Přístup do BT přes síť TCP/IP a Internetu

Access to security technology over TCP/IP network and Internet

Jiří Ručka

Bakalářská práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2007/2008

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jiří RUČKA**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Přístup do BT přes sít TCP/IP a internetu**

Zásady pro vypracování:

1. **Proveďte rešerši podle typů a principů.**
2. **Vyberte nejpokročilejší technologie vzdáleného přístupu v oblasti BT.**
3. **Popište metody a princip vzdáleného přístupu do jednotlivých BT.**
4. **Realizujte jednu z aplikačních možnosti a navrhněte další možné řešení.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LAUCKÝ, V.: Technologie komerční bezpečnosti I., Univerzita Tomáše Bati, Zlín, 2004. ISBN 80-7318-194-0**
2. **KŘEČEK, STANISLAV A KOL.: Příručka zabezpečovací techniky, Blatenská tiskárna, s.r.o., Blatná, 2003. ISBN 80-902938-2-4**
3. **Kindl J.: Projektování bezpečnostních systémů I díl, vydaní 2004, ISBN 80-7318-165-7**
4. **UHLÁŘ, J.: Technická ochrana objektů II., PA ČR, Praha,2001. ISBN 80-7251-076-2**
5. **Lošťáková A.: Technická zařízení pro ochranu osob a majetku,**
6. **Katalogové listy a informační materiály firem – Variant**
7. **Katalogové listy a informační materiály firem – Eurosat**
8. **Katalogové listy a informační materiály firem – MacroWeil**
9. **Katalogové listy a informační materiály firem – Sicurit**
10. **ČSN EN 50 134 Poplachové systémy – Systémy přivolání pomoci.**

Vedoucí bakalářské práce: **Ing. Rudolf Drga**
Ústav elektrotechniky a měření

Datum zadání bakalářské práce: **22. února 2008**

Termín odevzdání bakalářské práce: **3. června 2008**

Ve Zlíně dne 22. února 2008

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Smyslem práce je odhalit a nastínit jednotlivé možnosti vzdáleného přístupu. Tyto jednotlivé možnosti pro danou technologii zpracovat tak, aby měly informativní charakter a poukázat na strukturu a funkci těchto systémů. Dále budou v práci popsány základní typy bezpečnostních technologií a stručně vysvětleny jejich funkce. Rovněž budou zmíněna zařízení, která jsou schopna převést signály a informace do technologií založených na TCP/IP protokolu. V praktické části zpracuji, popíši a následně předvedu, pomocí schémat a ukázky, jak takový vzdálený přístup k bezpečnostní technologii vypadá.

Klíčová slova: Bezpečnostní technologie, Internet, TCP/IP, EZS, EPS, CCTV, Přístupový systém

ABSTRACT

Sence of this baccalauréate work is disclose and show individual possibilities far away access. This individual possibilities work up for given technology so that this information have had information characters and refer to structure and function this systems. Further will describe basic types security technologies and shortly explain their functions. As well will refer to equipment, which can transfer signals and information to technologies found on TCP/IP protocol. I will cover and demonstrate, how this far away access to security technologies seems in practice part.

Keywords: Security technology, Internet, Transmission control protocol (TCP/IP), Electronic Guard systém (EZS), Electronic fire systém (EPS), Access kontrol (ACS)

Děkuji všem odborníkům, kteří reagovali na mé oslovení při vypracovávání bakalářské práce, především panu Jiřímu Absolonovi, Jiřímu Kolinskému, Janu Novotnému, Jiřímu Zahrádkovi, Františku Kňourkovi, Jaromíru Vomáčkovi, Martinu Štětinovi, Karlovi Mokrému a v neposlední řadě vedoucímu mé bakalářské práce Ing. Rudolfu Drgovi, za odborné rady, konzultace a poskytnuté materiály, jenž přispěly k jejímu vytvoření.

Děkuji mé rodině a obzvlášť mým rodičům, že mi dali možnost vzdělávat se a za jejich morální i psychickou podporu. Zároveň bych chtěl poděkovat všem mým přátelům za duševní oporu.

Prohlašuji, že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků, je-li to uvolněno na základě licenční smlouvy, budu uveden jako spoluautor.

Ve Zlíně 31.5.2008

…….
Jiří Ručka

OBSAH

ÚVOD

Na dnešním trhu se můžeme setkat s celou řadou bezpečnostních prvků a systémů, které se zabývají ochranou majetku a zdravím člověka. Pod slovem ochrana si lze představit nejen odolnost bezpečnostních systémů proti trestné činnosti, která je čím dál více rozšířená a pachatelé jsou vybaveni moderními prvky, ale zároveň, které umožňují do jisté míry poškodit bezpečnostní technologie. Na druhou stranu bychom měli majetek a zdraví chránit i z hlediska živelných pohrom. K tomu nám slouží požární systémy.

Výběr tohoto tématu byl založen na objevení možností, které nám Internet v dnešní podobě nabízí a do které se rozvinul v posledním desetiletí. Zároveň nám pomáhá zdokonalit se v oblasti, jenž se bude dle mého názoru do budoucna stále více uplatňovat a rozvíjet.

Internet a jeho propracovanost považuji za moderní technologii. Pomáhá nám v získávání všeobecných informací a slouží i jako komunikační prostředek mezi lidmi. Je to v současné době nejzajímavější možnost komunikace, ale i schopnost komunikovat a ovládat umělou inteligenci ukrytou v bezpečnostních zařízeních. Kombinací Internetu, bezpečnostních technologií a zařízení, která převádějí data do technologií založené na Ethernetu a TCP/IP protokolů lze specificky přistupovat vzdáleně k těmto systémům odkudkoli.

Firmy zabývající se montáží a instalací zabezpečovacích systémů, které budou nastíněny v bakalářské práci, jsou potom schopny připojit se přes Internet k těmto systémům a odstraňovat určité problémy, či zjišťovat stav jednotlivých systémů. Velká výhoda vzdáleného přístupu přes Internet k bezpečnostním technologiím spočívá v tom, že pracovníci jsou odpovědni za instalaci, konfiguraci či různé korekce systémů a nemusí být fyzicky přítomni v místě aplikace. Výsledkem tohoto řešení je efektivnost a časová nenáročnost, která snižuje náklady.

Smyslem práce je odhalit a nastínit jednotlivé možnosti vzdáleného přístupu a zpracovat je tak, aby měly informativní charakter a poukázat na strukturu a funkci těchto systémů. Dále bych chtěl v práci popsat základní typy bezpečnostních technologií a stručně vysvětlit jejich funkci. Rovněž se zmíním o zařízeních, která jsou schopna převést signály a informace do technologií založených na TCP/IP protokolu. V praktické části zpracuji a následně předvedu, jak takový vzdálený přístup k bezpečnostní technologii vypadá.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ TECHNOLOGIE

Na bezpečnostní technologie můžeme pohlížet ze dvou hledisek.

1.1 V širším slova smyslu

Vychází ze slova „Bezpečnost“, což znamená určitá ochrana před nežádoucími situacemi, které mohou vzniknout v důsledku protiprávního jednání potencionálních pachatelů a které mohou ohrozit majetek, popřípadě zdraví osob. Vzniká tedy jako reakce na dnes již rozsáhlou trestnou činnost. Cílem bezpečnostních technologií je zabránit, odradit a omezit trestnou činnost delikventů a v neposlední řadě také signalizovat narušení daného objektu.

1.2 V užším slova smyslu

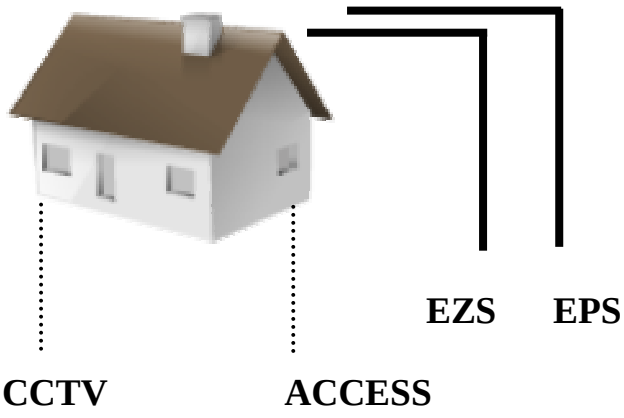
Jde o soubor technických zařízení, která slouží pro hlídání „bezpečného“ stavu, detekci negativní změny tohoto stavu, signalizaci a následné vyhlášení poplachu v daném objektu.

1.3 Rozdělení bezpečnostních technologií

Základní bezpečnostní technologie, které jsou zároveň nejrozšířenější jsou:

- EZS
- EPS
- ACCESS CONTROL
- CCTV

V dnešní době se setkáváme se zabezpečením objektů (firem, rodinných domů a jiných) pomocí systému EZS a EPS (viz kapitola 2 a 3). Jedná se o důležité základní technologie (Obr. 1), které mohou zajišťovat ochranu objektu. Systémy jako jsou CCTV či ACCESS, jsou považovány jako doplňkové (viz kapitola 4 a 5).



Obr. 1 Kombinace zabezpečení

Pozn.

▬ Hlavní (základní) zabezpečovací technologie

····· Doplňkové zabezpečovací technologie

2 VYBRANÉ MODULY A KOMUNIKATORY URČENÉ PRO KOMUNIKACI V ETHERNETOVÝCH SÍTÍCH

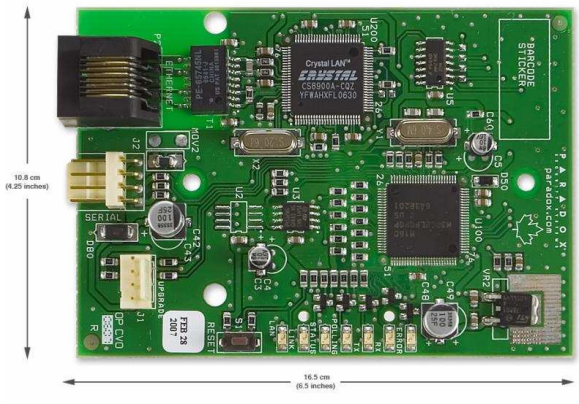
Kouzlo těchto zařízení spočívá ve vnitřním rozhraní pro Ethernetové sítě (TCP/IP). Také obsahují programovatelné vstupy a výstupy. Některé jsou specifické pro určité druhy systémů, jiné zase pracují individuálně a univerzálně pod jakýmkoli systémem. Některé se nastavují softwarem, jiné pouze přes webové rozhraní a k některým zařízením se pro nastavení komunikace musí přistoupit přes obě varianty (software i webové rozhraní).

2.1 B-NET (CENBNET)

Obr. 2 Modul CENBNET

- Modul pro připojení ústředny EZS (KYO320) do sítí LAN.
- Vzdálená správa.
- Webové rozraní.
- SW pro konfiguraci.

2.2 IP-100



Obr. 3 Modul IP-100

- Ethernetový komunikační modul Paradox IP100 umožňuje vzdálený přístup k ústřednám Digiplex EVO, Spectra série SP a magellan MG5000/5050 pomocí síťového rozhraní.
- webové rozhraní.
- SW pro nastavení IP adresace.

2.3 SpringNET

Obr. 4 Komunikátor SpringNET

- Univerzální modul pro různé úlohy automatizace a dálkovou správu objektů v rámci lokální sítě i dálkově přes INTERNET.
- Webový server Lantronix.
- SW pro nastavení parametrů pro sítě.

2.4 SmartLAN

Obr. 5 Komunikátor SmartLAN

- LAN komunikátor pro vzdálenou správu a komunikaci (web rozhraní, zasílání stavových emailů včetně příloh – mapy objektů).
- Pro EPS systémy INIM.

2.5 E080

Obr. 6 Modul E080

- Kombinuje prvky komunikačního zařízení a zařízení pro vzdálenou údržbu.
- Pro monitoring, správu uživatelů a konfiguraci ústředen v prostředí podnikových sítí LAN a WAN s protokolem TCP/IP.
- Připojuje se přímo na datovou sběrnici ústředny a do sítě Ethernet.
- Komunikuje s programem pro konfiguraci ústředen a dálkový servis Galaxy Gold nebo s programem pro správu uživatelů Security Director's Gold, který je určen pro správce systémů, programem Alarm Monitoring s možností ovládání podsystémů.

3 ELEKTRICKÁ ZABEZPEČOVACÍ SIGNALIZACE (DÁLE JEN EZS)

Problematikou EZS se zabývá norma ČSN EN 50 131-1 až 7.

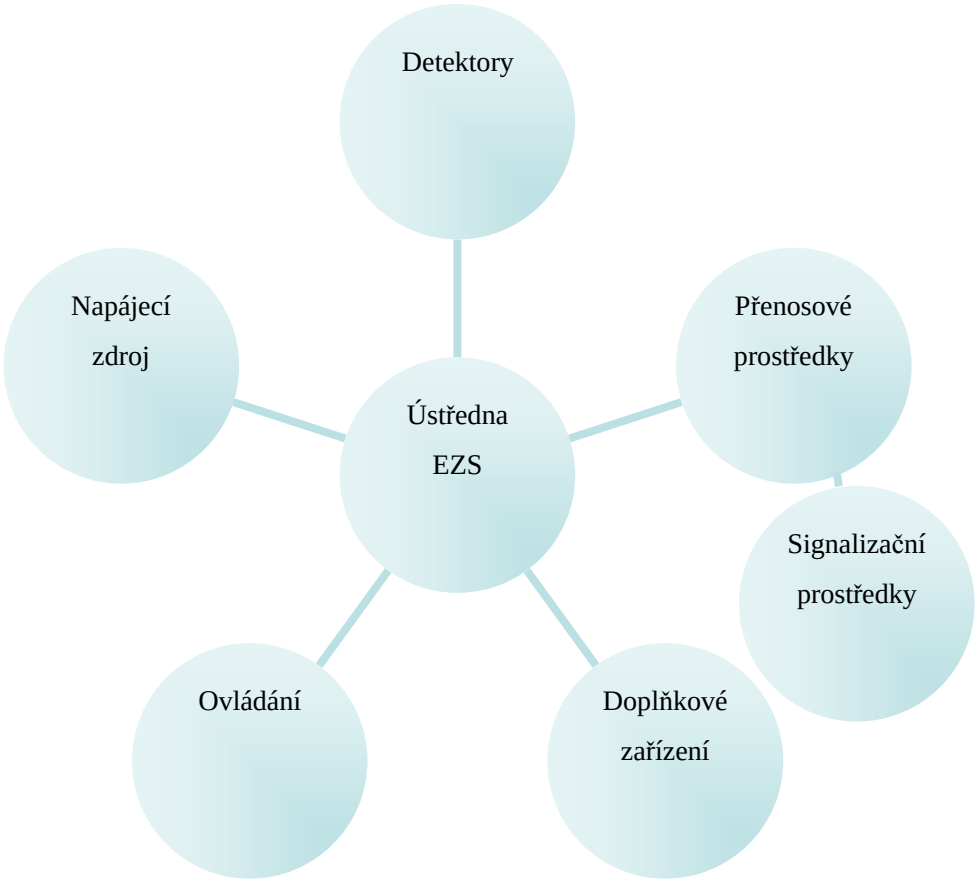
Obr. 7 Ústředna EZS s klávesnicí

Zařízení elektrické zabezpečovací signalizace:

Jde o soubor detektorů, tísňových hlásičů, ústředen, prostředků poplachové signalizace, přenosových zařízení, zapisovacích zařízení a ovládacích zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno na určitém místě narušení střeženého objektu nebo prostoru. [1]

Výsledným komplexem je zde elektronický zabezpečovací systém, což je poplachový systém pro detekci a signalizaci přítomnosti, vstupu nebo snahu o vstup pachatele do střeženého prostoru či objektu.

Jednotlivé EZS jsou složený z jednotlivých částí, které vykonávají určitý úkol a v souhrnu vytvářejí tzv. zabezpečovací řetězec.



Obr. 8 Blokové schéma řetězce EZS

Jedná se o stavebnicový systém, který lze postupně rozšiřovat. Ovšem základem při střežení či zajištění objektu je mechanické zajištění a elektronické zařízení slouží jako jeho doplněk.

3.1 Ústředna EZS

Hlavní funkcí ústředny EZS je sběr informací o stavu jednotlivých poplachových detektorů a na základě rozhodovací jednotky správně vyhodnotit tyto informace k vyvolání poplachového signálu.

V dnešní době se ústředny modernizují v hardwaru. Od několika i tisíc součástek, které obsahovaly ústředny se pomalu přešlo na stovky integrovaných obvodů. Nyní lze říci, že

tento systém dnes pracuje na bázi mikroprocesorů a jejich pomocných obvodů, integrovaných komparátorů, multiplexerů, A/D převodníky atd.

Podle třídy prostředí a způsobu použití ústředny se dnes vyrábí řada malých a středních ústředen s jedním až dvěmi speciálními obvody. Není ani výjimkou disková jednotka u ústředen pro rychlé přeprogramování, rychlý přenos dat či jejich archivaci.

V praxi se setkáme s řadou ústředen EZS, které mají jinou základní podstatu v elektronice, programovém vybavení, způsobu signalizace, ovládání a v neposlední řadě také připojováním vstupů a výstupů.

Ústředna EZS jako celek plní takovouto funkci:

- Přijímá a vyhodnocuje výstupní elektrické signály od detektorů
- Indikuje a vysílá informace o svém stavu systému
- Ovládá poplachové, signalizační , přenosová, zapisovací zařízení a jiné, která signalizují narušení
- Dodává elektrickou energií detektorům nebo dalším prvkům EZS
- Pomocí zámků (elektromechanických nebo kódových) či ovládacích klávesnic, je schopna uvést celý systém EZS nebo jeho určité časti do stavu střežení či do klidového stavu.
- Umožňuje diagnostiku EZS (narušení smyčky, vadný detektor, poruchy ústředny)

3.2 Stupeň vybavenosti ústředny EZS

Vyjadřuje odolnost systému vůči překonání a tím vyřazení celého systému nebo jeho části z funkčního provozu. Určitý stupeň vybavenosti určuje riziko chráněného objektu a stupeň zabezpečení, pro který mohou být použity. Ústředny EZS tedy dle stupně vybavenosti dělíme do čtyřech skupin pro riziko:

- **Stupeň 1: nízké** – předpokládá se, že narušitelé mají malou znalost EZS a že mají k dispozici omezený sortiment snadno dostupných zdrojů.
- **Stupeň 2: nízké až střední** – Předpokládá se, že narušitelé mají určitou znalost EZS a že použijí základní sortiment nástrojů a přenosných elektronických přístrojů.

- **Stupeň 3: střední až vysoké** – Předpokládá se, že narušitelé jsou obeznámeni s EZS a že mají úplný sortiment nástrojů a přenosných elektronických přístrojů.
- **Stupeň 4: vysoké** – Předpokládá se, že narušitelé mají podrobné informace pro zpracování podrobného plánu vniknutí a dále že mají kompletní zařízení a prostředky umožňující nahradit rozhodující prvky.

3.3 Způsob připojování smyček ústředny EZS

Vychází z prostého připojení smyček k ústředně EZS tak, aby bylo zajištěno především kvalita připojení a vhodná volba připojení, především dle typu objektu a možnosti instalace v objektu. Jinými slovy nezáleží jen na stupni zabezpečení EZS či jejich programování, ale na vhodném připojení smyček.

Smyčka – jedná se o skupinu detektorů, tísňových hlásičů nebo sabotážních kontaktů, které jsou propojeny společným vedením a na výstupu ústředny EZS vyhodnoceny.

Typy připojení smyček k ústředně:

1. **Analogové - smyčkové**
2. **Sběrnicové - s přímou adresací detektorů**
3. **Koncentrátorové – smíšené**
4. **Bezdrátové**
5. **Hybridní**

3.3.1 Analogové – smyčkové

Analogové ústředny poznáme tak, že každá poplachová smyčka je připojena do samostatného vyhodnocovacího obvodu ústředny. Vyhodnocovací obvod ústředny je řešen pro připojení proudové smyčky o určité hodnotě a toleranci.

U systému se smyčkovou ústřednou je negativní věcí rozsáhlá kabeláž, jelikož ke každému detektoru musí být připojen kabel příslušné smyčky. Kabel zpravidla obsahuje dva vodiče pro napájení (u napájených detektorů), dva vodiče pro poplachový kontakt detektorů, dva vodiče pro sabotážní kontakt detektorů a další vodiče pro další specifické funkce (indikace zakrytí detektoru, paměť na poplachové události atd.)

