace. Jejich použití je vhodné tam, kde je potřeba sejmout data za krátkou dobu (např. elektronické mýtné brány). První nevýhodou je čtení přes kapalinu nebo kov, které je téměř nemožné. Druhou nevýhodou je nejednotnost frekvence, která je jiná v Evropě, jiná v USA, Kanadě a Mexiku a také Asii a Japonsku.

- **mikrovlnný přenos** - (MW; 2,45 a 5,8 GHz) dosah až 10 m s velkou komunikační rychlostí až 2 Mb/s. Jejich konstrukce je mnohem složitější, tudíž celé zařízení dražší. Nevýhodou je zhoršená nebo žádná komunikace v blízkosti kapalin a kovů.

3.2 TECHNOLOGIE DETEKTORŮ

Mohli bychom zde popsat technologii všech bezpečnostních zařízení systému INELS. Těchto zařízení je široké spektrum, takže zde popíšeme pouze určitý okruh. [14][13]

3.2.1 Pasivní infračervené detektory

Činnost a princip infračervených detektorů PIR je založen na zachycení změn vyzařovaných z těles v okolí detektoru. PIR detektory pracují ve spektru infračervených vln o vlnové délce 760 nm až 1 mm. Tyto detektory využívají faktu, že každé těleso s teplotou vyšší jak -273 °C (absolutní nula) a nižší jak 560 °C vyzařuje vlnění v infračerveném pásmu. Příkladem je lidské tělo odpovídající vlnové délce 9,3 - 9,4 μm. Hlavním vyhodnocovacím prvkem celého detektoru je pyrocement. Je to kombinovaná polovodičová součástka na bázi tantalu a lithia, která má teplocitlivé prvky na infračervené záření. Pokud je prostor hlídaný PIR detektorem narušen a tím zaznamenán pohyb je vyhlášen poplach. Detektory mohou využívat dvojí optiku:

- **Fresnelovy čočky** – snímaný obraz je pomocí těchto čoček rozložen na několik zón (různé podle výrobců a způsobu záběru detektoru). Všechny zóny jsou soustředěny do pyroelementu.
- **Soustava křivých zrcadel** – jsou to dělená segmentovaná zrcadla vyráběná z plastu. Na povrchu je napařena kovová vrstva, která slouží jako odrazová plocha.

3.2.2 Ultrazvukové detektory

Pro svou činnost využívají část spektra neslyšitelné pro lidské ucho. Jsou to prvky aktivní. To znamená, že samotný detektor vysílá frekvenci nad 20 kHz. Tato vyslaná vlna je detektorem následně přijata a vyhodnocena jestli je ve stejném vztahu k vlně vyslané. Pokud je frekvence přijaté vlny stabilní, detektor je v klidu. Jakmile se přijatá frekvence změní, znamená to pohyb ve střeženém prostoru. Tento princip je založen na Dopplerovu jevu v pásmu ultrazvukových kmitočtů. Vztah může být vyjádřen pomocí následujícího vzorečku:

$$f_1 = \frac{f}{1-\left(\frac{v}{c}\right)^2}\ [Hz] \quad (1)$$

$\boldsymbol{f}$ – kmitočet vyslané vlny, $\boldsymbol{f_1}$ – kmitočet přijaté vlny, $\boldsymbol{v}$ – rychlost pohybu odrazené plochy

$\boldsymbol{c}$ – rychlost pohybu vlnění užitého k detekci.

3.2.3 Mikrovlnné detektory, bariéry

Mikrovlnné detektory a bariéry pracují na velmi podobném principu jako detektory ultrazvukové. Jediný rozdíl je jiná pracovní frekvence, která se pohybuje v oblasti elektromagnetického vlnění o vlnové délce větší než 1 mm a menší než 1 m, což odpovídá frekvenci 300 MHz – 300 GHz. V bezpečnostním průmyslu se používají zařízení pracující na frekvenci 2,5 GHz, 10 GHz, 24 GHz. Čím vyšší frekvence, tím se zmenšuje prostupnost elektromagnetických vln materiálnem. Tyto detektory jsou velice citlivé na rušivé elektromagnetickými jevy, jako je například spínání zářivkového světla, netopýři, myši.

4 NOVÉ TRENDY V TÉTO OBLASTI

V této kapitole bychom mohli uvést velice mnoho nových zařízení a technologií z oblasti bezpečnostního průmyslu. Dalo by se říct, že novým trendem v oblasti inteligentních budov se zaměřením na bezpečnostní průmysl je čím dál větší snaha o zakomponování systémů I&HAS, EZS, ACCES do samotných systémů inteligentních budov. Pokud by se podařilo sjednotit všechno tyto systémy tak, aby pracovali spolehlivě, bezpečně a jejich provedení s následnou instalací vyhovovalo veškerým normám, stačila by v objektu pouze jedna ústředna, která by řídila celý systém. Výrobci systémů inteligentních elektroinstalací se zaměřují převážně na sektory ovládání a regulace. Sektor bezpečnosti je samozřejmě funkční, ale je spíše okrajovou záležitostí. Mnohdy si prvky I&HAS, EZS a ACCES nevyrábí v rámci společnosti, ale nakupují od profesionálních výrobců, kteří se na bezpečnostní průmysl zaměřují.