Možné řešení přenosu informace od detektorů k ústředně po smyčce:

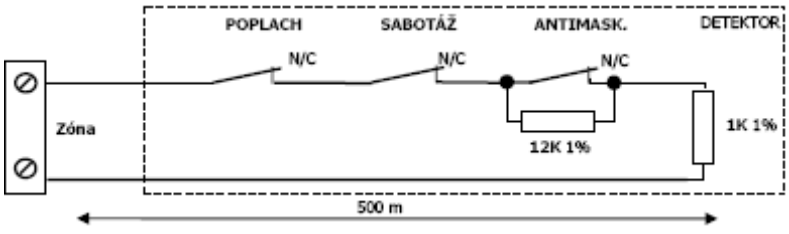
Rozpínací kontakt

Jde o jednoduché zapojení, kdy rozepnutím vzniká aktivace. Smyčka je nepřetržitě hlídaná proti přerušení. Nevýhodou je možnost zkratování celé smyčky a to jednak skřípnutím kabelu nebo sabotáží (úmyslně). Bohužel není zcela zaručena funkčnost detektorů při zkratu v kabeláži či svorkovnici. Použití se objevuje u požárních hlásičů anebo u detektorů elektrické zabezpečovací signalizace použitých v bytovém prostoru.

Jednoduše vyvážená smyčka

U této varianty dochází k hlídaní klidového stavu smyčky pomocí definovaného odporu (hodnota záleží na nastavení vstupu ústředny). Pokud dojde ke změně odporu, smyčka bude aktivována. Ve většině případů se využívá tolerance ve změně odporů (až 30% jmenovité hodnoty) a to proto, aby byla hlídána cela délka vyvážené smyčky. Odpor se umisťuje do nejvzdálenějšího bodu (poslední detektor). Zapojení pomocí odporu se používá pro více detektorů zapojených do jedné smyčky. Kontakty jsou zapojeny do série a vyvažovací odpor je vložen do nejvzdálenějšího kontaktu. Nevýhodou je při zapojení více detektorů do série, že nám není známo přesné místo aktivace smyčky.

V případě, že ústředna má několik drátových smyček, pak se doporučuje připojit každý detektoru na jednu smyčku.

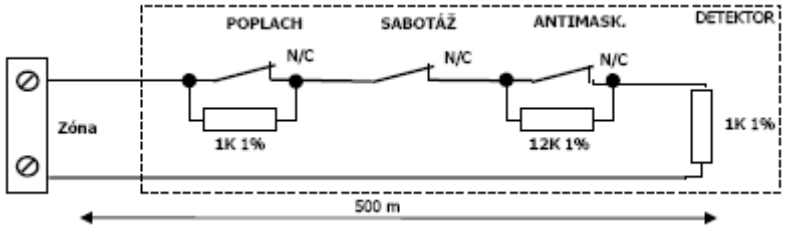


Obr. 9 Jednoduše vyvážená smyčka

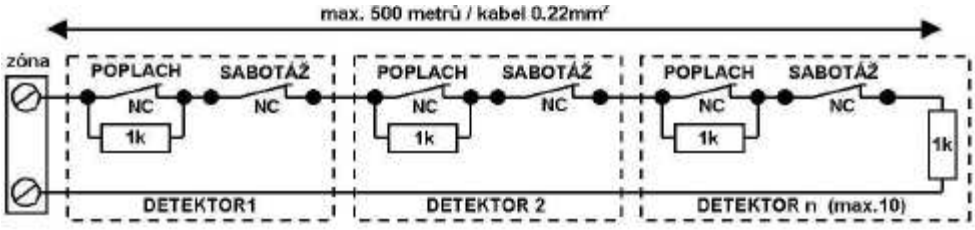
Dvojitě vyvážená smyčka

Z detektoru se přenášejí většinou dva signály. Jeden informuje o aktivaci detektoru a druhý signál zaznamenává sabotáž (narušení krytu). Jeden odpor přenáší klidový stav a druhý přenáší aktivaci detektoru. Pro klidový stav je nastavena základní hodnota odporu

(tolerance až 30%). Po jejím dvojnásobném překročení dojde k aktivaci. Do aktivaci sabotáží nepatří jen otevření krytu detektoru, ale i zkrat nebo rozpojení smyčky. [3]



Obr. 10 Dvojitě vyvážená smyčka



Obr. 11 Vyvážená smyčka pro více detektorů

3.3.2 Sběrnicové – s přímou adresací detektorů

Ústředny sběrnicové pracují na principu digitální datové komunikaci po sběrnici a to zapojením ústředna – detektor. Nedílnou součástí každého detektoru je komunikační modul. Na základě tohoto předpokladu ústředna v určitých časových obdobích vysílá signál pro aktivaci adresy jednotlivých detektorů a přijímá jejich odezvu.

U tohoto systému je výhodná minimální kabeláž (libovolná konfigurace kabelové sítě), detektory mohou být zapojeny v jakémkoli pořadí a používá se čtyřvodičová sběrnice, kde dva vodiče vykonávají potřebu pro napájení detektoru a dva vodiče datovou sběrnice. Jednou z dalších výhod je jednoznačná adresa detektorů, která hraje důležitou roli v případě vyhlášení poplachové situace, kdy nám ústředna ukáže, který konkrétní detektor byl aktivován a o jaký druh narušení objektu jde (poplach, sabotáž, zkrat atd.). V neposlední řadě přenosové trasy jsou značně odolné proti překonání, proto je ještě výhodnější tento systém použít tam, kde se nachází místo trvalé obsluhy nebo je-li přenos na pult centralizované ochrany, nebo na pult hlídací služby veden vícekanálově. Lze také

v libovolném čase ovládat pomocí softwaru u moderních ústředen tohoto typu, kterýkoliv detektor ze smyčky a přiřadit mu mód střežení nebo odchod z módu střežení.

Nevýhoda u tohoto typu se nachází v celkové délce vedení, z důvodů úbytku napětí, rovněž nemožnost dodatkových funkcí detektor, byť se firmy zabývající se výrobou snaží o výrobu detektorů s vlastním mikroprocesorem pro zpracování doplňkových funkcí.

3.3.3 Koncentrátorové – smíšené

V této době patří koncentrátorové – smíšené ústředny k nejrozšířenější. Jedná se o kombinaci sběrnicových ústředen a smyčkových ústředen. Pro komunikaci mezi ústřednou a detektorem se používá koncentrátory (expandéry), které se jeví jako pod-ústředny a komunikují s ústřednou po datové či analogové sběrnici (jedné i více). Koncentrátor plní funkci rozšiřitelnosti systému o další poplachové smyčky. Detektory jsou zapojeny ke koncentrátorům za pomocí smyček. Vyhodnocování probíhá různě dle typu ústředny. Varianty jsou:

- Analogový multiplex – jednotlivé smyčky se připojují na sběrnici a vyhodnocení impedance smyčky s určitou odezvou provádí ústředna.
- Integrace vyhodnocovací logiky včetně vyrovnávací paměti přímo do koncentrátoru. Naprostá datová podoba komunikace.

Je-li kapacita ústředny nedostatečná, nelze připojit na každý vstup koncentrátoru jednotlivé detektory. Tím se neušetří kabelové vedení a musel by se každý detektor připojit kabelem až přímo do ústředny. V opačném případě stačí přivést kabel k nejbližšímu koncentrátoru. Pak můžeme mluvit o ústředně s přímou adresací detektorů a tím přebírá všechny výhody tohoto systému.

Používá se tento systém pro rozsáhlé objekty a při realizaci je potřeba přizpůsobit systém nákladům na zřízení a zvolit správnou úroveň adresace detektorů (tedy rozdělení detektorů do smyček). Nesmíme ani zapomenou na správné dimenzování, jak datových tak napájecích vodičů v rozsáhlém systému. Lze realizovat dodatkové funkce přes datovou sběrnici.

3.3.4 Bezdrátové

Bezdrátové ústředny mají své specifika především své frekvenční pásmo kolem 430MHz s výkonem 10mW a také přenos poplachové informace od detektoru je 8bitový, kódovaný a adresa detektoru je 4bitová. Podstatou realizace bezdrátové ústředny je, co nejmenší klidový odběr. Dosah je zpravidla 100 – 200m, ale v objektu z důvodů stínění (zdi, dveře) musíme počítat s menším dosahem. Detektory jsou napájeny 9V článkem nebo lithiovou baterií. Pokles napětí na jednotlivých detektorech je hlídaný akusticky, ústřednou popřípadě samotným detektorem.

Bezdrátové mají své opodstatnění především tam, kde není možné vést kabeláž (historické památky, vzácné malby na omítkách atd.), ale i v normálních objektech neboť instalace je snadná a rychlá. Kdykoliv lze rozšířit systém o další prvek či změnit konfiguraci (např. přemístění).

3.3.4.1 Jednosměrný přenos

Jednosměrný přenos využívá vysílače v detektoru a přijímače v ústředně. Systémy tedy neměly kontrolu o stavu funkčnosti detektorů. Modernizované jednosměrné přenosy dodržovaly pravidelnou kontrolu přenosové cesty pomocí vysílaného signálu. Problémem je zde spotřeba baterii při časté kontrole. Ovšem při ušetření spotřeby baterií tím, že bude kontrola probíhat v delších časových úsecích vznikne velká časová prodleva v informovanosti o funkčnosti či nefunkčnosti prvku. U jednosměrného přenosu se vyskytuje problém u četného pohybu osob např. ve veřejných budovách, neboť jednotlivé prvky neví, zda je systém v klidovém stavu nebo ve střežení, ale i přesto musí vysílat informaci o poplachovém stavu ústředně.

V klidovém stavu ústředna poplach nevyhodnotí, ovšem tímto vysíláním se vyčerpává energie napájecího zdroje, což je jedna z nevýhod. Tou další je třeba zmínit rušení signálu a jednoduchost zjištění kmitočtu či modulace systému. Pak není problém zahltit přijímač stejným kmitočtem s větší intenzitou.

3.3.4.2 Obousměrný přenos

Mezi výhody obousměrného přenosu patří duplexní systém, kde detektor má přijímač i vysílač. Automaticky si samy mohou najít volné kanály pro přenos, pakliže se objeví rušení

v těchto již nalezených kanálech jsou schopny opět si vyhledat další volné pásma. Odstraněny jsou zde všechny nedostatky jednosměrných systémů a to především tak, že při zapnutí si ústředna ověří funkčnost a stav detektorů (prvků) v systému, rovněž detektory v klidovém stavu nevysílají a neplýtvají energie z napájecího zdroje a je umožněn vzdáleně test chůzí. Navíc ústředna si skutečně ověří, jestli se jedná o falešný poplach nebo o skutečnou poplachovou informaci.

3.3.5 Hybridní

S hybridním systémem či připojením smyček se můžeme setkat až v poslední době. Jedná se o spojení, jak bezdrátových adresovatelných prvků, tak drátových vstupů. Vstupy a prvky je možné ovládat pomocí systémové či bezdrátové klávesnice.

Nevýhody přebírají od smyčkových ústředen v podobě neadresovatelnosti prvků v systému a hlavně rozsáhlou kabeláži. Na druhou stranu hybridní ústředny mají výhody bezdrátových ústředen v podobě jednoduchosti, rychlosti montáže a adresovatelnosti prvků v bezpečnostním systému.

4 ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE (DÁLE JEN EPS)

Problematikou EPS se zabývá norma ČSN EN 54 a podléhá státnímu dozoru dle zákona o požární ochraně č. 133/1985 Sb.

Obr. 12 Ústředna EPS

Zařízení elektrická požární signalizace:

Jde soubor technických zařízení, skládajících se z ústředny EPS, hlásič požáru a doplňujících zařízení. Tato zařízení tvoří systém, jehož hlavním úkolem je zaznamenávat a vyhodnocovat požár hned od prvopočátku jeho vzniku a požár signalizovat opticky i akusticky na ústředně EPS. Většinou se signalizace umisťuje tam, kde je stálá služba, která může na signalizaci reagovat, tedy požár zlikvidovat anebo přivolat další pomoc (HZS). [1]

Do hlavních úkolů patří tedy:

- Rychlé a spolehlivé určení místa požáru (již při jeho počátku zahoření)
- Vyhlášení poplachu
- Aktivace a řízení evakuačního systému v dané oblasti
- Ovládání a signalizace stavu dalších požárních bezpečnostních zařízení
- Automatická komunikace s hasičským záchranným sborem (HZS)

EPS lze nazvat jako souhrnný systém elektronické ochrany objektu, který přispívá k požární ochraně.

EPS můžeme rozdělit do základních částí a to na:

- Požární hlásiče – vstupní prvek
- Ústředna EPS
- Požární poplachová zařízení – výstupní prvek

4.1 Požární hlásiče

Jde o zařízení, které umí sledovat, měřit fyzikální veličiny ve střeženém prostoru a jejich změny provázející požár vyhodnocovat popřípadě předat ústředně EPS. Uvnitř hlásičů je vyhodnocovací obvod, který rozhoduje o tom, zda jednotlivé parametry nebo jejich změny překračují příslušnou mez.

Základním rozdělení je na:

Manuální – tlačítkové

Slouží pro vyhlášení požárního poplachu za pomocí lidského činitele, který požár objevil nebo jiný nebezpečný stav či jev. Tlačítko požárního hlásiče je vždy červené barvy. Jde o mikrospínač s elektronikou (někdy také zakončovací rezistor). Je navržen tak, aby se neaktivoval náhodně nebo sám. Většinou je spínač ukrytý pod sklíčkem, které pomůže obsluze při zjištění, kterým hlásičem byl vyhlášen poplach. Pro ochranu proti úrazu střepy je sklíčko naříznuté a pokryté fólií.

Automatické – samočinné

Sledují určitý fyzikální i chemické jevy, v případě potřeby na ně reagují a posílají signál ústředně EPS. Reagují automaticky podle svého vyhodnocení na příslušné parametry v oblasti kouře, nárůstu teploty či vyzařování plamene. Proces u samočinných hlásičů se jednoznačně vyznačuje detekcí, vyhodnocení detekce, zpracování výsledku ústřednou a jasným zavedením dalších opatření v objektu.

Do této kategorie patří:

1. Kouřové hlásiče
    - Ionizační
    - Optické
2. Teplotní hlásiče
    - Bodové
    - Liniové – analogové, digitální
    - Lineární
3. Chemické
4. Vyzařování plamene

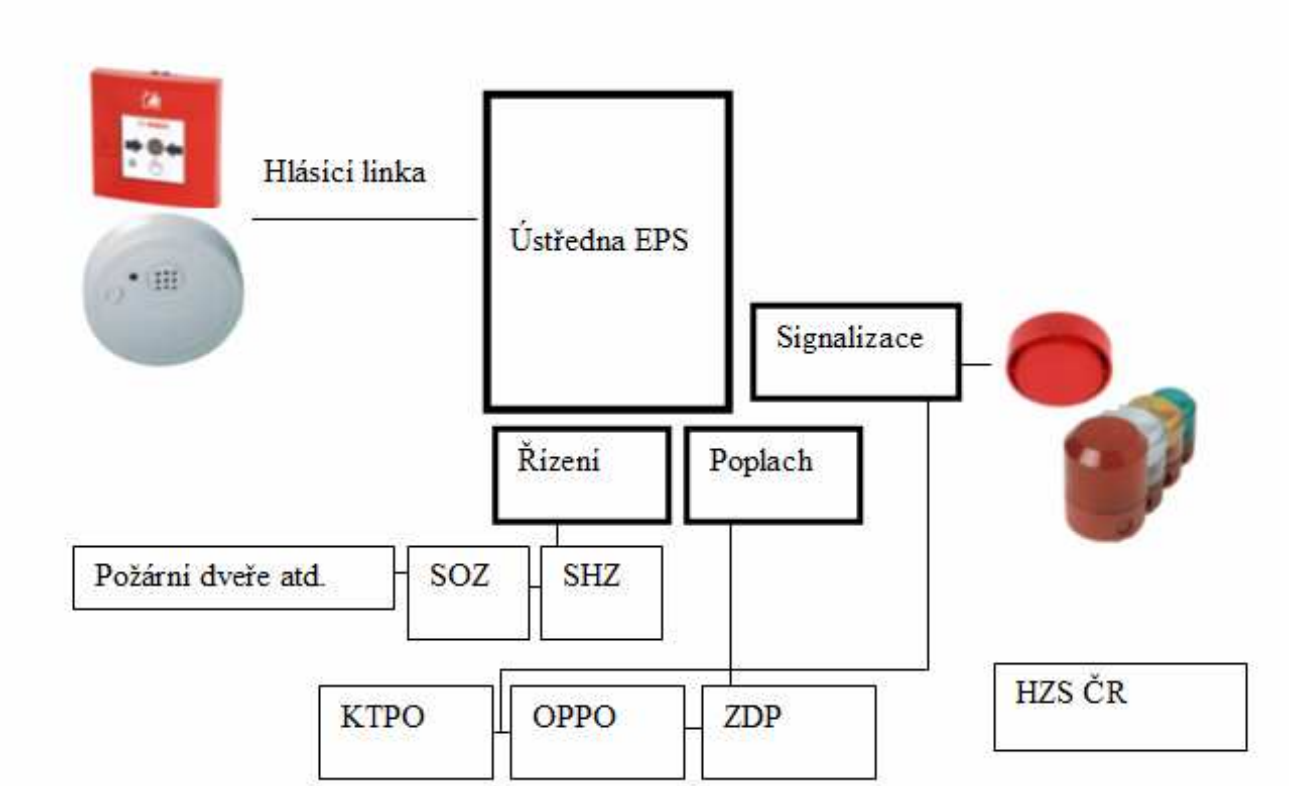
Běžně se vyrábí hlásiče dle časové reakce na změnu fyzikálního či chemického jevu, a to hlásiče bez zpoždění, kde je reakce bezprostřední po překročení mezní hodnoty anebo se zpožděním, kde rychlost změny parametru musí překračovat danou mez po určitou dobu.

4.2 Ústředna EPS

Tvoří centrální jednotku systému požární ochrany. Sbírá informace ze všech hlásičů ať už manuální – tlačítkových nebo automatických – samočinných. Tyto informace vyhodnocuje, zpracovává a reaguje na ně v podobě určitě odezvy (vyhlášení poplachu, signalizace poruchy atd.).

Ústředna EPS umožňuje:

- Nastavování, ovládání a diagnostiku systému
- Nepřetržité napájení hlásičů a dalších prvků i při výpadku sítě
- Signalizaci provozních stavů – provoz, porucha, požár
- Kontrolu provozuschopnosti celého systému, popřípadě ohlášení poruchy (akusticky, opticky)
- Vyhodnocuje signalizaci z hlásících linek
- Paměť na poplachové události pro zpětnou analýzu poplachu



Obr. 13 Schéma systému EPS

Vysvětlení prvků na blokovém schématu:

SOZ – samočinné odvětrávací zařízení

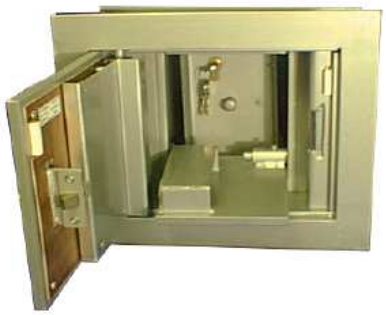
Jedná se zařízení, které slouží k odtahu tepla a kouře případně zplodin z hoření v stavebním objektu. Používají se mechanismy pružinové, hydraulické, stlačený plyn nebo elektromotor a to na pokyn ústředny EPS nebo automaticky na základně signálů z vlastních detektorů. Všechny systémy by měly být řádně koordinovány a řízeny tak, aby nedošlo k nežádoucímu spuštění či vzájemnému rušení jejich funkcí.

SHZ – stabilní hasící zařízení

Jsou zřízeny za účelem odstranění jedné ze základních podmínek hoření (snižování teploty zapálené hořlavé látky, produkující teplo a omezování dostatečného množství kyslíku). Jejich princip je založen na vytěsnění kyslíku jiným plynem stejného objemu a ochlazení hořící látky pod zápalnou teplotu. Pakliže je jedna z podmínek hoření odstraněna, pak se daří požár eliminovat. Technologie SHZ nabízejí ochlazení hořící látky pomocí sprinklerů (kropící zařízení), drenčerového systému, atomizací vody, plynných substancí.

KTPO – klíčový trezor požární ochrany

Jedná se o výrobek, který umožňuje rychlý a bezproblémový vstup pro zásahovou jednotku Hasičského záchranného sboru v objektu. Při vyhlášení poplachu se Hasičský záchranný sbor pomocí klíče umístěného v KTPO dostane rychle a bez porušení dveří do objektu.



Obr. 14 Klíčový trezor požární ochrany (KTPO)

OPPO – obslužné pole požární ochrany

Jedná se o univerzální zařízení k připojení na ústřednu elektrické požární signalizace (EPS). Slouží k zobrazení určitých provozních stavů ústředny EPS v jednotné formě zobrazení a také umožňuje zásahovým silám hasičského záchranného sboru HZS obsluhu bez přítomnosti provozovatele v případě požárního poplachu.

Obr. 15 Obslužné pole požární ochrany (OPPO)

ZDP – zařízení pro dálkový přenos požárního poplachu

Jde o doplňkové zařízení systému EPS, které umožňuje zajištěný přenos poplachového signálu či poruchy z ústředny EPS na místo ohlašovny požárů. ZDP při jeho použití je plnohodnotným náhradníkem trvalé obsluhu ústředny, proto se provádí nepřetržitá kontrola

přenosových cest a kontrola provozuschopnosti. Přenosové cesty ze zařízení dálkového přenosu do zařízení dálkového přenosu v ohlašovně požáru mohou být:

- za pomocí pevné linky
- za pomocí komutovaných telefonních linkách (vyšší frekvenční pásmo)
- za pomocí radiového spojení

Základní rozdělení ústředen EPS:

- Konvenční neadresné
- Konvenční adresné
- Analogové
- Interaktivní

4.2.1 Ústředny EPS konvenční neadresné

Tyto ústředny se vyznačují připojením hlásičů k ústředně proudově vyváženou hlásící linkou (smyčkou). Nelze určit, který hlásič vyvolal poplach, neboť nemá svou adresu. Je možné připojit na jednu hlásící linku až 20 (32) hlásičů a to i odlišného typu.

4.2.2 Ústředny EPS konvenční adresné

Výhodou těchto ústředen spočívá v adresném systému hlásičů a tak lze zjistit, který hlásič poplach vyvolal. Vyhodnocování poplachu se odehrává v ústředně EPS. Hlásiče mají dva stavy (klid – poplach). Modernější ústředny nabízejí připojení pomocí oddělovacích izolátorů do kruhových smyček. Izolátory se po určitém počtu hlásičů připojí do smyčky a v případě poruchy hlásiče nebo vedení jsou schopny vyřadit vadnou část systému mezi dvěmi izolátory a zbylá část funguje dále.

4.2.3 Analogové ústředny EPS

Hlásiče monitorují stav v hlídaném objektu a předávají více stavové (analogové) údaje do ústředny. Pomocí algoritmů je ústředna vyhodnocuje a určuje, zda se jedná o normální stav, poruchu, před-poplach nebo přímo poplach. Každý hlásič má svou adresu a tak lze zjistit

odkud signál přišel. Jelikož se přenese velký objem dat do ústředny EPS je kladen větší nárok na kabeláž. Základem pro připojení hlásičů s ústřednou se používá kruhová sběrnice.

4.2.4 Interaktivní ústředny EPS

V tomto systému EPS se používají interaktivní hlásiče. Ty rozlišují úroveň jednotlivých signálu, které do hlásičů směřují z okolí a změnu jejich parametru v čase. Každý takovýto hlásič obsahuje mikroprocesor, který zpracovává za pomocí příslušného algoritmu zpracovává a vyhodnocuje informace ze svého okolí. Hlásič poté vytváří definovaný elektrický signál, který odpovídá určité požární situaci a ten je vzápětí předán ústředně EPS. I v tomto případě jsou v tomto systému hlásiče adresné, tudíž můžeme na ústředně vidět, který hlásič určitou situaci vyvolal. Hlavní výhodou interaktivních systémů v porovnání s analogovým systémem je menší zatížení přenosové cesty mezi detektory a ústřednou a velká odolnost vůči negativním jevům (elektromagnetická indukce způsobená souběhem vedení kabeláže). [1]

4.3 Požární poplachové zařízení

Jsou to taková zařízení, které přijímají a přeměňují elektrický poplachový signál z ústředny EPS na vhodnou podobu srozumitelnou určitým osobám. Zpravidla nejsrozumitelnější se jeví akustická a optická.

4.3.1 Akustická poplachová zařízení

Do kategorie akustických poplachovým zařízení patří signalizační tabla ústředen, sirény, bzučáky, celá řada požárních zvonů a také to mohou být akustické piezo-měniče.

4.3.2 Optická poplachová zařízení

Do optických poplachovým zařízení patři celá řada majáků (žárovkových, výbojkových), signálky, kontrolky a displeje. Je-li EPS systém s rozhraním a připojením na PC, pak může funkci optického poplachového zařízení vykonávat monitor PC.

5 ELEKTRONICKÉ PŘÍSTUPOVÉ SYSTÉMY (ACCESS CONTROL)

Doporučené zásady pro přístupové systémy jsou uvedeny v normě ČSN EN 50-133-1-7.

Obr. 16 Přístupový systém

5.1 Funkce přístupového systému

Jde o elektronický systém zajišťují kompletní přehled kontroly vstupu do chráněných prostorů. Tedy komplex zařízení, které ve zkratce říkají „KDO“, „KAM“ a „KDY smí. V dnešní době jde o zcela efektivní nástroj, jak zpřístupnit chráněný prostor jen oprávněným lidem. Ve funkci jako poplachový systém lze na výstupu připojit i zábranný systém, který vyhlásí poplach při delším otevírání dveří než je potřeba, nebo snaha o otevření dveří pro který daná osoba nemá přístupovou úroveň.

Elektronický přístupový systém (dále jen Access Control) určuje:

- Kdo se může do daného prostoru dostat – držitel karty nebo media s jeho informacemi
- Kam se může až uživatel dostat – je nastavena přístupová úroveň
- Kdy se může uživatel do prostoru dostat – časová zóna

Celý princip přístupových systémů spočívá v autentizaci osoby, která se chce dostat do zájmového prostoru. Pomocí přístupového systému lze kontrolovat libovolný počet vstupních míst. A provádět různá nastavování úrovní a časových zón pro uživatele a jiné parametry.

Autentizace je proces pro jednoznačné ověření člověka, který vstupuje do přístupového systému, na základě informací uložené na kartě-čipu.

5.2 Přístupové systémy a jejich výhody

Přístupové systémy snižují náklady vynaložené na ostrahu chráněného objektu (prostoru) a rovněž náklady na zámkové systémy. Při zavedení přístupového systému se zcela odbourají určité rizika a to v podobě:

- Není nutné vlastnit klíče (tím nehrozí jejich ztráta či duplikát).
- Pří ztrátě tokenu (karty) nebo pří ukončení pracovního vztahu se zaměstnavatelem, lze kartu jednoduše smazat ze systémové databáze.
- Nahlédnutí jen do oprávněných prostorů - každý uživatel (zaměstnanec) má svou jedinečnou kartu a za její pomocí se nastaví individuální přístup a sledování držitele karty.
- Velmi velká flexibilita – omezené možnosti přístupu.

5.3 Autentizační přístupy

- **Založeny na heslu** – nutná znalost hesla, jenž zná pouze oprávněný uživatel. Nevýhodou je možnost odchycení hesla, a proto se tento autentizační přístup používá tam, kde se požaduje minimálních bezpečnostních požadavky na chráněný prostor.
- **Založeny na předmětu** – nutnost vlastnit identifikační předmět (kartu neboli token). Výhodou je jedinečnost a nemožnost duplikátů. Čtecí technologie:
    - **Barium ferit**
    - **Magnetický pásek**
    - **Čárový kód**
    - **Wiegand**
    - **Bezkontaktní technologie**

- **Klávesnice**
- **Kombinace klávesnic a karet**

➢ **Založeny na biometrii –** porovnávání jedinečných biologických hodnot uživatelů s databází. Přístupy s využitím biometrie zahrnují:

- **Otisk prstů**
- **Tvar ruky**
- **Obličej**
- **Obraz sítnice (duhovky)**
- **Žilní řečiště**
- **Hlas**

5.4 Základní prvky přístupového systému

Každý elektronický přístupový systém obsahuje specifická zařízení s určitou funkcí, kterou v systému zastupují. Základem jsou zařízení (hardware), která obsahují ve svém jádru posloupnost instrukcí (software), které přiřazují zařízením (hardwaru) určitý stupeň inteligence. U zařízení pro přístupové systémy lze označit software jako systémový. Jde o firmware, tedy o programové vybavení implementováno přímo v elektronickém zařízení. Tento software je i bez napájení uchováván v paměti (EPROM, ROM a jiné). Za podpory mikroprocesoru jsou tyto implementované sekvence příkazů vykonávány ve prospěch zařízení použitých v přístupových systémech.

5.4.1 Hlavní části přístupového systému

Kapitola pojednává o jednotlivých zařízeních, která jsou nedílnou součástí přístupového systému a bez kterých by přístupový systém nemohl být realizován. Především u nejpoužívanější bezkontaktní technologie.

5.4.1.1 Identifikační médium (KARTA)

Každá karta je unikátní a má rozměr platební karty. Liší se pouze tloušťkou. Existují i speciální transpondéry, které mají stavbu jako přívěšek na klíče (klíčenka). Kromě uchovávání důležitých informací v paměti karty mohou být na povrch karty vytištěny

personální informace (sublimační tiskárnou) nebo natištěné na polepce, která se přilepí na kartu. Mezi nejpoužívanější technologie používané v oblasti karet patří Wiegand. Skládá se ze dvou antén, z nichž jedna má funkci přijímače a druhá vysílače. A rovněž svůj miniaturní obvod v podobě čipu.

5.4.1.2 Dveřní zámek

Do hlavní priority elektronických potažmo i jiných systémů dveřních zámků spadá především funkce zablokování pohybu části bezpečnostního zámku, jako je závora, střelka nebo i ručně ovládaná klika.

V této souvislosti rozlišujeme:

- Elektrické otvírače
- Elektromechanické zámky
- Elektromotorické zámky
- Magnetické zámky
- Elektromotorické vložky

5.4.1.3 Čtecí snímač (ČTEČKA)

Princip zařízení je založen na periodickém vysílání pulsů snímače (čtečky karet) do okolí a pakliže v blízkosti se objeví karta, pak přes anténu karty (tranpondéru) využije signálu k nabití kondenzátoru uvnitř karty energií a tuto energii využije k aktivaci kondenzátoru a následnému vyslání zpětné informace do čtečky karet. Můžeme tedy říci, že čtečka karet nemá svou vlastní inteligenci a všechny informace zpracování za čtečku karet řídící panel (interface), který posílá data do řídící jednotky, která provede vyhodnocení nebo pošle data do řídícího počítače a ten po zpracování dat pošle odpověď. Na čtečce je umístěna LED dioda (optická signalizace) a rovněž i zvuková signalizace.

5.4.1.4 Řídící panel (INTERFACE)

K rozhraní pro čtecí zařízení karet je možné připojit dvě tyto čtecí zařízení. Interface má řadu reléových výstupů i vstupu pro další připojení zařízení.

5.4.1.5 Řídící jednotka

Základní jádro přístupového systému. Obsahuje firmware s nadefinovanými algoritmy pro různé zpracován informací z řídícího panelu. Většinou práci vykonává operační systém (OS), který řeší úlohy a funkce, které jsou rozdělené na 11 základních úkolů. Každý sektor řeší danou problematiku a ve výsledku jsou tyto sektory spojeny do výsledku.

5.4.1.6 Docházkový terminál (pro možnost pracovat s daty přístupového sytému)

Grafické zařízení umístěné ve firmách na přístupových místech (vrátnice), kde obsluha má možnost sledovat, obsluhovat přístupové systémy a to především při haváriích, kdy je nezbytné vykonat opatření a odblokovat únikové cesty zabezpečené přístupovým systémem.

5.5 Provedení přístupových systémů

U provedení přístupového systému se zabýváme většinou zpracováváním a předáváním dat z databáze celého systému k zařízením a naopak.

5.5.1 Autonomní provedení systému

Autonomní systém se používá pro menší objekty, kde se požaduje ovládání a přístup pro jedny dveře nebo menší počet dveří. Autonomní systém pracuje zcela samostatně. Autonomní systém se skládá klávesnice, kde se zadává heslo do systému pro daný přistup a v kombinaci s použitím karty, která se přiloží blízko k bezkontaktnímu snímači nebo se protáhne magnetická karta snímačem.

Řídící jednotka autonomního systému obsahuje paměť dle výrobce na počet událostí (500 až 100 000) a počet karet, které jsou evidovány v systému.

Jejich nastavení se provádí přímo připojením k autonomní jednotce přes rozhraní RS 232 i přesto, že většina notebooku už toto rozhraní nemá. Pak lze dokoupit převodník např. USB na RS-232.

Obr. 17 Autonomní systém obsahující bezkontaktní snímač a klávesnici

5.5.2 On-line provedení systému

On-line systémy pracují v reálném čas a jejím základem je řídící počítač, se kterým komunikují řídící jednotky přístupového systému. Výhodou takových systémů je jejich cena. Neobsahují žádnou paměť a vše je vyhodnocováno v reálném čase s řídícím počítačem, který přijímá data a posílá odpověď. V případě poruše kdekoliv na sběrnici či řídícím počítači dojde k zablokování zámků a systému, což je nevýhoda u tohoto provedení.

Nastavení se provádí z libovolného místa v sítí nebo z řídícího počítače.

5.5.3 Off-line provedení systému

Systém Off-line myslí už na problémy, které by mohl vzniknout a proto při poruše na sběrnici systému nebo na řídícím počítači, přebírá hlavní funkci řídící jednotka umístěná v blízko vstupního místa. Ta rozhoduje o propuštění do daného místa nebo ne. Tyto události zaznamenává a při obnově porušeného systému pošle ihned data do řídícího počítače.

5.6 Zpracování informací u přístupového systému

Jde o sbírání a vyhodnocování informací z přiložených karet pro následné vzdálené nebo místní vyhodnocení o přístupu k danému místu.

5.6.1 Centralizované zpracování

V systémech s centralizovaným zpracováním informací jsou data sbírána panely přímo u čteček a posílána na řídicí počítač k vyhodnocení. Pokud je např. na čtečce přečtena karta, posílá čtečka číslo této karty na počítač nebo jinou vyhodnocovací jednotku. Počítač

porovná přijaté číslo s obsahem své databáze a pokud kartu vyhodnotí jako platnou (pro aktuální místo i čas), odešle zpět na panel povel k odblokování dveřního zámku. Slabina takovéhoto systému je zřejmá- v případě výpadku řídicího počítače nebo přerušení komunikační linky mezi počítačem a panely přestane systém správně fungovat. Problém vyřeší jen vestavěná inteligence v řídicích panelech, která bude potíže s výpadky komunikace eliminovat.

U systémů s řídicím počítačem kontroluje řídící jednotka jen tzv. facility kód, teprve po

této kontrole posílá číslo karty k počítači. Pokud panel nemůže s počítačem komunikovat, přechází panel do Off-line režimu. V něm panel zkontroluje jen facility kód karty a pokud tento odpovídá kódu, který má panel uložen ve své paměti, povolí držiteli karty průchod dveřmi. Panel nemá v tomto režimu možnost zkontrolovat, zda je karta použita na správném místě a ve správném čase. Jednoduše řečeno, přístup získá kdokoliv, kdo má kartu se správným facility kódem (těchto karet však může být velké množství).

Facility kód je číslo zapsané do karty v okamžiku její výroby nebo programování. Tento kód zajišťuje, že i když někdo duplikuje kartu s určitým ID číslem, nebude nová karta na jiném objektu s jiným facility kódem fungovat. Jde v podstatě o druhý, skrytý kód, který čtečka kontroluje. Pokud se z karty přečtený neshoduje s uloženým facility kódem, přístup bude odmítnut.

5.6.2 Distribuované zpracování

U distribuovaného zpracování informací se databáze nahrávají přímo do řídících jednotek, které potom samy rozhodují o tom, zda kartu přes sledovaný vchod vpustí nebo ne. Připojenému počítači se jen předává informace o výsledku rozhodnutí. Počítač tento údaj zaznamená do svého deníkového souboru nebo vytiskne na připojené tiskárně. Je zřejmé, že v této konfiguraci výpadek komunikace s počítačem spolehlivost přístupového systému nijak neovlivní. Navíc některé panely mohou uchovávat i velké množství proběhlých událostí ve své vnitřní paměti a najednou je předat počítači až ve chvíli, kdy je komunikace znovu obnovena. Díky své architektuře nabízejí systémy s distribuovaným zpracováním informací mnohem vyšší spolehlivost a rychlejší odezvu než ty, které jsou odkázány na činnost centrálního počítače. [6]

6 CCTV (SYSTÉMY PRŮMYSLOVÉ TELEVIZE)

Problematikou CCTV se zabývá norma ČSN EN 50-132-1-7.

Obr. 18 CCTV kamera

Jedná se velmi vhodný doplněk výše uvedených bezpečnostních technologií, tzv. uzavřené televizní okruhy (Close Circuit Television). Kamerové zabezpečovací systémy a jejich obraz je přístupný každému, kdo je součástí speciálního uzavřeného typu televizního okruhu (dále jen CCTV).

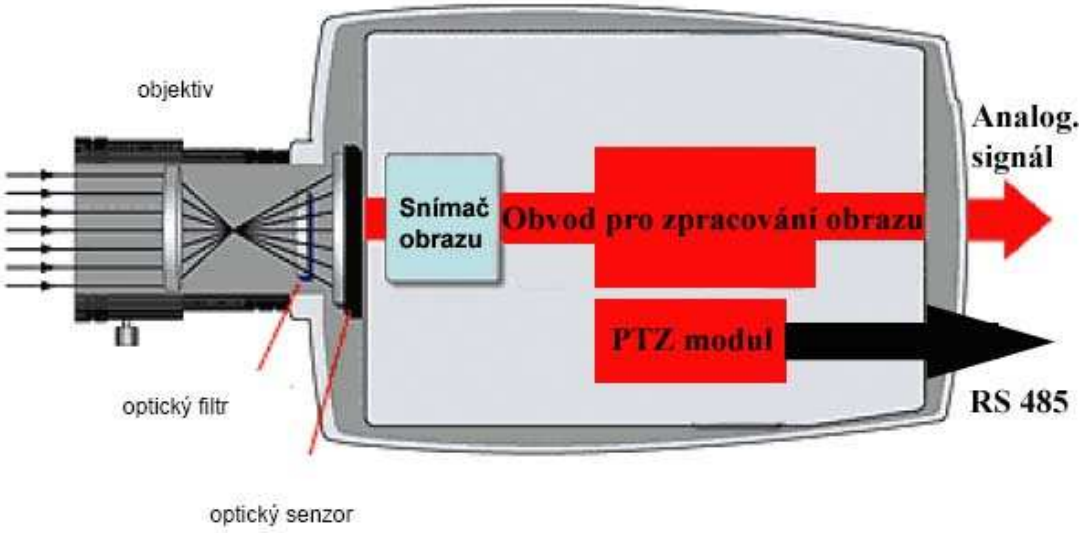
Provádějí tzv. video-monitoring, tedy snímají jevy či události, které se objevují před kamerovými zařízeními a s těmito snímanými událostmi lze dále určitým způsobem pracovat. Především se signál v kameře musí určitým způsobem zpracovat a převést na elektrický signál, který dále může být směrován do záznamového zařízení, pokud důležitost signálu je velká a má být uložena na médium nebo může být signál směřován přímo na zobrazovací zařízení (monitor).

Rozlišení kamer dle její výstupní informace:

- Analogové kamery
- Digitální kamery (IP kamery)

6.1 Analogové kamery

Analogové kamery už v dnešní době jsou na ústupu a jestliže se využívají, pak jejich nerozdělitelnou součástí jsou digitální videorekordéry, které digitalizují obraz a rovněž umožňují připojit všechny analogové kamery přes digitální videorekordér do počítačové sítě (LAN, WAN). Analogové kamery se dají připojit do počítačové (datové) sítě nejen pomocí digitálního videorekordéru, ale pokud není potřeba záznamu stačí připojení přes video server (v dnešní době možnosti připojit jednu až čtyři analogové kamery). Pakliže by analogové kamery byly připojeny pouze k analogovému videorekordéru (VCR), pak nelze vykonávat žádný vzdálený monitoring.



Obr. 19 Analogová kamera

6.1.1 Zařízení pro převod analogového signálu do sítí TCP/IP

Analogové kamery, které se dnes používají stále ve větší míře než digitální IP kamery je možné jejich analogový výstupní signál převést do Ethernetových sítí. Signál odpovídající Ethernetové síti odpovídá sadě internetových protokolů TCP/IP. A signál je veden za těmito zařízeními jako datový paket.

6.1.1.1 DVR (Digital video recorder)

Hardware, který obsahuje řadu kompozitních vstupů (BNC) pro analogové kamery a záznamové médium (Harddisk). Záznamové médium slouží pro uchování obrazové scény v digitální podobě, neboť předností DVR je digitalizace obrazu. Obsahem balení je CD se softwarem pro nastavení. DVR má rozhraní pro sítě LAN (TCP/IP), kde pomocí UTP kabelu je možnost připojit DVR do počítačových sítí a umožnit vzdálenou správu. Modernější DVR obsahují programovatelné vstupy, kde lze připojit například detektor pohybu a na základě nastavení se po vyhlášení poplachu začne nahrávat záznam.