4.1 BIOMETRIE

Biometrie pojednává o identifikaci a rozeznávání lidí na základě jejich odlišností, které jsou vrozené ve fyzických nebo fyziologických rysech. Pojem biometrie je shrnutí všech technologií, které můžeme použít pro identifikaci člověka. Rozdělení biometrické identifikace: [17]

- **Fyzické** - otisk prstů, rozpoznání obličeje, rozpoznání duhovky, geometrie ruky/prstů, rozpoznání hlasu, rukopis, dynamika úhozů na klávesnici, dynamika pohybu myší, ťukání.
- **Fyziologické** - sítnice, cévní řečiště, krev, srdeční puls, spektrum kůže, rentgen chrupu, zvukovod, geometrie ucha, rty, RFID nehtu, nehtové lůžko, DNA.

Nejběžnější používanou biometrickou ochranou je identifikace pomocí otisku prstu. Tento způsob je velmi spolehlivý. Pokud ho zkombinujeme s RFID kartou nebo číselným heslem, je zabezpečení na vysoké úrovni. Principem identifikace podle otisku prstu spočívá ve srovnání markant (Minutiae Points), které má každý člověk odlišné a hlavně na jiném místě otisku. Tyto markanty můžou mít 5 podob:

- rozvětvení,
- zakončení linie,
- bod, ostrůvek,
- krátká linie.

Obr. 21. Markanty [17]

Velkou výhodou biometrické identifikace je absence ztráty identifikačního zařízení (RFID karty, čipu). Z toho plyne, že identifikačním procesem na ověření totožnosti může projít jen osoba, která má daná povolení pro vstup nebo provedení přidělené operace. Otisk prstu má tři hlavní výhody:

- nelze je zapomenout nebo ztratit,
- použití zvládne i negramotný člověk,
- pro větší bezpečnost možná kombinace s jinými identifikačními prvky.

Otiskem prstu můžeme například autorizovat platební transakce, použít pro oprávněný vstup do místnosti nebo celého objektu. Pro snímání otisku prstu můžeme použít statickou metodu nebo metodu přejetí prstem.

4.1.1 Statické snímání

Je nejběžnější metoda, při které uživatel přitlačí otisk prstu na senzor, který otisk následně oskenuje a porovná s databází. Skenovací senzor musí být ve velikosti celého otisku prstu. Mezi velkou výhodu je jednoduché použití, které spočívá pouze v přiložení otisku na daný senzor. Tento senzor má ovšem mnohem více nevýhod:

- na senzoru zůstává skrytý otisk prstu,
- skenování může být zkomplikováno ušpiněním senzoru, který následně odmítne přístup osobě, která přístup má,
- uživatelé se musí naučit, jakou silou přitlačit otisk prstu na senzor, aby byla naskenována potřebná část pro identifikaci.

4.1.2 Snímání přejetím prstu

Senzor má tvar malého pásku, přes který uživatel plynule přejede svým prstem. Senzor zaznamenává informace o otisku prstu po páscích, které následně složí dohromady a porovná opět s databází. S tímto senzorem se můžeme setkat ve velké míře u notebooků. Tato technologie má pouze jednu nevýhodu, která spočívá v naučení „grifu“ pro přejetí prstu. Mezi výhody pak můžeme zařadit:

- senzor je neustále čistý (co přejetí, to očištění),
- na senzoru nemůže zůstat žádný skrytý otisk,
- uživatel má lepší pocit, který vyvolává nezanechání svého otisku na senzoru.

4.2 ZAKOMPONOVÁNÍ BEZPEČNOSTNÍCH PRVKŮ

Jak už bylo psáno na začátku kapitoly 4, je snahou zakomponovat bezpečnostní prvky do systémů inteligentních elektroinstalací. Konkrétním případem je připojení prvků I&HAS a EPS na sběrnici CIB, tak aby prvky komunikovaly s centrální jednotkou. V současné době pro připojení těchto prvků na sběrnici CIB slouží modul binárních vstupů, který funguje jako prostředník mezi centrální jednotkou a daným prvkem. Tato instalace vyžaduje větší prostorové nároky na umístění samotného binárního modulu. Pokud by se prvek I&HAS nebo EPS uměl připojit přímo na samotnou sběrnici, ušetřilo by se místo i náročnost instalace.