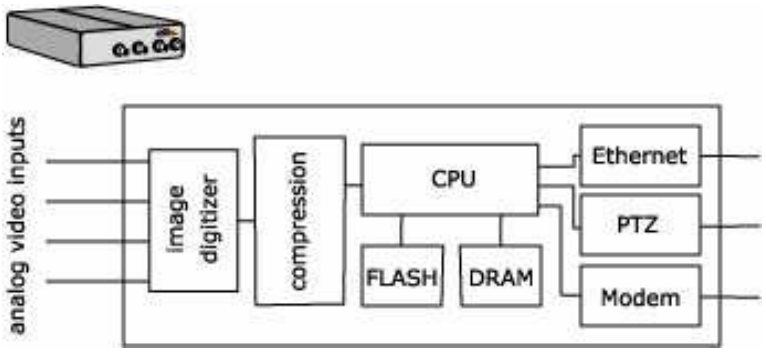
Obr. 20 DVR zařízení

6.1.1.2 Video server (Video enkodér)

Video server (také video enkodér) je vybaven jedním nebo více analogovými video vstupy, digitalizátorem obrazu, obrazovým kompresorem a webovým serverem se síťovým/modemovým rozhraním. Video servery digitalizují analogový zdroj videa a předávají pomocí počítačové sítě digitalizované záběry, takže efektivně mění běžnou analogovou kameru na síťovou kameru. To představuje ideální řešení pro integraci se stávajícím analogovým CCTV (Cloused Circuit TeleVision) systémem.

Obr. 21 Video server

Systém a skladba video serveru:



Obr. 22 Video server a jeho skladba

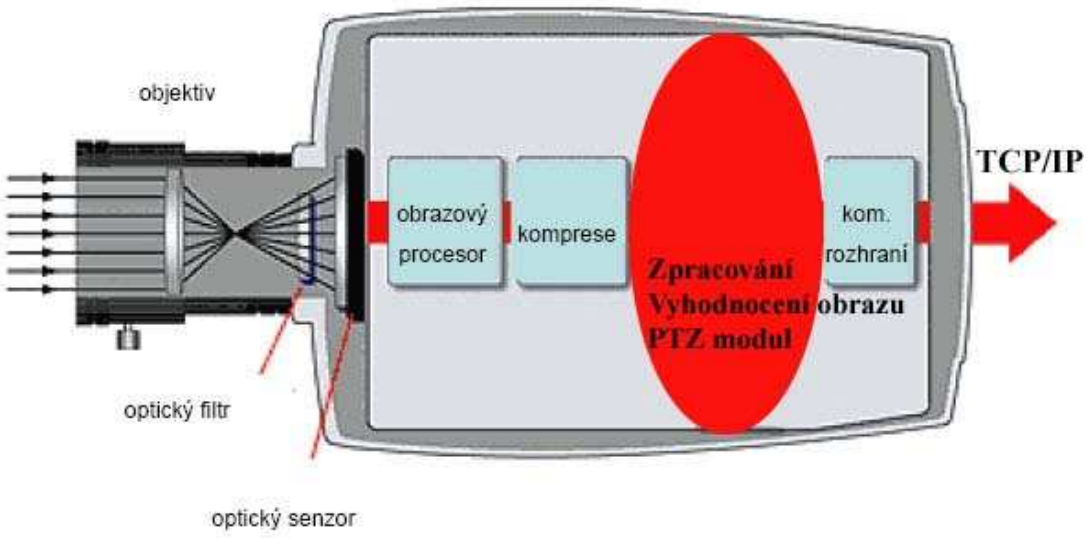
Pomocí vestavěných sériových portů dokáže video server ovládat vybavení, jako jsou kamery s funkcí natáčení a zoomu (Pan/Tilt/Zoom). Vstupy mohou být použity pro aktivování serveru k tomu, aby začal posílat záběry. Servery vybavené obrazovým bufferem dokáží poslat i záběry před alarmem.

Video server může také být připojen ke speciálním kamerám, jako jsou velmi citlivé černobílé kamery, miniaturní kamery nebo mikroskopické kamery. [12]

6.2 Digitální kamery (IP kamery)

IP kameru (síťovou kameru, webkameru) můžeme popsat jako kameru a počítač v jednom. Zachycuje a vysílá živé záběry přímo přes IP síť a umožňuje tak autorizovaným uživatelům lokálně nebo na dálku sledovat, ukládat a spravovat video záběry pomocí standardní síťové infrastruktury založené na IP protokolu. [7]

IP kamera má svou tovární IP adresu, která slouží pro její jednoznačnou identifikaci v síti do které je připojená. Při změně IP adresy, lze kdykoliv kameru resetovat pomocí tlačítka nebo SW. Obsahuje navíc i vlastní webový server, FTP server, FTP klienta, e-mailový server, programovatelné vstupy a výstupy a některé IP kamery obsahují i pohybový detektor.



Obr. 23 Digitální kamera

6.3 Rozdělení kamer podle jejich využití

- Vnitřní
- Vnitřní / Venkovní
- DOME
- PTZ (otáčení, naklápění, zoom)
- Den / Noc
- Antivandal provedení

6.4 Porovnání síťového videa a analogového videa

V následující tabulce je srovnání jednotlivých sekcí a možností síťového videa a analogového videa. Na základě srovnání si můžeme udělat vlastní názor na výhody a nevýhody jednotlivých možností.

	Systém síťového videa	***Systém analogového videa***
Přístup	Otevřený nebo omezený přístup dle potřeby. Schopnost vzdálené administrace odkudkoli přes webový prohlížeč.	Uzavřený okruh. Neumožňuje vzdálený přístup.
Snadnost použití	Na dálku možnost spravovat a prohlížet záběry pomocí standardního prohlížeče na jakémkoli PC. Záběry mohou být zaznamenány na pevném disku, což umožní snadné ukládání, snadné prohledávání a žádné zhoršení kvality obrazu nebo opotřebení záznamu. Pevný disk můžete kvůli bezpečnosti umístit i na vzdálené místo.	Vzdálená administrace nebo monitorování není možné. Záběry musí být ukládány na video kazety, které neustále vyžadují výměnu kazet a mnoho místa pro ukládání. Kvalita záznamu se časem zhoršuje. Video rekordér musí být umístěn poblíž kamery. To může potenciálně umožnit neoprávněným osobám přístup k video kazetě.
Kvalita	Digitální záběry neztrácejí kvalitu ani při přenosu ani při ukládání. Digitální obraz je vytvořen pomocí formátu Motion-JPEG. Jednou vytvořené záběry už nemohou ztratit kvalitu. Každý snímek ve video streamu je ostrý.	Kvalita obrazu se ztrácí při použití delší kabeláže a rozlišení magnetické pásky je poměrně malé. Navíc se kvalita obrazu časem zhoršuje.
Systémové požadavky	Všechno potřebné pro vysílání živého videa přes síť je už v kameře. Stačí připojit kameru k síti. Prohlížet, zaznamenávat a spravovat záběry můžeme z jakéhokoli počítače v síti (umístěného kdekoli).	Připojení ke koaxiálnímu kabelu, k multiplexeru, k videorekordéru a k lokálně umístěnému CRT (cathode ray tube) monitoru

Instalace	Prostě se síťová kamera připojí k nejbližšímu síťovému připojení a přidělí se mu IP adresa.	Koaxiální kabel se připojí ke každé analogové kameře pak se připojí k multiplexeru.
Kabeláž	 Jeden standardní síťový kabel dokáže současně posílat záběry stovek síťových kamer.	 Jeden koaxiální kabel dokáže přenášet pouze obraz z jedné kamery. Pokud máte dvě kamery, potřebujete dva kabely. To často vede k rozsáhlým kabelovým vedením s tlustými a citlivými kabely, které jsou připojeny k lokálně umístěné kontrolní místnosti.
Škálovatelnost	Přidávání dalších síťových kamer do systému je snadné.	Velmi obtížná. Každá analogová kamera vyžaduje vlastní kabel. Kvalita obrazu se ztrácí s rostoucí délkou kabelu.
Náklady	Kvalitní síťový kabel obvykle stojí o 30% až 40% méně než koaxiální kabel. Síťový kabel dokáže také podporovat stovky síťových kamer a jiných zařízení. Síťová infrastruktura založená na IP je častokrát už nainstalována, což redukuje náklady na pouhou cenu kamery.	Koaxiální kabely jsou drahé. Obvyklý koaxiální kabely typu RG59 75 Ohmů stojí o 30% až 40% více než kvalitní síťový kabel. Potřebujete více kabelů, protože každá analogová kamera vyžaduje svůj vlastní. Vysoké náklady na údržbu a instalaci, plus cena analogové kamery, plus cena videorekordéru a video kazet. [13]

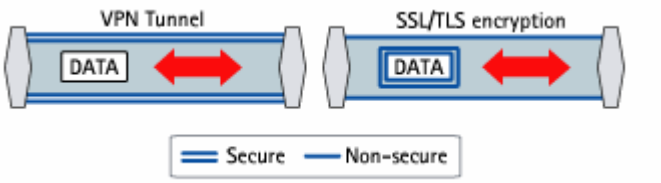
tabulka 1 Srovnání kamerových systémů

7 PŘÍSTUP K BT PŘES SÍŤ TCP/IP A INTERNET

Dnešní bezpečnostní technologie nabízejí řadu možností a funkcí, které jsou nezbytně pro ochranu zdraví a majetku. Jednou z rozšířených a moderních je možnost připojit bezpečnostní zařízení do počítačových sítí a následně do sítě Internet. Všechny zařízení, které bychom chtěli umístit do komunikačních (počítačových) sítí musí obsahovat síťové rozhraní. Jedná se o moduly či inteligenci podporující protokoly pro datové sítě. Nejpoužívanějším protokolem, který uskutečňuje posílání dat a komunikaci po síti je protokol TCP/IP. Jedná se o složení dvou protokolů TCP a IP. Jednotlivé zařízení nebo moduly, které připojí bezpečnostní zařízení do sítě obsahují jednoznačný identifikátor, kterým je IP adresa. To je důležité v případě, kdy v dané síti veřejné či privátní požadujeme vzdálený přístup k technologiím. Většinou IP adresa se přiřazuje na základě přímého připojením počítače křížený kabelem a pomocí konfiguračního softwaru. Z hlediska bezpečného přístupu k technologiím existují dvě základní možnosti, jak zachovat stupeň soukromí. Jedná se o šifrovanou komunikaci.

- VPN (Virtual Private Network)
- HTTP přes SSL/TLS (HTTPS)

U VPN metody je použito „tunelu“ vytvořeného mezi vnitřními body. Pouze ten bod, který zná „klíč“ může pracovat v tomto tunelu. Ostatní síťová zařízení nebudou mít přístup k datům. U metody přes certifikát SSL/TLS (HTTPS) se používá přímo šifrování dat samotných. Do jednotky se nainstaluje certifikát a ten může být poskytnut třetí straně nebo lokálně. Po navázaní mezi dvěmi zařízeními, klient ověří certifikát serveru a pokud mu bude věřit začne šifrovaná komunikace. [14]



Obr. 24 Rozdíl mezi metodami VPN A HTTPS

7.1 TCP (Transmission control protocol)

Základní internetový protokol, který představuje transportní vrstvu a je základem pro vytvoření spojení mezi počítači a uskutečňuje přenos dat. Jeho vlastnosti:

- Spolehlivá transportní služba, což představuje dodání dat k cíli bez ztrát a ve správném pořadí
- Jedná se o službu, která si vyžádá spojení, uskuteční spojení a ukončí spojení po dokončení přenosu dat
- Umožňuje plně duplexní spojení, tedy komunikace a přenos dat v obou směrech

7.2 IP (Internet protocol)

Jde o základní protokol Internetu. Jedná se o datový protokol pro posílání dat. Data se zasílají v datagramech. Datagramy se zasílají pomocí jednoznačných identifikátorů – IP adres k cíli. Každý datagram je samostatná datová jednotka a musí obsahovat informace o odesílateli a příjemci, aby mohlo k odeslání dat vůbec dojít. Jeho vlastnosti:

- Nezaručuje správné doručení datagramů ve správném pořadí (spolehlivost řeší TCP nebo aplikace ve vyšších vrstvách)
- Segmentuje a sestavuje datagramy

7.2.1 IPv4

Protokolová verze IP protokolu. Pouze 32 bitové adresy, což v dnešní době je nedostačující a je nedostatek IP adres.

7.2.2 IPv6

Protokolová verze IP protokolu. Již 128 bitové adresy. Zajišťuje větší bezpečnost a podporu mobilních zařízení. Rozděluje přenášené data a umožňuje jednoduchý převod z verze IPv4.

7.3 Internet

Jedná se o světově rozsáhlou, veřejnou a vzájemně propojenou počítačovou síť tvořenou jednotlivými menšími sítěmi, které jsou spojeny pomocí protokolu IP. Vlastnosti Internetu:

- Slouží pro přenos informací
- Poskytuje služby jako chat, sdílení souborů, elektronická pošta, on-line hraní her, www stránky a jiné.

7.4 Počítačové sítě

Jedná se o technické prostředky s jejichž pomocí se uskutečňuje spojení a výměna dat (informací) mezi počítači.

7.4.1 LAN síť

Local Area Network – **LAN** – běžně síť v jedné nebo několika sousedních budovách. V rámci budovy se používá strukturovaná kabeláž kombinují UTP kabely a optické kabely. Pro spojování budov se používají optické kabely nebo bezdrátové spoje.

7.4.2 MAN síť

Metropolitan Area Network – **MAN** – je označení pro síť většího rozsahu pokrývající např. území velkého podniku nebo města. Velmi zjednodušeně lze říci, že MAN je LAN s velkým počtem budov nebo několik LAN spojených vysokorychlostní páteří.

7.4.3 WAN síť

Wide Area Network – **WAN** – je síť tvořená větším či menším počtem vzájemně vzdálených LAN. LAN jsou spojovány většinou pronajatými datovými okruhy. Použité aktivní prvky (dnes již téměř výhradně směrovače) umožňují nejen přenos dat, ale ve stále větší míře i spojování telefonních ústředen.

7.4.4 PAN síť

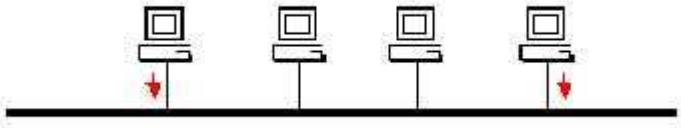
Personal Area Network – **PAN** – sítě jsou osobní počítačové sítě, které nemají velkou přenosovou rychlost, ale snaží se o odolnost proti rušení, malou spotřebou energie a

jednoduchá modifikace sítě. Dosah je pouze pár metrů. Zástupci této sítě jsou Bluetooth, IrDA, ZigBee. [9]

7.5 Technologie Ethernet

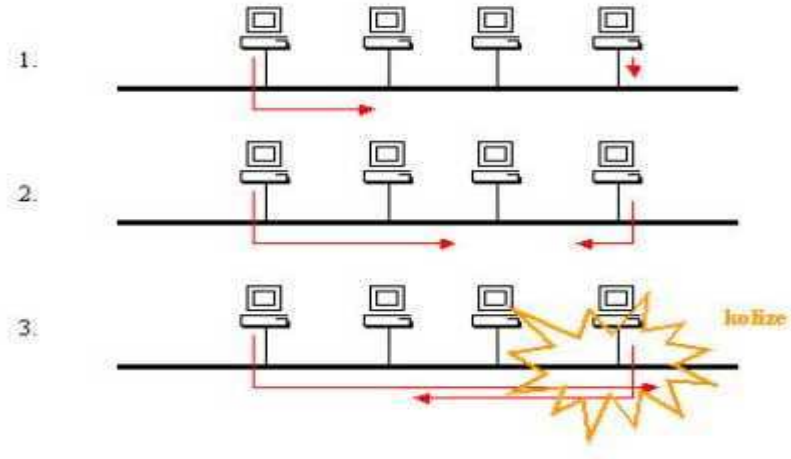
Ethernet je nejrozšířenější a nejpoužívanější síťovou technologií. Ethernet v dnešní době pronikl i do průmyslového prostředí, aby byla sjednocena komunikace mezi zařízeními v automatizační sítích. Označuje se jako „EtherNet/IP“. Rozdíl mezi Ethernetem a EtherNet/IP je použití speciálních protokolů ControlNet a DeviceNet. Klasický Ethernet je založen na principu metody CSMA/CD.

CSMA (Carrier Sense Multiple Access) - stanice připravená vysílat data si "poslechne" zda přenosové médium (kabel) nepoužívá jiná stanice. V případě, že ano, stanice zkouší přístup později až do té doby dokud není médium volné. V okamžiku kdy se médium uvolní začne stanice vysílat svá data.



Obr. 25 Metoda CSMA

CD (Collision Detection) - stanice během vysílání sleduje zda je na médiu signál odpovídající vysílaným úrovním (tedy aby se např. v okamžiku kdy vysílá signál 0 nevyskytl signál 1). Případ kdy dojde k interakci signálů více stanic se nazývá kolize. V případě detekce kolize stanice generuje signál JAM a obě (všechny) stanice které v daném okamžiku vysílaly generují náhodnou hodnotu času po níž se pokusí vysílání zopakovat.



Obr. 26 Metoda CD

K obrázku:

fáze 1 - stanice vlevo si poslechla na drátu zda někdo vysílá, zjistila, že ne a začala sama posílat data; v okamžiku kdy ještě signál nedorazil ke stanici vpravo si tato stanice ověřila stav média, zjistila, že je možnost zahájit vysílání

fáze 2 – obě stanice posílají data

fáze 3 – stanice vpravo zjistila kolizi a generuje signál JAM, všechny vysílající stanice zastavují vysílání a generují náhodné číslo [10]

7.5.1 Verze Ethernetu

Ethernet - původní varianta s přenosovou rychlostí 10 Mbit/s. Definována pro koaxiální kabel, kroucenou dvojlinku a optické vlákno.

Fast Ethernet - rychlejší verze s přenosovou rychlostí 100 Mbit/s definovaná standardem IEEE 802.3u. Převzala maximum prvků z původního Ethernetu (formát rámce, algoritmus CSMA/CD apod.), aby se usnadnil, urychlil a zlevnil vývoj. V současnosti ji lze považovat za základní verzi Ethernetu. Je k dispozici pro kroucenou dvojlinku a optická vlákna.

Gigabitový Ethernet - zvýšil přenosovou rychlost na 1 Gbit/s. Opět recykloval co nejvíce prvků z původního Ethernetu, teoreticky i algoritmus CSMA/CD. V praxi je ale gigabitový Ethernet provozován jako přepínaný s plným duplexem. Důležité je především použití

stejného formátu rámce. Původně byl definován pouze pro optická vlákna (IEEE 802.3z), později byla doplněna i varianta pro kroucenou dvojlinku (IEEE 802.3ab).

Desetigigabitový Ethernet - představuje zatím poslední standardizovanou verzi. Jeho definice byla jako IEEE 802.3ae přijata v roce 2003. Přenosová rychlost činí 10 Gbit/s, jako médium zatím slouží výlučně optická vlákna a opět používá stejný formát rámce. Algoritmus CSMA/CD byl definitivně opuštěn, tato verze pracuje vždy plně duplexně. V současnosti se vyvíjí jeho specifikace pro kroucenou dvojlinku.

7.5.2 Typy Ethernetu

10Base5 - Původní Ethernet na koaxiálním kabelu o rychlosti 10 Mbit/s. Koaxiální kabel o impedanci 50 Ω tvoří sběrnici, ke které se připojují pomocí speciálních tranceiverů a AUI kabelů jednotlivé stanice.

10Base2 - Ethernet na tenkém koaxiálním kabelu o rychlosti 10 Mbit/s. Koaxiální kabel tvoří sběrnici, ke které se připojují jednotlivé stanice přímo. Kabel je impedance 50 Ω (RG-58) nesmí mít žádné odbočky a je na koncích zakončen odpory 50 Ω (tzv. terminátory).

10Base-T - Jako přenosové médium používá kroucenou dvojlinku s rychlostí 10 Mbit/s. Využívá dva páry strukturované kabeláže ze čtyř. Dnes již překonaná síť, která byla ve většině případů nahrazena rychlejší 100 Mbit/s variantou.