Tento způsob komunikačního provedení by měl i jednu nevýhodu. Jako samotné prvky celého systému by i tento uměl komunikovat pouze se zařízeními se stejným komunikačním protokolem. To by pro výrobní firmy inteligentních systémů znamenalo zaměření výroby i na prvky bezpečnostního průmyslu.

ZÁVĚR

Podstatou bakalářské práce bylo zjištění využitelnosti inteligentního systému INELS v bezpečnostním průmyslu a popsání jednotlivých bezpečnostních prků a technologií, kterými systém INELS disponuje.

První část práce se zabývá problematikou inteligentních elektroinstalací všeobecně i se zaměřením na bezpečnostní průmysl. Mezi další důležitý bod patří topologické znázornění sběrnicových systémů, které jsou následně rozkresleny a popsány. Od sběrnicové topologie je velmi blízko k samotné komunikaci systému s prvky připojené na sběrnici. Jsou zde popsány veškeré typy komunikačních médií, které lze v dnešní době použít a vzájemně kombinovat (v návaznosti na systém). Dále jsou v práci zahrnuty celosvětově uznávané komunikační standardy. Jsou zde popsány jejich charakteristiky, vlastnosti, použití, ale také principy funkčnosti a komunikace.

Druhá kapitola se zaměřuje na inteligentní systém INELS. Prvním bodem kapitoly je komunikační sběrnice CIB, na které je systém založen. Jsou zde opět popsány vlastnosti, charakteristiky, možnosti napojení, rozšíření a další důležité informace. V této kapitole jsou také popsány jednotlivé prvky systému INELS. Vybrány byly pouze prvky, které jsou pro systém z hlediska funkčnosti nezbytné a prvky spadající do bezpečnostního průmyslu.

Třetí kapitola pojednává o bezpečnostních technologií využívaných v inteligentních budovách se zaměřením na systém INELS. Je zde uvedena technologii RFID, používaná jako přístupový autorizační prvek do objektů nebo místností s omezeným přístupem. Tuto technologii je vhodné kombinovat s kamerovými a bezpečnostními systémy. Dále jsou popsány technologie a principy základních bezpečnostních detektorů.

Poslední kapitola pojednává o nových trendech v oblasti inteligentních budov se zaměřením na bezpečnostní průmysl, kde je uvedena biometrická identifikace a zakomponování prvků do systémů inteligentních budov.

CONCLUSION

The substance of this thesis was to determine usability of intelligent system INELS in the security industry and describes the various security elements and technologies which disposes of the INELS system.

The first part deals with smart wiring and generally focused on the security industry. Another important point is the topological representation of the bus systems which are described and embedding here. From the bus topology is near to the communication of system with elements which are connected to the bus. There is a description of all types of communication media which could be used and combined with each other (in relation to the system) today. The thesis also included world-renowned communication standards. There is s description of their characteristics, properties and uses but also principles of functionality and communication.

The second chapter is focused on the intelligent system INELS. The first point of chapter is a communication of CIB which is basic part of system. There are descriptions of the characteristics, features, connection options, extensions and other important information. This chapter also describes the various elements of INELS. There were selected only elements of the system in terms of functionality and the necessary elements within the security industry.

The third chapter discusses about the security technologies which are used in intelligent buildings with the focus on system INELS. There is a set of RFID technology, used as an access authorization element in buildings or rooms with limited access. This technology is good combined with a camera and security systems. The following describes technologies and principles of the basics security detectors.

The last chapter discusses about the new trends in intelligent buildings focusing on the security industry where indicated biometric identification of systems is and incorporating of elements to the systems of intelligent buildings.

SEZNAM POUŽITÉ LITERATURY

[1] MOTÝL, Petr. Výhody integrovaného přístupu k řízení techniky budov. AUTOMA [online]. 2010, 3, [cit. 2010-05-02]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=40765>.

[2] Zálešák, Martin,. Technika prostředí v oboru Integrované systémy v budovách = Environmental technology in the field of integrated systems in buildings : teze habilitační práce /- Ve Zlíně : Univerzita Tomáše Bati, 2009. 42 s. : ISBN 978-80-7318-834-4 (brož.).

[3] MERZ, Hermann, HANSEMANN, Thomas, HUBNER, Christof. *Automatizované systémy budov.* Vaclav Bartoš. 1. Vyd. Praha : Grada Publishing, a.s., 2008. 264 s. ISBN 978-80-247-2367-9

[4] VOJÁČEK, Antonín. Sběrnice LonWorks - 1.část - Úvod. [online]. 5.4.2005 , [cit. 2010-04-18]. Dostupný z WWW: < http://automatizace.hw.cz/mereni-a-regulace/ART151-sbernice-lonworks--1cast--uvod.html>.