10Base-F - Varianta s optickými vlákny o rychlosti 10 Mbit/s. Používá se pro spojení na větší vzdálenost, nebo spojení mezi objekty, kde nelze použít kroucenou dvojlinku. Tvořila obvykle tzv. **páteřní síť**, která propojuje jednotlivé menší celky sítě. Dnes je již nahrazována vyššími rychlostmi (Fast Ethernet, Gigabit Ethernet).

100Base-TX - Varianta s přenosovou rychlostí 100 Mbit/s, které se říká **Fast Ethernet**, používá dva páry UTP nebo STP kabelu kategorie 5.

100Base-T2 - Používá dva páry UTP kategorie 3, 4, 5. Je to varianta vhodná pro starší rozvody strukturované kabeláže.

100Base-T4 - Používá čtyři páry UTP kategorie 3, 4, 5. Také vhodná pro starší rozvody strukturované kabeláže.

100Base-FX - Fast Ethernet používající dvě optická vlákna.

1000Base-T - Ethernet s rychlostí 1000 Mbit/s, nazývaný **Gigabit Ethernet**. Využívá 4 páry UTP kabeláže kategorie 5e, je definován do vzdálenosti 100 metrů.

1000Base-CX - Gigabit Ethernet na bázi měděného vodiče pro krátké vzdálenosti, učený pro propojování skupin zařízení.

1000Base-SX - Gigabit Ethernet používající mnohavidové optické vlákno. Je určen pro páteřní sítě do vzdáleností několik set metrů.

1000Base-LX - Gigabit Ethernet používající jednovidové optické vlákno. Je určen pro větší vzdáleností až několika desítek kilometrů.

10GBase-T - Ethernet s rychlostí 10 Gbit/s, nazývaný **Ten Gigabit Ethernet**(nebo také EFM - Ethernet on the first mile). Využívá 4 páry S/FTP (jednotlivé páry stíněné metalickou fólií + metalický oplet kolem všech párů dohromady) kabeláže kategorie 6A (Category 6 Augmented - šířka pásma 500 MHz), je definován do vzdálenosti 100 metrů. V současné době (rok 2007) je ve vývoji nestíněná varianta UTP kabeláže kategorie 6A. [11]

8 PŘÍSTUP K EZS PŘES TCP/IP A INTERNET

K ústřednám EZS lze přistupovat na základě různých variant. Jednotlivé schémata vysvětlují, jak nastavení, které nutné pro komunikaci pomoci TCP/IP sítí a Internetu, tak schéma vzdáleného připojení.

8.1 Schéma vzdáleného přístupu k EZS přes převodníky varianta č. 1

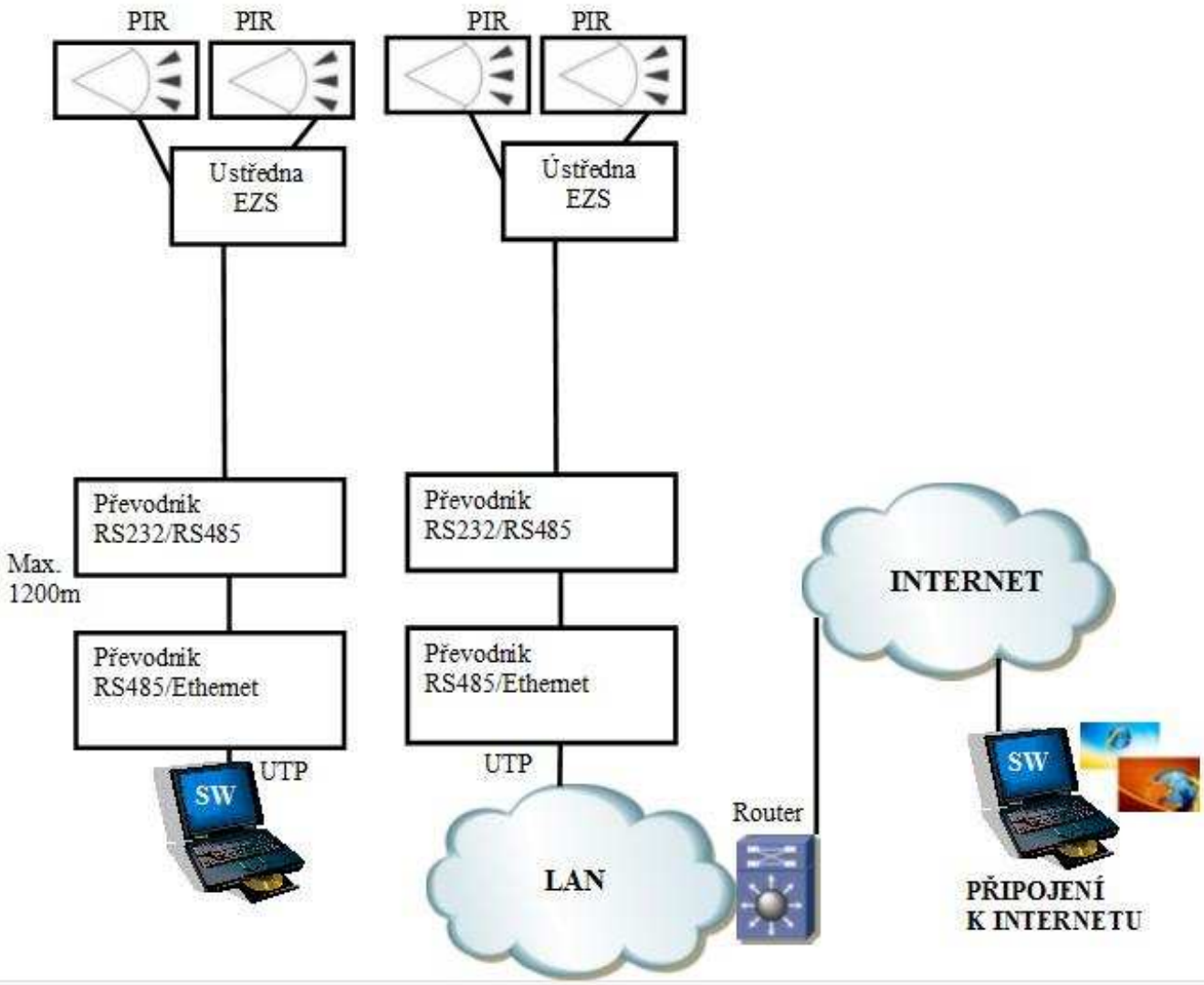


Schéma blíže k levému okraji znázorňuje prvotní konfiguraci ústředny EZS pomocí aktivního převodníku (dle výrobce) z výstupu RS 232 ústředny na RS 485 pro dosažení větší vzdálenosti mezi ústřednou sítí (až 1200m). Tedy můžeme pohlížet na tento převodník jako na prodloužení kabelu. Převodník z rozhraní RS 485 na rozhraní Ethernet, řeší převod signálu do TCP/IP datových paketů. K převodníků připojíme pomocí UTP

kabelu Cat. 5E a koncovky RJ-45 PC. Pak se dá nastavit ve webovém rozraní převodníků komunikace a IP adresace, která bude přiražena ústředně a ústředna po ni bude komunikovat po TCP/IP sítích.

Na obrázku blíže k pravému okraji je znázorněno zapojení po nastavení IP adresace, kdy se odpojí PC od převodníků a pomocí UTP kabelu Cat. 5E se připojí převodník do LAN sítě (určitého aktivního prvku sítě). Pokud budeme chtít přistoupit do ústředny bude stačit ze sítě LAN pouze znalost IP adresy a mít SW určený pro vzdálený monitoring či správu k ústředně. Jestliže se chceme připojit z velmi vzdáleného místa mimo LAN síť, kde je ústředna připojena, pak se nedoporučuje i přesto, že je to možné přistupovat přes otevřené Internetové rozhraní, ale za pomocí šifrování, které umožňují přímo určité převodníky nebo pomocí VPN služby.

8.2 Schéma vzdáleného přístupu k EZS přes převodníky varianta č. 2

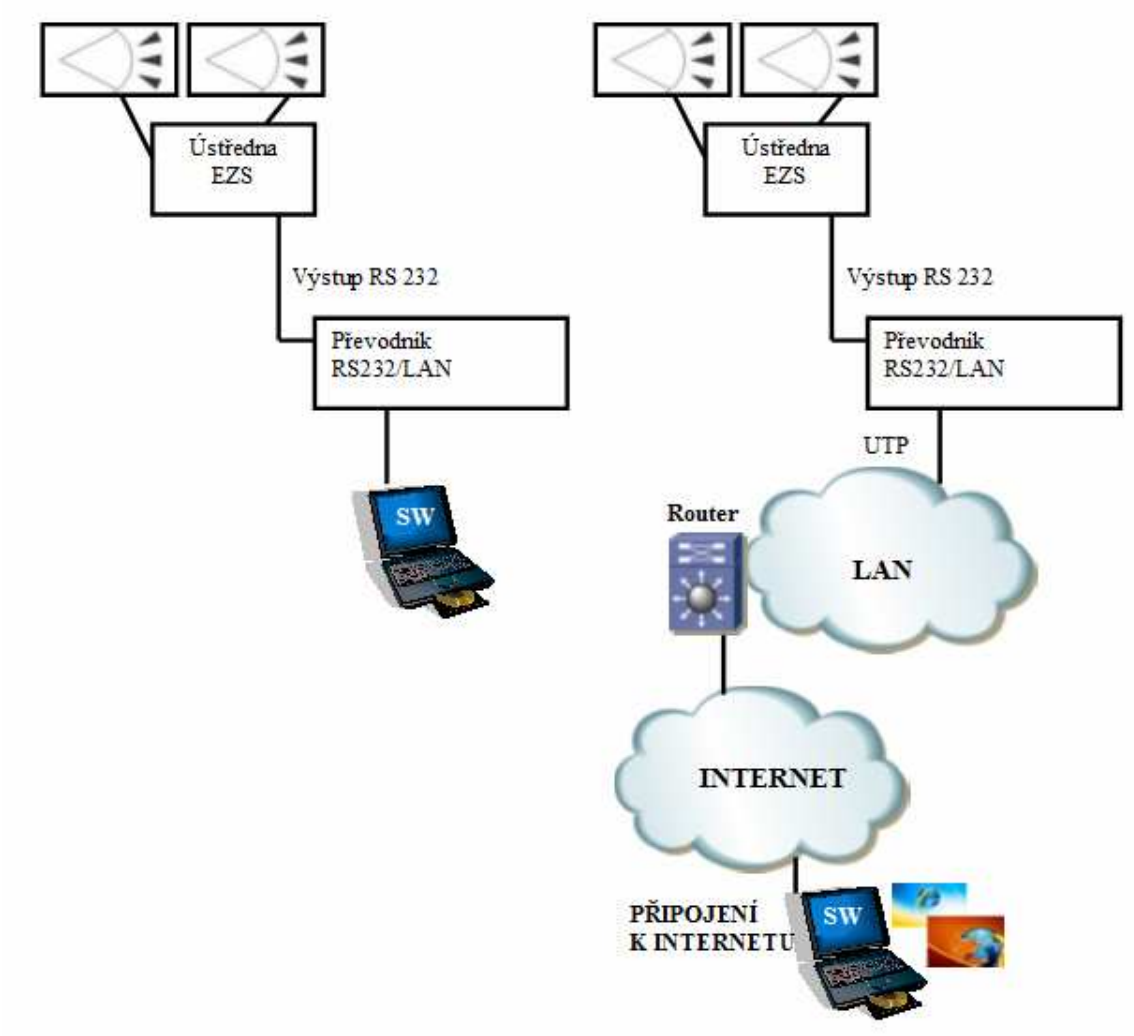
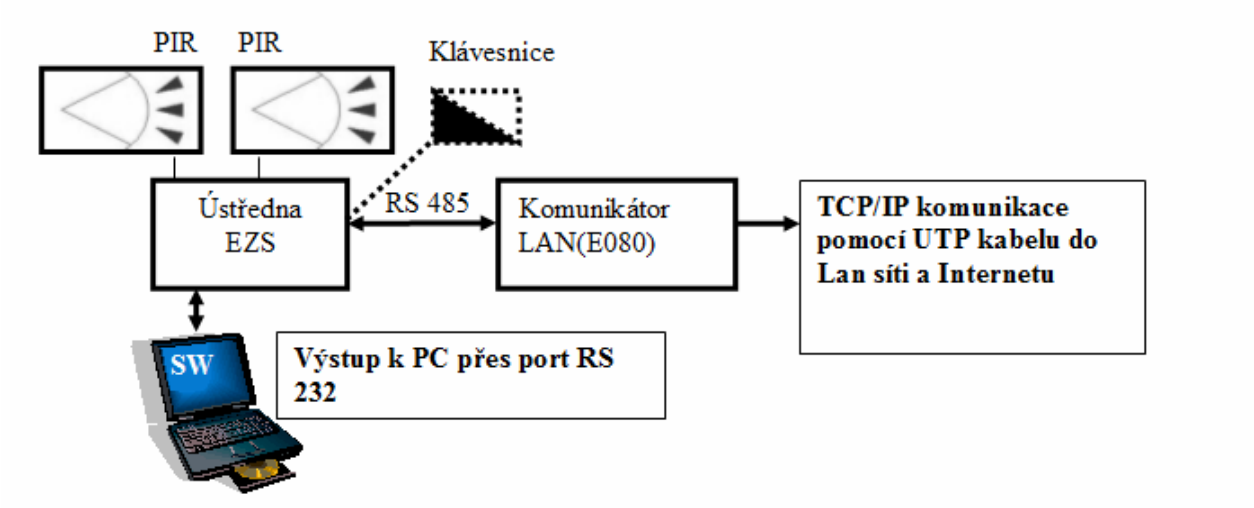
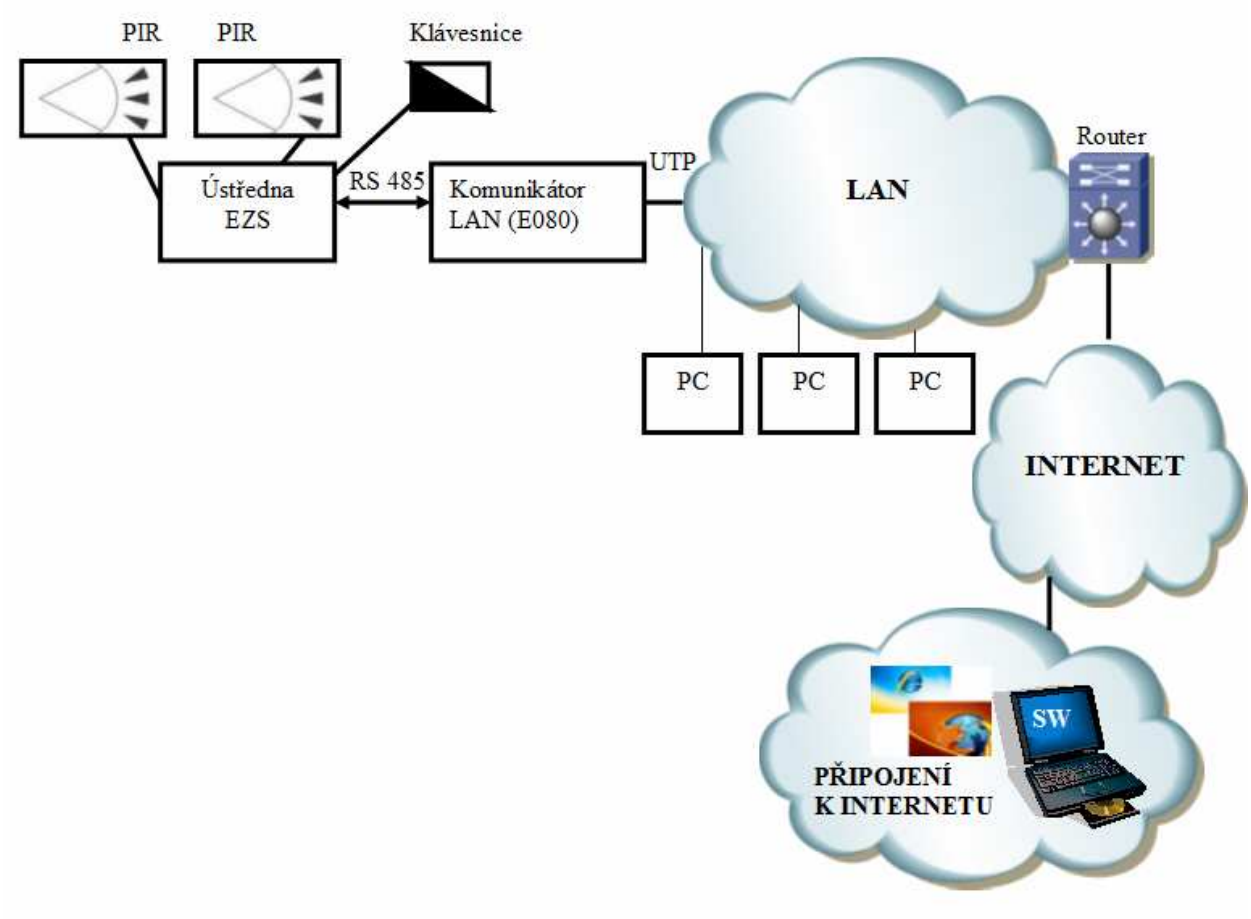


Schéma blíže k levému okraji znázorňuje prvotní konfiguraci ústředny EZS pomocí aktivního převodníku (dle výrobce) z rozhraní ústředny RS 232 na rozhraní Ethernet. Použití převodníků se používá pro kratší vzdálenosti do 100m. Převodník z rozhraní RS 232 na Ethernet, řeší převod signálu do TCP/IP datových paketů. K převodníků připojíme pomocí UTP kabelu Cat. 5E a koncovky RJ-45 PC. Pak se dá nastavit ve webovém rozraní převodníků komunikace a IP adresace, která bude přiražena ústředně a ústředna po ni bude komunikovat po TCP/IP sítích.

Na obrázku blíže k pravému okraji je znázorněno zapojení po nastavení IP adresace, kdy se odpojí PC od převodníků a pomocí UTP kabelu Cat. 5E se připojí převodník do LAN sítě (určitého aktivního prvku sítě). Pokud budeme chtít přistoupit do ústředny bude stačit ze sítě LAN pouze znalost IP adresy a mít SW určený pro vzdálený monitoring či správu k ústředně. Jestliže se chceme připojit z velmi vzdáleného místa mimo LAN síť, kde je ústředna připojena, pak se nedoporučuje i přesto, že je to možné přistupovat přes otevřené Internetové rozhraní, ale za pomocí šifrování, které umožňují přímo určité převodníky nebo pomocí VPN služby.

8.3 Schéma vzdáleného přístupu k EZS přes komunikátory varianta č. 1



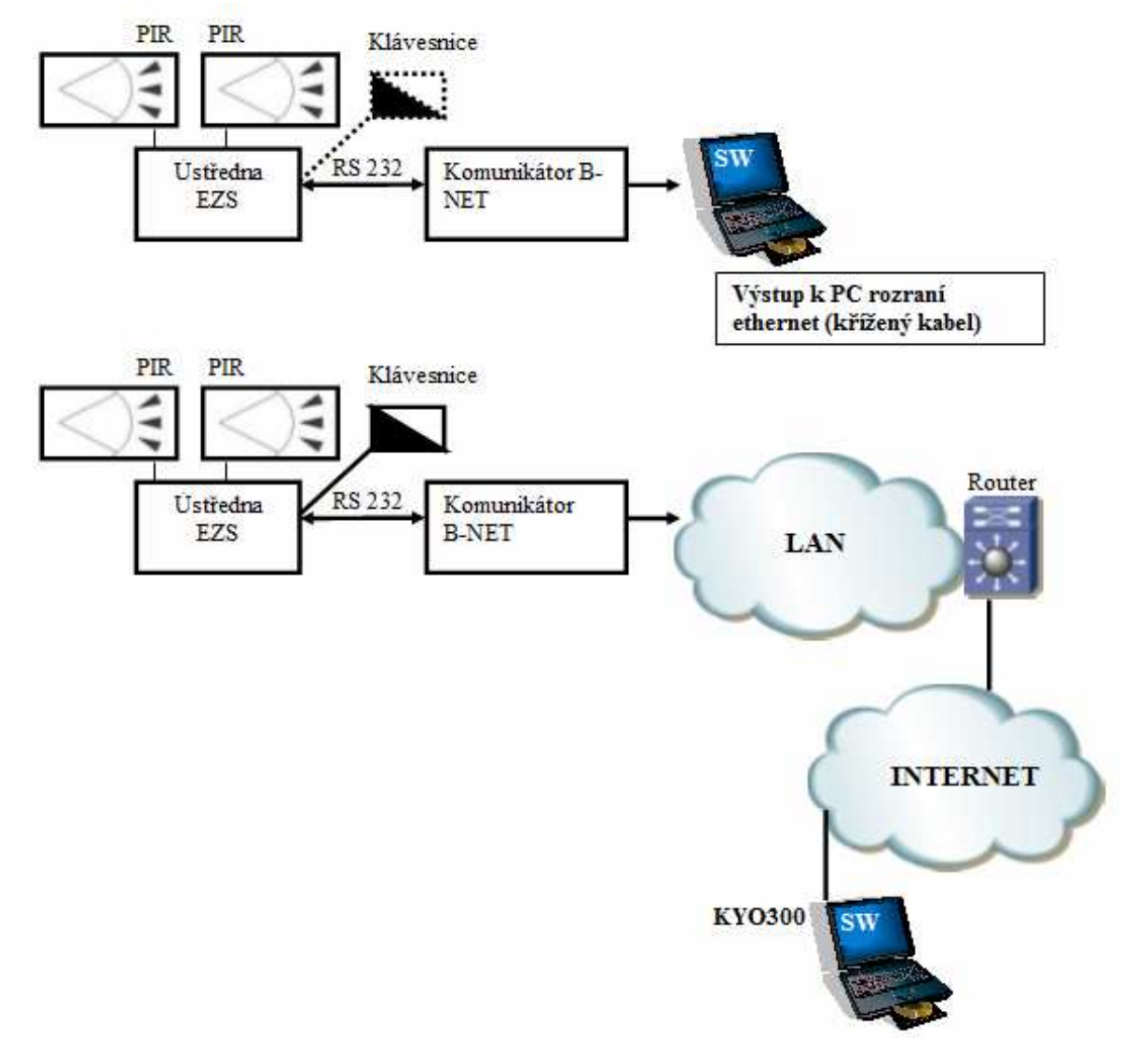


Obrázek pro nastavení parametrizace ústředny je vytvořen na základě podkladů pro ústřednu Galaxy G3, která umožňuje pomocí Ethernet (LAN) komunikátoru uvést ústřednu do TCP/IP sítí a tím vzdáleně provádět lokální monitoring, správu uživatelů EZS, Instalační programování, dálkovou diagnostiku.

Na linku RS 485, která je na výstupu z ústředny se připojí Ethernetový komunikátor. Pro ústřednu Galaxy G3 je přímo vytvořen speciální Ethernetový komunikátor s označením E080. Tento komunikátor nemá vlastní inteligenci v podobě webového rozhraní. Veškeré nastavení IP adresace pro sítě se provádí připojením PC k ústředně přes linku RS 232 a pomocí SW lze tento modul E080 konfigurovat a nastavovat, nebo u tohoto typu ústředny nastavení pro komunikaci v sítích TCP/IP se dá pomocí klávesnice ústředny. Po nastavení priorit nezbytných pro uvedení ústředny s modulem do LAN sítí se PC odpojí a modul E080 se zapojí pomocí UTP kabelu Cat. 5E do aktivního prvku sítě. Tím lze pří znalosti IP adresy a nezbytného konfiguračního SW, který umožňuje komunikaci po Ethernetu je možno ústřednu naprogramovat, změřit parametry systému EZS (hodnoty napájecího napětí, proudové odběry,odpory poplachových smyček a další parametry), zjistit poruchové

stavy a případně systém ovládat. V případě správy nikoli v rámci LAN sítě, ale přes Internet z libovolného místa bych opět doporučil šifrování dat nebo v lepší případě používat VPN službu, která zaručuje u těchto důležitých dat větší bezpečí.

8.4 Schéma vzdáleného přístupu k EZS přes komunikátory varianta č. 2



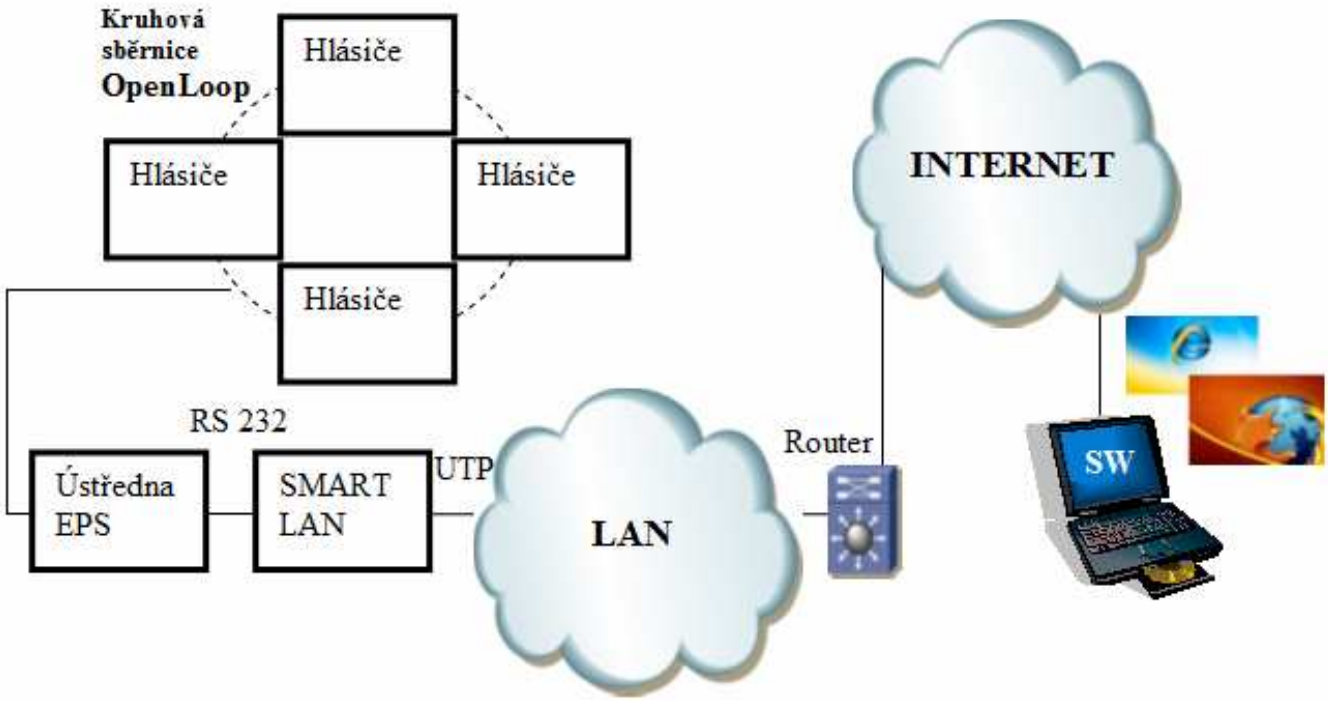
Pro variantu vzdáleného přístupu číslo 2, jenž je zapojena prostřednictvím Ethernet komunikátor B-NET. Modul B-NET neboli CENBNET je vytvořen pro ústředny Bentel. Specificky lze použít pro ústřednu KYO 320. Umožňuje dálkovou správu systému. Konfigurace se realizuje pomocí klávesnice nebo pomocí přímo PC připojeného k modulu pomocí kříženého kabelu UTP Cat. 5E. CENBNET modul má svou specifickou IP tovární

adresu, kterou lze přes konfigurační software změnit na požadovanou dle sítě, kde bude umístěná. V případě použití veřejné IP adresy se dá systém ovládat přes Internet. Možnost je použití i pevná vnitřní IP adresy, ale pak doporučím přistoupit přes VPN službu, kde se vytvoří zabezpečený tunel, který se připojí do sítě LAN (libovolné) a po navázání spojení a ověření přístupu do sítě se PC, z kterého požadujeme vzdálenou správu bude chovat jako by byl fyzicky umístěn a připojen v sítí LAN. Pak komunikace dle práv a přístupu již probíhá v rámci sítě LAN. Pak již stačí přes SW parametrizovat ústřednu. Některé moduly obsahují mimo SW aplikací i vlastní vnitřní inteligenci na kterou se můžeme pomocí IP adresy, jenž se předem nastavila připojit a provádět nastavení i tímto způsobem. Pak není problém ústřednu naprogramovat, změřit parametry systému EZS (hodnoty napájecího napětí, proudové odběry,odpory poplachových smyček a další parametry), zjistit poruchové stavy a případně systém ovládat.

9 PŘÍSTUP K EPS PŘES TCP/IP A INTERNET

K systémům případně ústřednám EPS lze rovněž přistoupit na základě převodníků nebo komunikátoru speciálně vyvinutých pro Ethernetové rozhraní nebo převod linek RS 232 či RS 485 do Ethernetu.

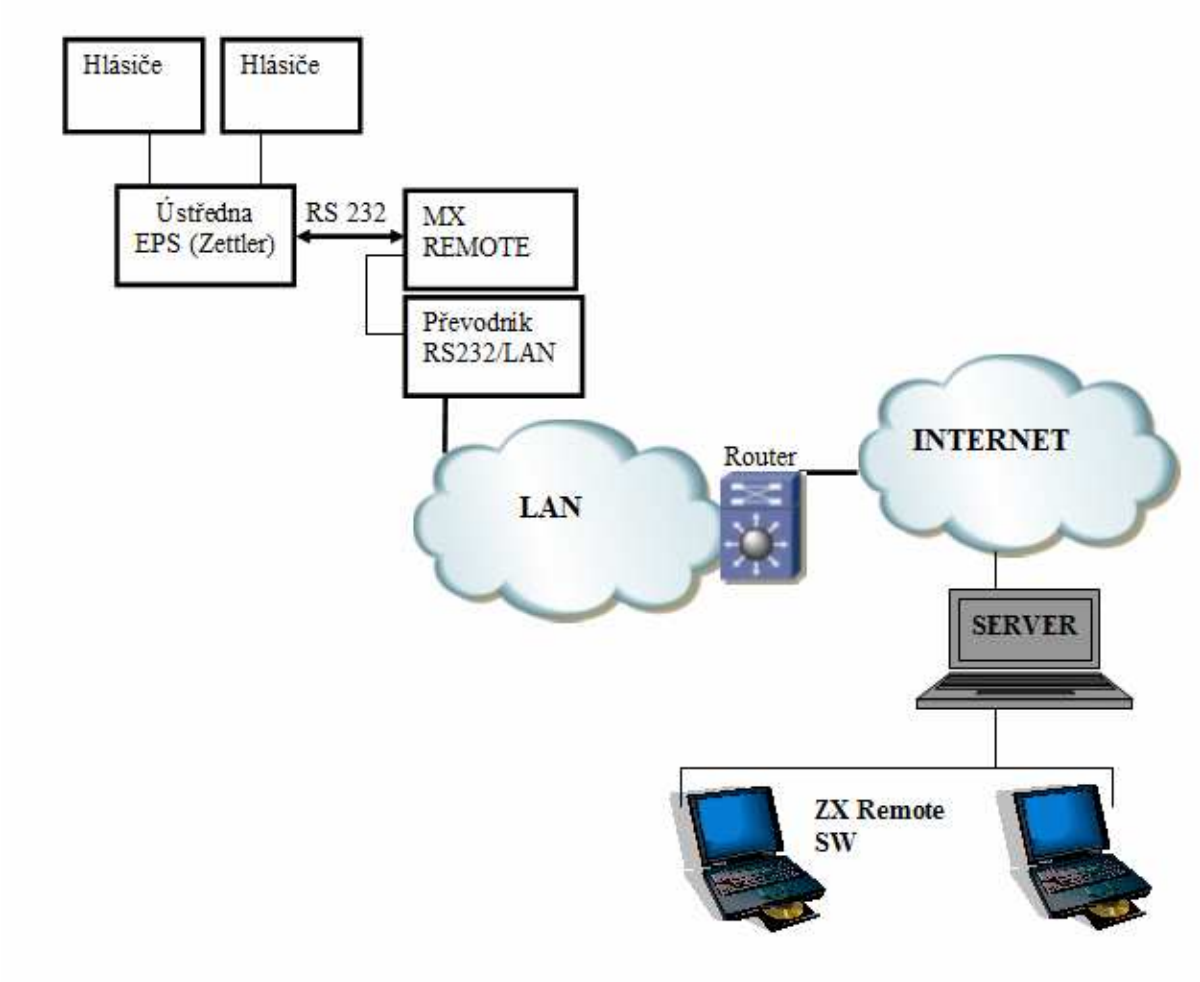
9.1 Schéma vzdáleného přístupu k EPS přes LAN komunikátor



Způsob zapojení pro EPS systém, jak je vidět na obrázku se řeší pomocí ústředny EPS značky INIM, pomocí kruhové sběrnice OpenLoop speciálně vyvinuté pro připojení hlásičů umožňuje ústředně automaticky načíst data o hlásičích, přiřadit jim adresy a kontrolovat jejich stav. Také je odolná vůči rozpojení a zkratování linky. Modul pro rozhraní Ethernet s názvem SmartLAN, jenž umožňuje vzdálenou správu systému přes web rozhraní, posílání emailů a taky vzdálené programování pomocí programovacího softwaru se instaluje k ústředně přes linku RS 232 a má nastavenou statickou IP adresu, která se dá změnit. Při připojení do sítě Ethernet se můžete z Internetu připojovat, buď přes VPN, pokud tuto službu poskytuje router, nebo po zadání veřejné IP adresy do web prohlížeče,

ale pak router musí přesměrovat spojení na ústřednu, resp. modul SmartLAN. Základem SmartLAN modulu je inteligence Janus. S pomocí této karty lze dálkově zprávu a programování. Karta je schopna posílat detailní výpis události na E-mail i s přílohy obsahující tzv. mapy objektu.

9.2 Schéma vzdáleného přístupu k EPS přes MX Remote

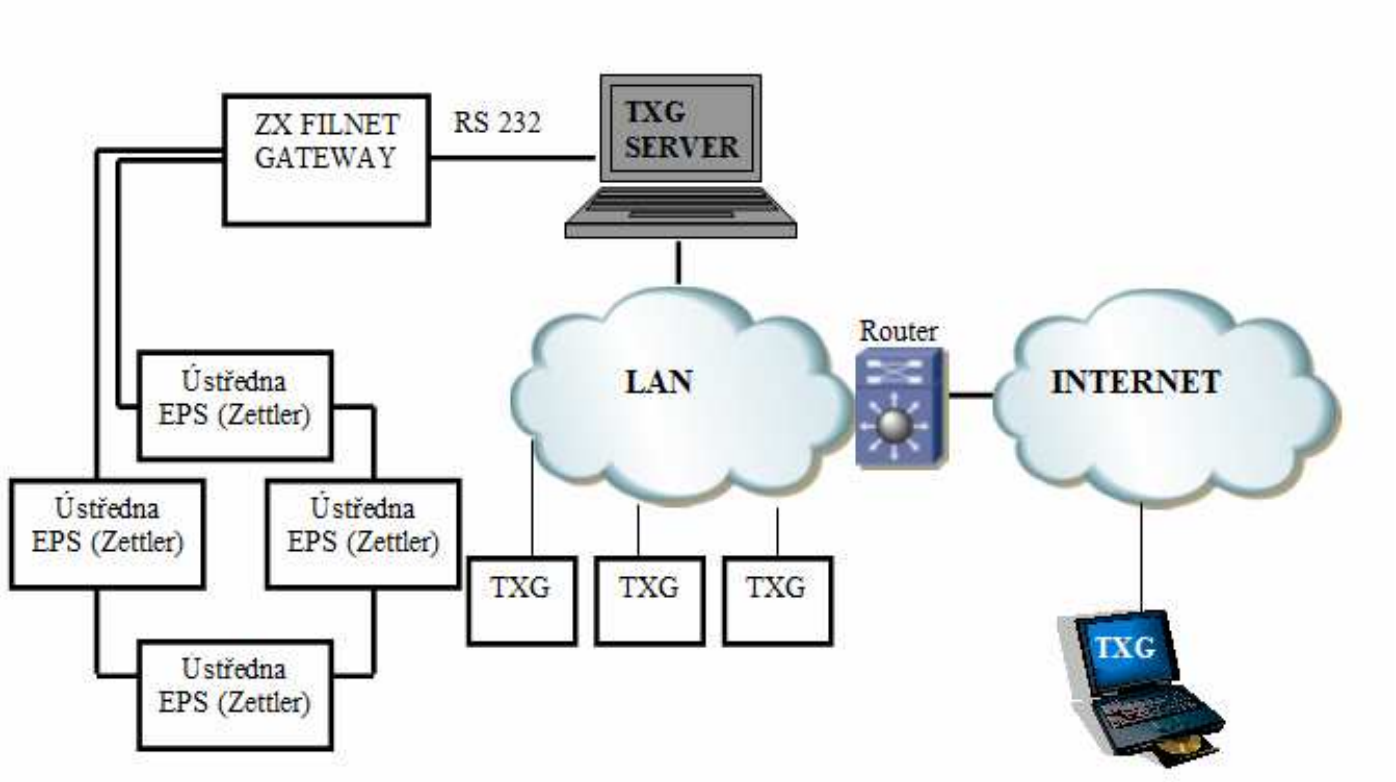


Metoda založena u ústředny Zettler Expert na nadstavbovém interface MX Remote. Tento interface je propojen s ústřednou po lince RS . Interface, jenž obsahuje linku RS 232 se připojí k převodníku na Ethernetové rozhraní (TCP/IP), a tak pracuje v datovém prostředí sítí založených na TCP/IP protokolu.

Dále existují různě diagnostické SW pro systémy EPS. K ústřednám ZETTLER Expert se používá ZX Remote, který umožní kompletní dálkovou správu a dohled systému EPS. V schématu je uvedeno SW ZX Remote připojený na Server ZX Remote, který sbírá

data z ústředny pomocí převodu signálů přes rozhraní MX Remote a převodníků na TCP/IP datové pakety, které jsou průchozí přes datové sítě k serveru.

9.3 Schéma vzdáleného přístupu k EPS přes ZX Filnet



V případě zapojení schématu (kapitola 8.3) ústředny EPS respektive při použití více ústředen v kruhovém zapojení jsou ústředny vzájemně propojeny a následně signál přiveden do síťové desky ZX Filnet, které zajišťuje síťové aplikace pro dvě a více ústředen v systému EPS. To je přivedeno na řídící Server TXG. Ke kterému buď z vnitřní sítě nebo přes Internet je možné na základě IP adresace vykonávat monitorování a řízení celého systému. Architektura je založena na bázi Klient / Server. Distribuce nadstavby je pro maximální počet 99 klientů připojených přes LAN/Internet a každý klient má specifické přístupové možnosti, různé zobrazení informací a je možno stanovit i stupeň obsluhy.