[5] VOJÁČEK, Antonín. Sběrnice LonWorks - 2.část - LonTalk protokol. XXX [online]. 11.4.2005, 1, [cit. 2010-04-18]. Dostupný z WWW: <http://automatizace.hw.cz/mereni-a-regulace/ART152-sbernice-lonworks--2cast--lontalk-protokol.html>.

[6] VOJÁČEK, Antonín. Sběrnice KNX pro řízení budov : 1.část [online]. 1997-2009 [cit. 2010-05-02]. Dostupný z WWW: <http://www.automatizace.hw.cz/mereni-a-regulace/ART251-sbernice-knx-pro-rizeni-budov--1cast.html>.

[7] VOJÁČEK, Antonín. Sběrnice KNX pro řízení budov - 2.část - kabely, propojení a EIB [online]. 1997-2009 [cit. 2010-05-02]. Dostupný z WWW:<http://www.automatizace.hw.cz/clanek/2006082701>.

[8] www.phpe.cz [online]. 2009 [cit. 2010-05-13]. Co je inteligentní instalace?. Dostupné z WWW: <http://phpe.cz/Inteligentni.htm>.

[9] VALEŠ, Miroslav. *Inteligentní dům*. 2. vyd.: ERA, 2008. 136 s. ISBN 978-80-7366-137-3.

[10] KLABAN, Jaromír. Inels a sběrnice CIB – moderní systém inteligentní elektroinstalace. Automa [online]. 2008, 12, [cit. 2010-04-27]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=38218>.

[11] URBAN, Luboš. Programování PLC podle normy IEC EN 61131-3 – víc než jednotné jazyky. AUTOMA [online]. 2005, 2, [cit. 2010-05-13]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=30310>.

[12] Tecomat.cz [online]. 2005 [cit. 2010-05-02]. ŘÍDICÍ SYSTÉMY PRO STROJE, PROCESY A BUDOVY. Dostupné z WWW: <http://tecomat.cz/index.php?lang=cs&m1id=1&m2id=3&m3id=0&mid=185>.

[13] Systém inteligentní elektroinstalace [online]. 2010 [cit. 2010-05-04]. Produkty. Dostupné z WWW: <http://inels.cz/index.php?sekce=produkty&akce=show&id=56>.

[14] Ivanka, Ján,. Systemizace bezpečnostního průmyslu I/.3. vyd. Zlín : Univerzita Tomáče Bati ve Zlíně, 2009. 123 s. : ISBN 978-80-7318-850-4 (brož.).

[15] DOKOUPIL, Aleš. RFID z pohledu bezpečnosti. AUTOMA [online]. 2009, 07, [cit. 2010-05-04]. Dostupný z WWW: <http://www.odbornecasopisy.cz/index.php?id_document=39331>.

[16] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 2. autoriz. vyd.: Cricetus, 2002. 350 s. ISBN 80-902938-2-4.

[17] IMA.cz [online]. 2010 [cit. 2010-05-10]. Startpage. Dostupné z WWW: <http://www.ima.cz/download/cz/aktuality/2infodenima/14_Merka_Bull_Biometrika_IMA.pdf>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AC	Alternating Current
ACCESS	Systém kontroly vstupů
CCTV	Closed-circuit television
CIB	Common Installation Bus
CPU	Central Processing Unit
CSMA	Carrier Sense Multiple Access
CSMA/CA	CSMA s předcházením kolizím, Carrier Sense Multiple Access With Collision Avoidance
ČSN	Česká norma
DC	Direct Current
DNA	Deoxyribonukleová Kyselina
EEPROM	Electrically Erasable Programmable Read-Only Memory
EHS	European Home Systems
EIB	European Installation Bus
EN	Evropská norma
EPS	Elektronická požární signalizace
GSM	Global System for Mobile Communications
HF	High Frequency
HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol Overview
I&HAS	Sntruder and Hold-up Alarm Systém (poplachové zabezpečovací a tísňové systémy)
IDM	INELS Designer & Manager
IEC	International Electrotechnical Commission
IP	Internet Protocol

IR	Infrared
LAN	Local Area Network
LED	Light-emitting diode
LON	Local Operating Network
MW	Microwave
PCO	Pult centralizované ochrany
PIR	Passive infrared sensor
PLC	Programmable logic controller
RF	Radio frequency
RFID	Radio Frequency Identification
SCADA	Supervisory Control And Data Acquisition
SD	Secure Digital
SFSK	Spread frequency shift keying
SIM	Subscriber Identity Module
SMS	Short Message Service
SNVT	Standart Network Variable Types
TCP	Transmission Control Protocol
TP	Twist Pair
UDP	User Datagram Protocol
UHF	Ultra high frequency

SEZNAM OBRÁZKŮ