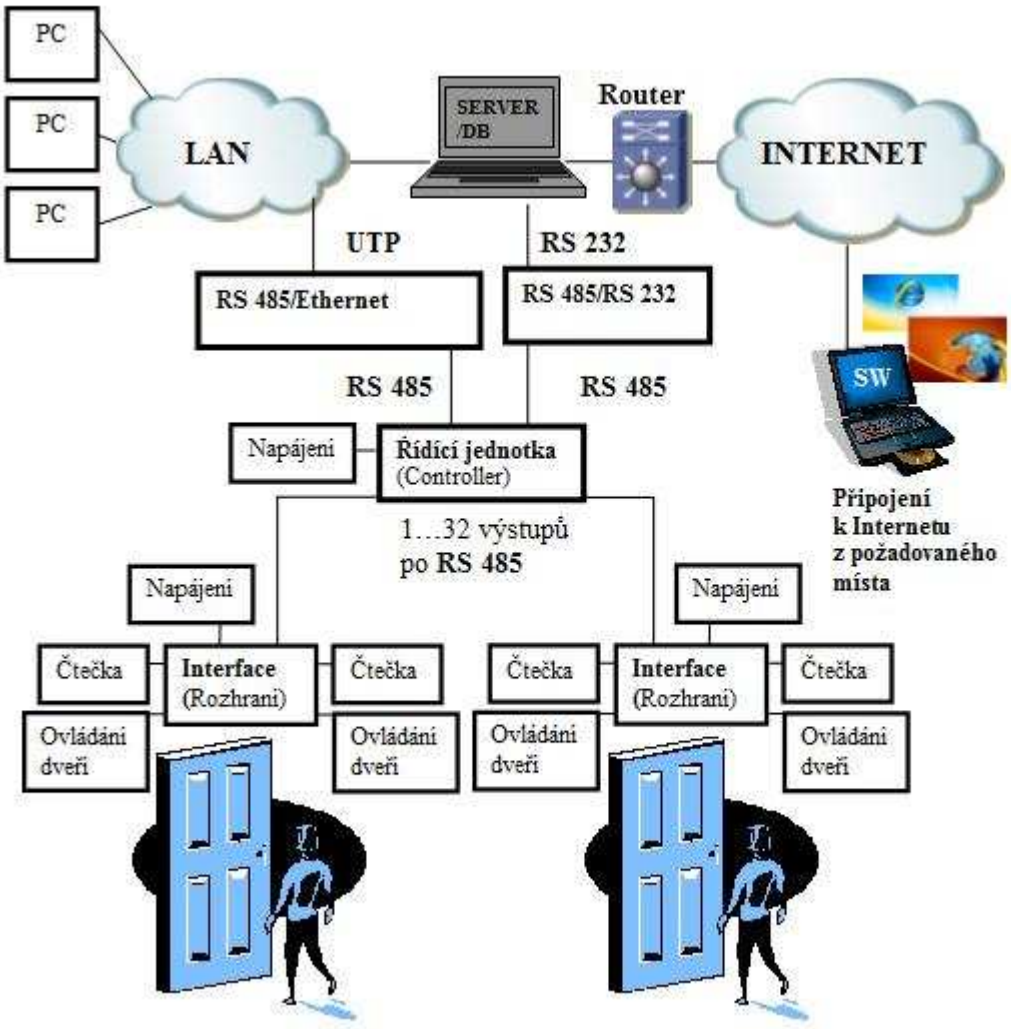
10 PŘÍSTUP K PŘÍSTUPOVÉMU SYSTÉMU (ACCESS CONTROL) PŘES TCP/IP A INTERNET

I u přístupových systémů se můžeme setkat se vzdáleným přístupem. Po konzultaci s odborníky, ale pouze v rámci LAN sítí, a v případě VPN služby lze přistoupit i vzdáleně přes Internet

Konfigurace v rámci sítí případně Internetu se pak řeší pomocí:

- Pomocí textových souborů a jejich následným přenosem službou a protokolem FTP
- Pomocí webového rozhraní – do prohlížeče se zadá IP adresa zařízení a číslo portu, následně do okna se zapíše přihlašovací jméno a heslo, tím se zjistí, kdo se přihlásil a jaké má práva při konfiguraci v systému (dáno předem softwarem) tedy pomocí protokolu http
- Telnet
- VPN

10.1 Schéma vzdáleného přístupu k ACS přes převodníky

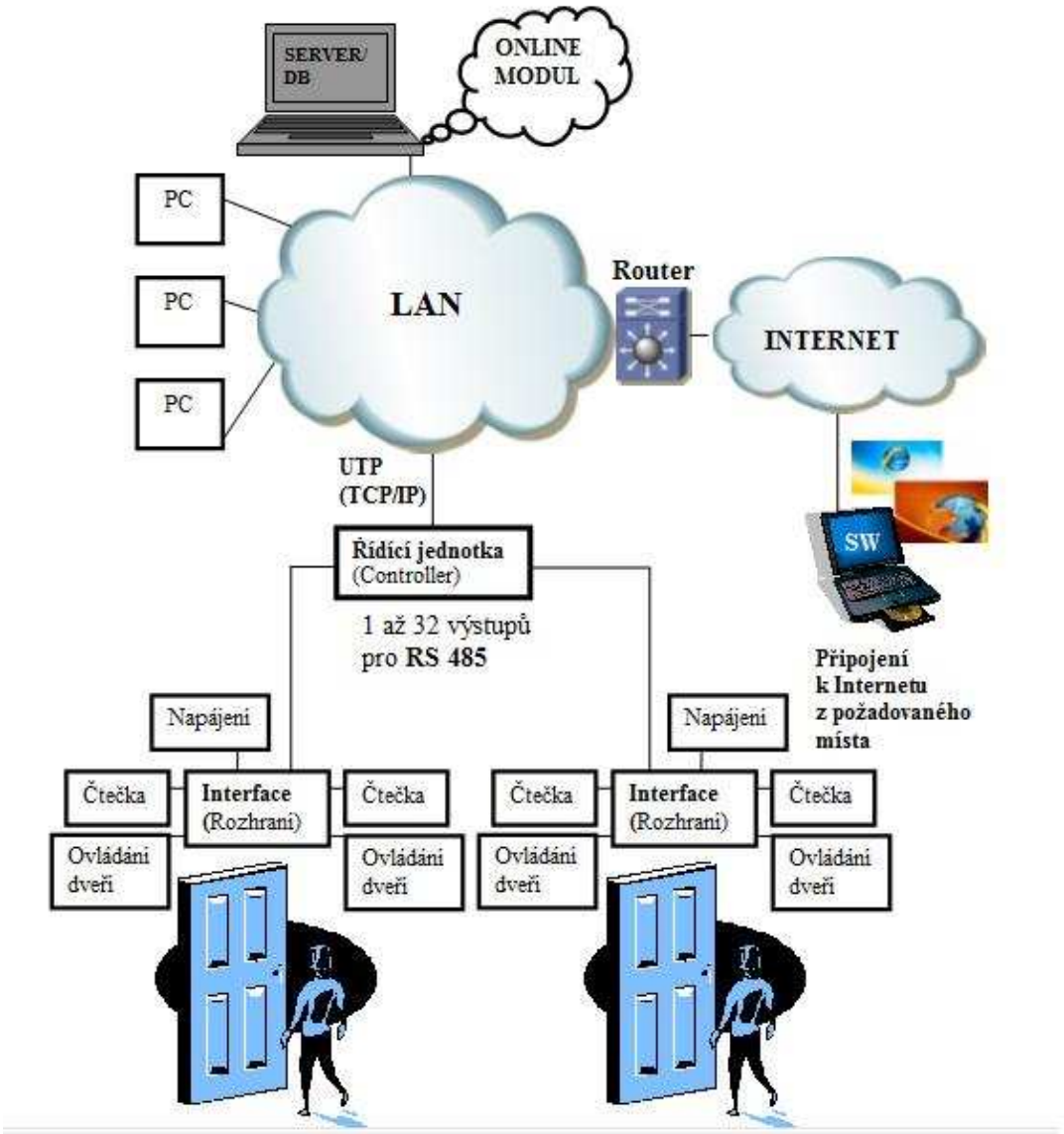


Skladba přístupového systému od čteček až po řídící jednotku, zajišťuje základní funkce a inteligenci celého ACS. Na schématu máme možnost vidět základní schéma pro přístup a jaká je možnost převedení signálů ASC do Ethernetových sítí. Z řídící jednotky je signál veden po lince RS 485 (dle výrobce), pak se musí signál převést do Ethernetové sítě (TCP/IP) pomocí inteligentního převodníku z linky RS 485 na Ethernet. Ten se následně připojí do aktivního prvku sítě a při jeho nastavené IP adresaci přebírá inteligenci odpovídající topologii Ethernetových sítí. Pak není problém libovolného místa z LAN sítě do webového prohlížeče zadat IP adresu převodníku a nastavit požadovanou IP adresaci převodníku pro vzdálený dohled přes Internet. V místě LAN sítě je umístěn server, který plní funkci databáze s obsahem a kompletní souhrnem informací o ACS. K tomuto serveru lze připojit řídíc jednotku přes sběrnici RS 232. Tyto souhrnné informace plní představu

o přístupových právech, časové zóny, informace o osobách, kteří se pohybují v určitých místech.

Dle systému lze mít určitý počet čteček na příslušný počet rozhraní, ale zároveň i na jednu řídící jednotku připadá určitý počet rozhraní. V případě schématu se jedná vždy o 2 čtečky připojené k rozhraní a rozhraní je připojené k řídící jednotce, kde je počet omezen na 32.

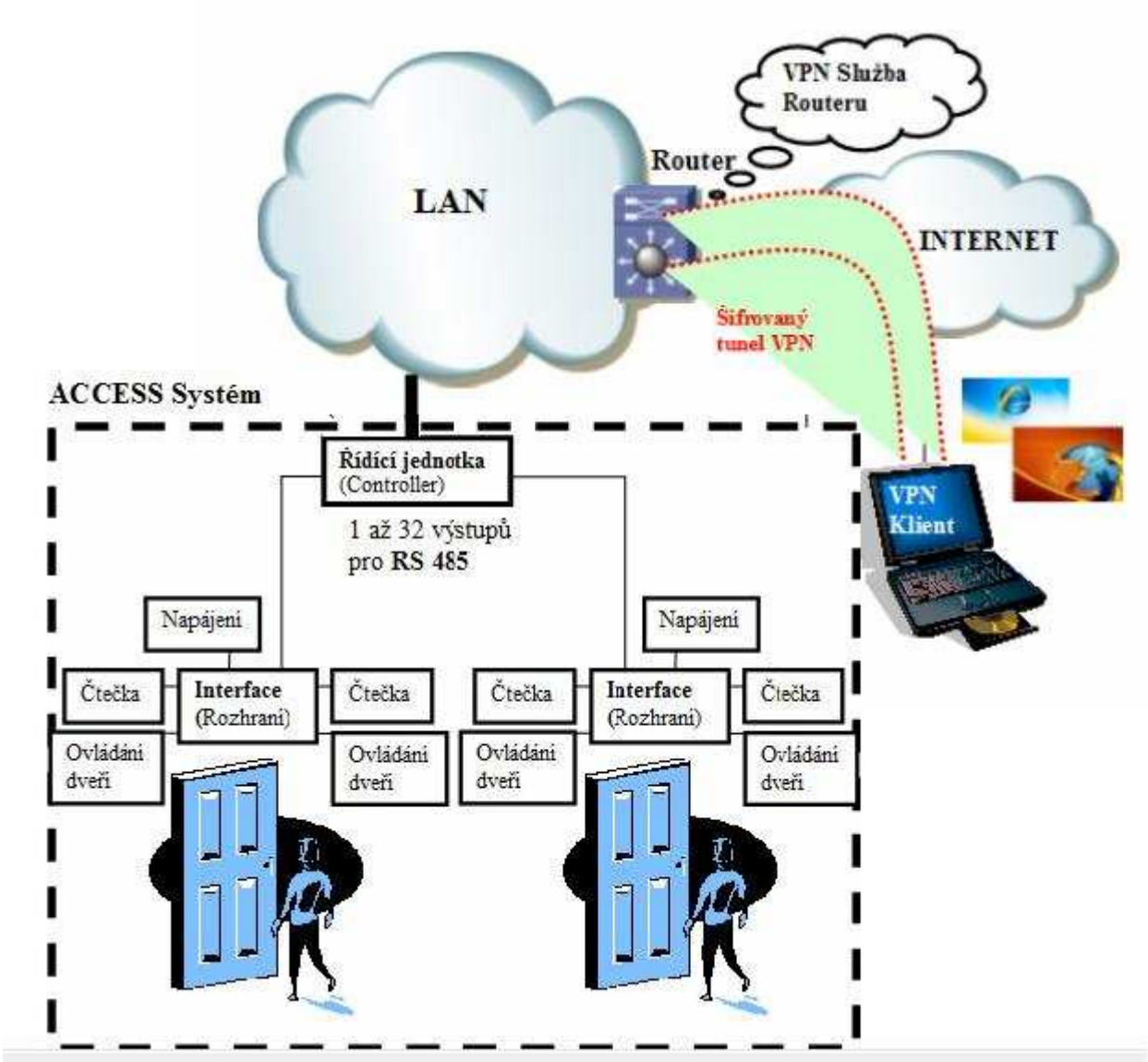
10.2 Schéma vzdáleného přístupu k ACS



Jiná varianta ACS pro přístup ze sítí LAN a Internetu představuje inteligentnější řídící jednotku. Ta obsahuje firmware a speciální rozhraní TCP/IP pro komunikaci v Ethernetových sítích. Pak není problém řídící jednotku přímo zapojit do aktivního prvku

sítě. Pak stačí spustit prohlížeč webových stránek a zadat IP adresu řídící jednotky. Ta má své webové rozhraní. Po vyplnění přihlašovací údajů a hesla se objeví prostředí webové, kde můžeme provést parametrizaci a nastavení modulu. Řídící jednotky zpravidla obsahují vnitrní paměť na počet událostí v řádech tisíců. Paměť je zde proto, aby v případě nějaké poruchy systémů bylo možné stále kontrolovat jednotlivé přístupy, časové zóny a evidenci osob v dané lokalitě. Po připojení k serveru systému řídící jednotka naváže spojení a předá data do databáze serveru. To můžeme pokládat za jednu z velkých předností systémů.

10.3 Schéma vzdáleného přístupu k ACS přes VPN



Nyní na schématu je vytvořen vzdálený přístup přes VPN službu. VPN služba je odvislá od možností sítě LAN a dle její struktury může být server s VPN službou, který se může různě konfigurovat. Pro vzdálený přístup k přístupovému systému musí být splněny podmínky již předem. Prvním faktem je přesně stanovená IP adresa serveru, který obsahuje databázi s informacemi o přístupovém systému. Jelikož ani systém přístupu ve firmách by neměl být otevřený systém, ale zavřený kvůli hrozícímu nebezpečí, musí se stanovit nejlépe IP adresa vnitřní sítě, která nebude přiřazena DHCP serverem. Tedy mluvíme o pevné vnitřní IP adrese. I přesto však můžeme použít jakoukoli IP adresu, pak by se ovšem jednalo o náročnější systém a jeho propracovaní. Při znalosti IP adresy zařízení nebo řídícího počítače stačí pouze nastavit (provádí ve firmách správce sítě) vzdálený přístup, tedy nastavit porty, firewall a přístupová práva do sítě. Tyto vygenerované údaje jsou podstatně pro další část. V následující části musíme nainstalovat na PC z kterého se chceme dostat do systému VPN klienta pro danou platformu operačního systému. Po instalaci stačí vyplnit již známe údaje do sítě a navázat spojení. Většinou jsou ve firmách ještě nadstavby SW pro přístup na síťové disky. Proto někdy je potřeba u ověřených osob použít přihlašovací jméno a heslo do firemní sítě. Poté vytvoří zabezpečená cesta až do vnitřní sítě na počáteční VPN server, který zjisti na základě údajů, zda je přístup povolen, jestliže je to známá osoba pro server pak spojení proběhne úspěšně a my se nacházíme s PC v síti, kde se nachází ACS. Ačkoliv jsme s počítačem řádově i stovky metrů od dané sítě po připojení se PC jeví jako by byl fyzicky připojen do aktivního prvku firemní sítě. Po přístupu přes VPN server končí zabezpečená cesta, protože není potřeba bezpečnost v zabezpečené vnitřní síti.

11 PŘÍSTUP K CCTV PŘES TCP/IP A INTERNET

Přístup ke kamerovým systémům je velmi specifický a odvíjí se od použitých kamer a zařízení pro obrazové monitorování či záznam. Nejdůležitější je mít v daném objektu počítačovou síť (LAN) s připojením k Internetu. Jestliže objekt je připojen k Internetu, pak už jen stačí vybrat druhy kamer popřípadě záznamové rekordéry a sledování obrazu v reálném čase přes Internet může být realizován. V kapitole 2.4 (CCTV) jsem se zmínil o analogových kamerách či digitálních (IP) kamerách. Vzdálený přístup přes Internet je reálný u obou druhů kamer. Akorát u analogovým kamer se musí signál digitalizovat (většinou pomocí digitálního záznamového rekordéru nebo video serveru) a převést tento signál na pakety odpovídající protokolu TCP/IP. U IP kamer je signál ihned digitalizován přímo v kameře a v podobě paketů je obrazový signál posílán prostřednictvím LAN sítí dále až k monitorovacímu či řídícímu pracovišti.

11.1 Schéma vzdáleného přístupu k analogovým kamerám pomocí DVR

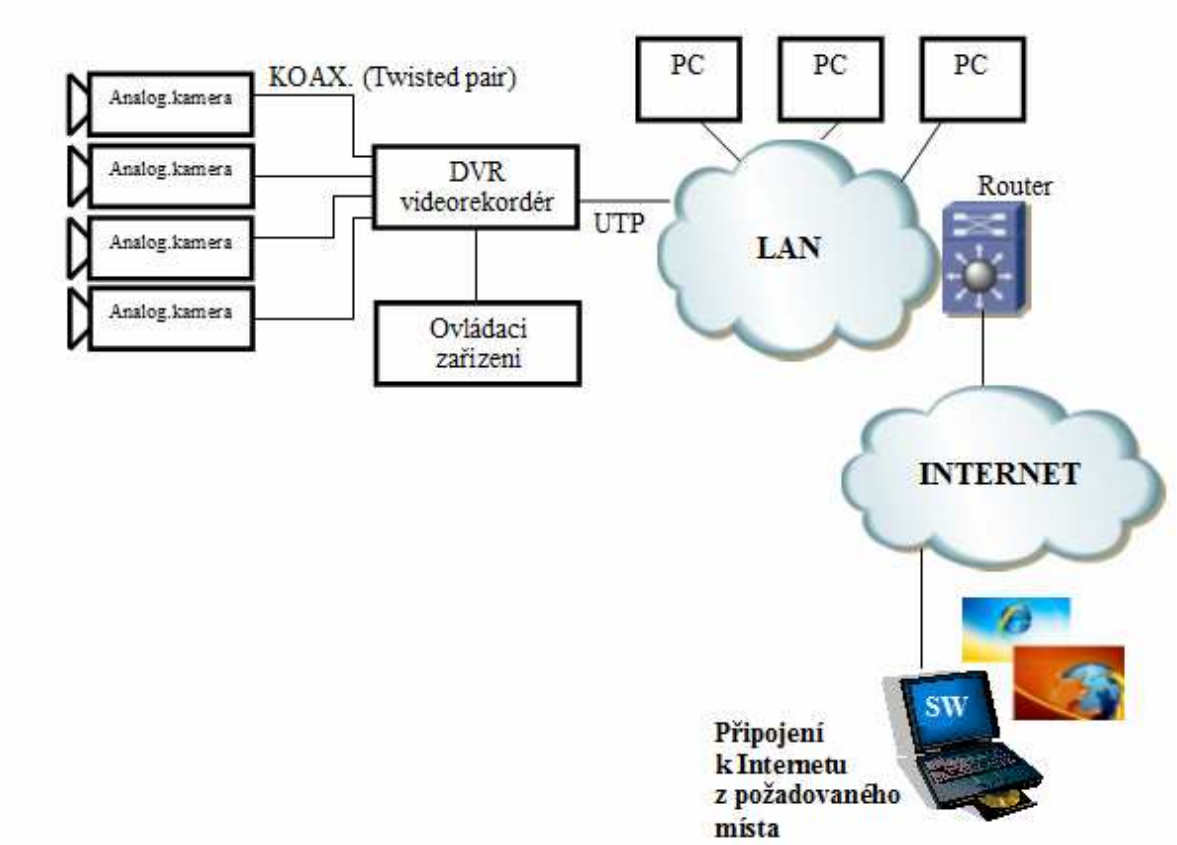
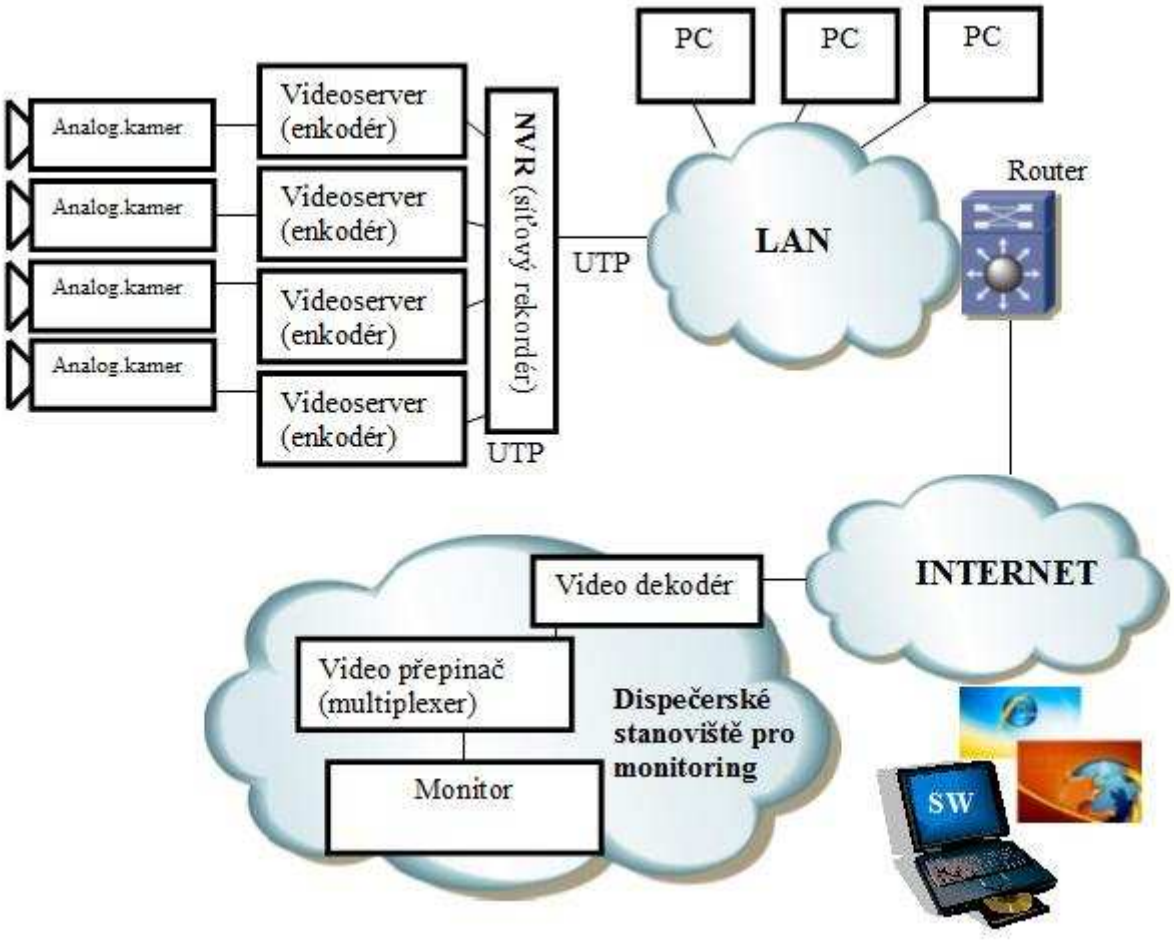


Schéma představuje zapojení analogových kamer, které stále v dnešní době prezentují 80% instalací proti digitální IP kamerovým systémům. Signály s kamer jsou připojeny koaxiální kabelem nebo kroucenou dvojlinkou k DVR. DVR dle typu a výrobce umožňují přes rozhraní RS 485 připojit ovládací zařízení, jenž slouží pro pohyb a ovládání analogovým kamer. Samozřejmě standardem je rozhraní pro TCP/IP sítě. DVR má dvě podstatné funkce jednou je digitalizace obrazu a druhá integrace analogovým kamer do Ethernetových sítí. DVR vlastní webové rozhraní pro nastavení provozu DVR. Komunikace se nastavuje pomocí externího PC připojeného pomocí UTP kabelu Cat. 5E přímo k DVR. Pakliže DVR vlastní webové rozhraní automaticky by měla mít tovární IP adresu pro snadnost a dostupnost při připojení externího PC. Následně stačí pro PC nastavit IP adresu o číslo menší nebo větší dle rozsahu a už by měla komunikace fungovat. K tomu by měl existovat i SW pro právě nastavení DVR. Pomocí UTB kabelu Cat. 5E se DVR připojí do LAN sítě. Uvnitř sítě se nachází řada dalších IP zařízení a počítačů. V případě přístupu stačí DVR nastavit buď veřejnou IP adresu nebo vnitřní pevnou IP adresu. Záleží pro jaký účel a komu chceme DVR se záznamem případně kamery zpřístupnit. Obě varianty jsou reálné. Ovšem bezpečnější je opět dle možností využít VPN službu. Pak s PC, kde je připojení k Internetu s patřičnou rychlostí stačí mít nainstalovaného klienta VPN nebo znát pouze IP adresu, kterou je potřeba zadat do webového prohlížeče a můžeme se dostat na webové rozhraní pro konfiguraci DVR nebo pomocí speciálního SW, kde vyplníme spojení k DVR si prohlížet aktuální dění či záznam z kamer.

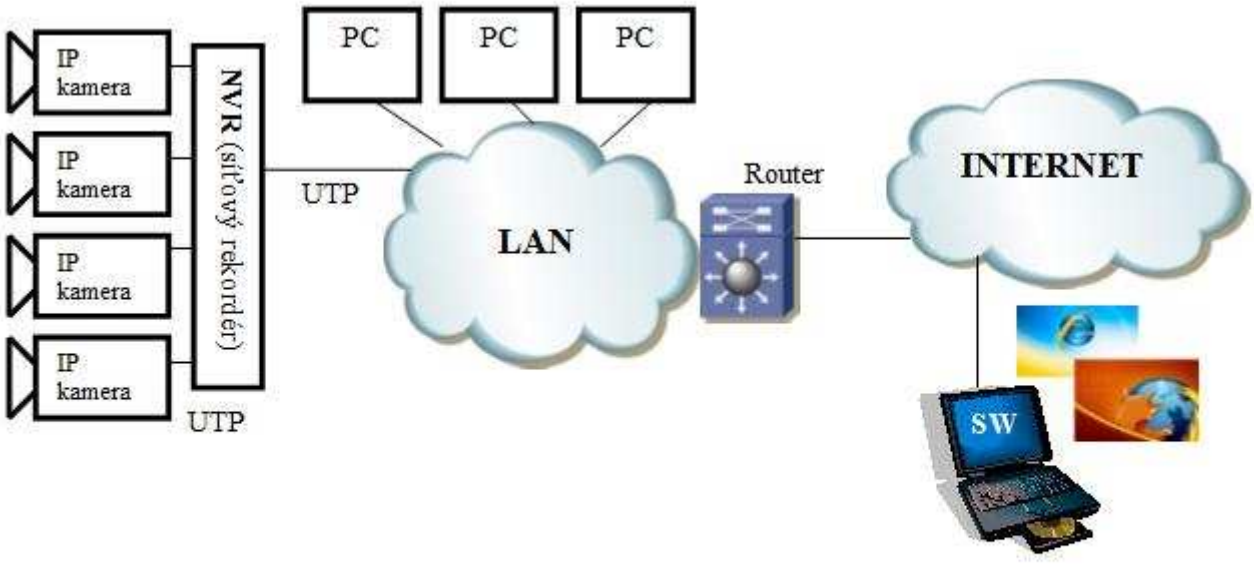
11.2 Schéma vzdáleného přístupu k analogovým kamerám pomocí Video serverů



Další možností, jak zpřístupnit kamerové systémy založená na analogovém principu do Internetu se nachází v relativně nové podobě zařízení, který se nazývá Video server (enkodér). Ten má své webové rozhraní jako DVR. Akorát většinou se setkáme s Video servery s jedním vstupem, takže připojíme maximálně jednu kameru k jednomu video serveru. Video server tedy obsahuje i programovatelné vstupy a výstupy pro další možnosti jako funkce PTZ či připojení detektoru. Kamera připojená k Video serveru obsahuje IP adresu, která odpovídá jedné analogové kameře. Jestliže je požadován záznam z těchto kamer, stačí přidat NVR zařízení. Na vstupy NVR se přivedou jednotlivé video servery, které přebírají za analogové kamery Ethernetovou inteligenci. NVR je umístěn v síti LAN. Připojení k Internetu většinou ve firmách jsou na velké úrovni v oblasti rychlosti, proto nebude se zobrazováním takový problém jako například u kamerových systémů u RD. Pro zobrazení z analogových kamer na libovolnou vzdálenost pomocí Ethernetu na určitém

monitorovacím stanovišti s klasickými analogovými monitory je možné. Existují tzv. Video dekodéry. Ty plní funkci převodu Ethernetového datového paketu na signál odpovídající analogovému signálu, jenž se přivádí na video přepínač a ten zajistí rozdělení na příslušný monitor. Jsou tedy pryč časy, kdy analogové systémy nebylo možné uplatnit na vzdálený monitoring. Otázkou však zůstává, jestliže se jednou analogový signál digitalizuje v video serveru a posílá přes Ethernet, zda následné dekódování obrazového signálu na analogový nezpůsobí zhoršení kvality obrazu. Ovšem to je věc pro odborníky. Během zjišťování informaci jsem se setkal i s názorem, že takto je to skutečně reálně zapojení,ale v praxi, co do kvality obrazu už nemá tento systém takový efekt.

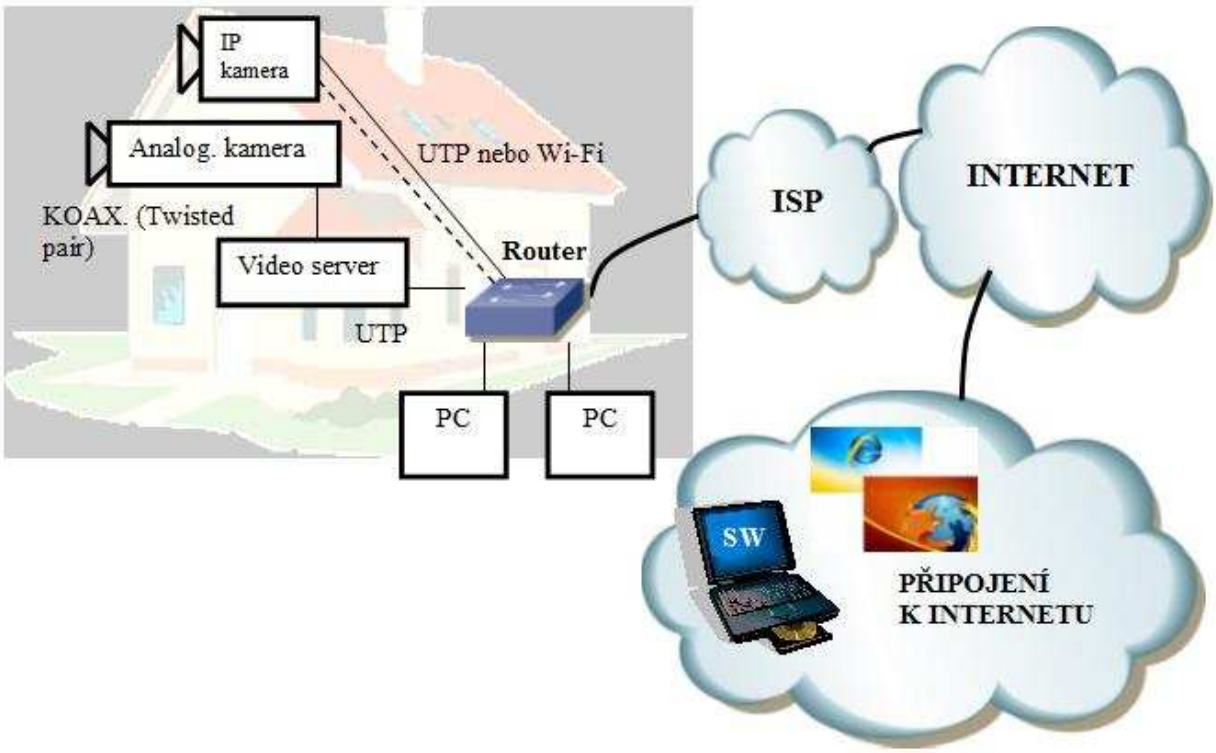
11.3 Schéma vzdáleného přístupu k digitálním IP kamerám



Byť rozšířenou, ale zatím nedostačující technikou, která nabírá rychlý vzestup jsou kamerové systémy založeny na IP technologiích. Na schématu si můžeme všimnout, že již není potřeba žádné převodníky do Ethernetového rozraní. Vše řeší digitální kamery s TCP/IP komunikací sama. Při potřebě záznamu z kamer se řeší rovněž pomocí NVR se speciálně uzpůsobený HW a SW pro potřebu záznamu. Pomocí výstupu z NVR se připojí toto zařízení do aktivního prvku sítě a odtud už nic nebrání vzdálené správě. Jednotlivé IP kamery mohou mít nastavenou svou IP adresu a proto je možno přistoupit odkudkoli přímo

k jednotlivým kamerám nebo pokud nechceme sledovat aktuální dění před IP kamerami, pak stačí znát IP adresu NVR zařízení a pomocí SW můžeme nahlížet vzdáleně do záznamu. Vše se odehrává na směrování a konstrukci LAN sítí a Internetu. Podstatnou věcí je ovšem rychlost, aby především monitoring v čase byl plynulý je doporučená rychlost pro odesílání dat do sítě, kde je IP kamera umístěna na 512 kbps. Základem vzdáleného přístupu k IP kamerám či záznamu z nich je relativně rychlé připojení k Internetu, znalost IP adresace, správné nastavení IP kamer případně NVR a SW pro aplikace.

11.4 Schéma vzdáleného přístupu k digitální kameře IP instalované v rodinném domě



Dnešní síťové kamerové systémy se instalují nejen do firemních sítí, ale rozmáhají se instalace i do rodinných domů, kde tyto kamerové systémy mají své oprávněné místo. Jak již bylo zmíněno výhodou je jednoduchost propojení do celosvětové sítě Internet a tím pádem i možnost vzdáleně z libovolného počítače, si prohlížet a monitorovat situaci doma.

Pro instalaci do rodinného domu je podstatné vybrat vhodnou kameru a především mít v rodinném domě připojení k Internetu. Jelikož chceme monitorovat vzdáleně oblast pře kamerou, pak záleží na uploadu, tedy na rychlosti Internetu směrem do Internetu. Doporučená minimální rychlost pro upload u kamer je 512 kbps.

V RD jsou instalace daleko méně náročně svou strukturou než u firem. V podstatě stačí mít speciální router se směrováním do WAN sítě. Router obsahuje vstupy pro UTP kabel s RJ-45 konektorem nebo je možnost i přenos Wi-Fi. Router rovněž obsahuje webové rozraní s dvěmi rozhraními. Jedno je pro lokální síť, kde pomocí PC a zadání IP adresy do webového prohlížeče se dostaneme do webového rozhraní, kde se provádí přiřazení IP adresy buď dle služby DHCP (automaticky), pevné nastavení IP adresy nebo lze nastavit i IP adresaci dle VPN služby (dle možností routeru). Druhé rozhraní už se tváří jako Internetové s možností tzv. Internetového surfování.

IP kamery nebo analogové pomocí Video serveru přivedeme do routeru na jednotlivé vstupy (pro UTP kabel s kontektorem RJ-45. Pro vzdálené sledování kamer umístěných v RD se musí provést nastavení IP adresace. Jelikož se jedná o náš majetek a chceme ho sledovat zabezpečeně v rámci pouze přihlašovacího jména a hesla, pak stačí od ISP si vyžádat veřejnou pevnou IP adresu (za poplatek) a tu přiřadit požadované kameře. U kamer se také připojí PC přímo kříženým kabelem ke kameře a pomoci SW dodávaného běžně ke kameře se provede nastavení. Na PC nastavíme IP adresu blízko rozsahu IP adres kamery. Nyní může začít s nastavováním a to vše prostřednictvím SW pro kameru. Nesmíme zapomenou na přihlašovací jméno a heslo správce, které je nutné nastavit pro větší bezpečnost. Následně odpojíme od IP kamery PC a připojíme kameru do routeru. Pro ověření správnosti nastavení poslouží PC zapojený rovněž do routeru v rámci domácí sítě. V tom případě využijeme webového prohlížeče a napíšeme IP adresu veřejnou, kterou jsme kameře nastavili od ISP (za poplatek). Pak bychom se měli dostat na webové rozhraní kamery. Přes webové rozhraní konfigurujeme kameru a to vždy správce kamery, jenž řeší celkově nastavení a monitoring. Samozřejmostí u těchto kamer je nastavení uživatelů dle typu kamery. Najednou může dění sledovat i 10 pověřených osob s omezenými právy. Můžeme zaznamenávat obrázky jednotlivě nebo jestliže obsahuje kamera pohybový detektor lze nastavit scény pro detekci pohybu a následně při poplachu posílat na E-mail nebo FTP server obrázky. Samozřejmosti jsou další možnosti dle výrobce kamery. To už bude řešit technik přímo se zákazníkem. I pro domácí použití doporučuje v rámci možnosti

routeru použít VPN službu routeru. V tomto případě necháme nastavení provádět zkušeného uživatele, který sítím rozumí. Opět bude potřeba nainstalovat na PC VPN klienta a vyplnit údaje o zabezpečeném spojení a zkusit se připojit, ovšem mimo místo instalace kamery neboť připojit se přes VPN službu a klienta přímo v dané lokální síti není možné, neboť VPN vytváří šifrovanou cestu mezi dvěmi sítěmi nikoliv v rámci lokální sítě.

II. PRAKTICKÁ ČÁST

12 ÚKOLY PRO REALIZACI A ZPŘÍSTUPNĚNÍ IP KAMERY PRO VZDÁLENÝ PŘÍSTUP PŘES TCP/IP (LAN) SÍŤ A INTERNET

Čím dál častěji se nejen na Internetových obchodech, ale i přímo u firem nabízí moduly či komunikátory pro připojení určitého zařízení do počítačové sítě. Proto se zařízení záhy stane síťovým zařízením a může využívat všechny výhody komunikace přes počítačovou síť. V souvislosti s výhody jsou rovněž u těchto technologií řada úskalí, které se vyznačují zranitelností systému a odhalení od počítačových hackrů. Proto přenos dat a celý systém by měl obsahovat řadu zabezpečovacích možností. V dané síti existují brány firewall, šifrování a řada dalších užitečných pomocníků proti ochraně dat. Pro realizaci vzdáleného přístupu byla vybrána bezpečnostní technologie CCTV a síťová kamera **Vivotek PT 7135**, která bude umístěna v síti UTB ve Zlíně.

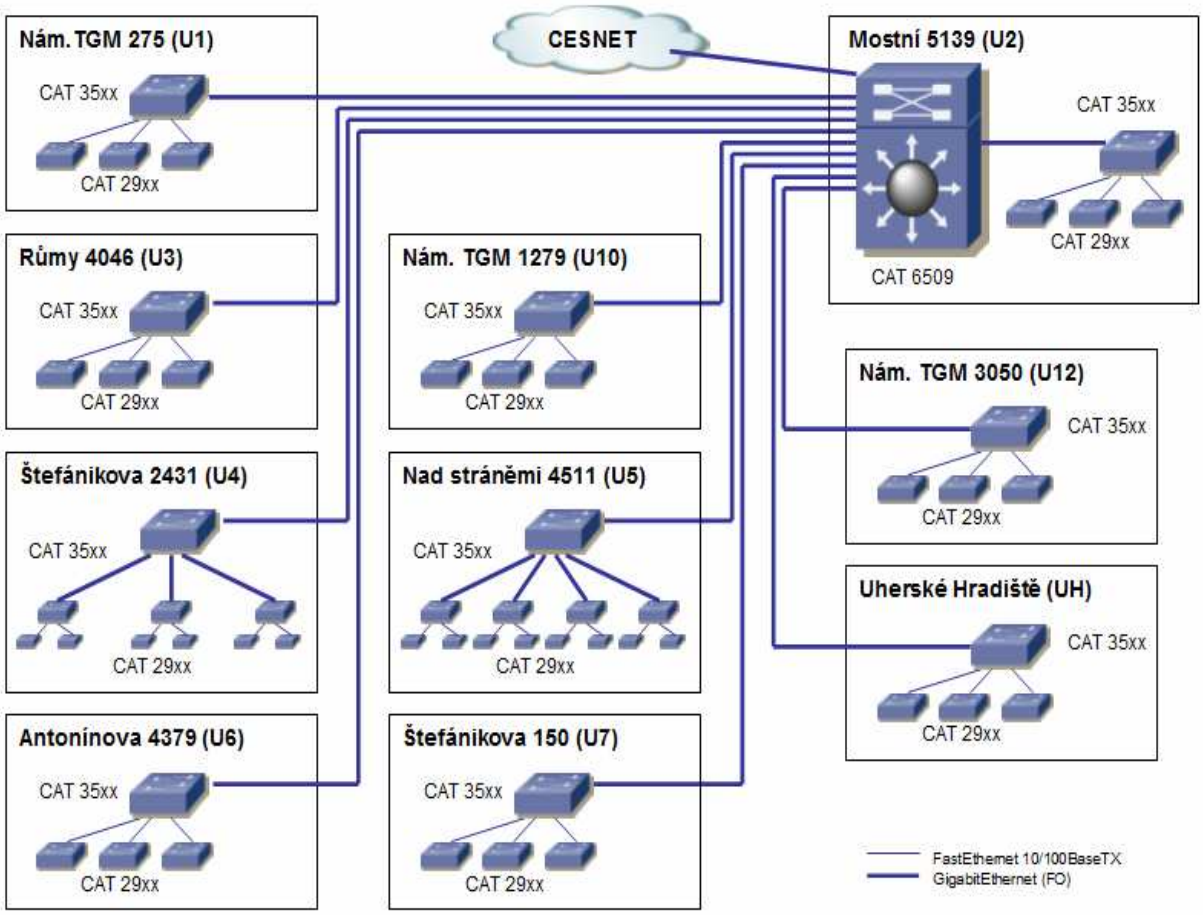
Pro připojení IP kamery značky Vivotek PT 7135, která byla vybrána pro realizaci vzdáleného přístupu v oblasti bezpečnostních technologií, ale i u jiných kamer se musí dbát na tyto základní otázky:

1. CO budeme chtít monitorovat – musíme jasně specifikovat o jaký objekt se jedná, co se v něm nachází a co je potřeba střežit či monitorovat.
2. JAK to budeme chtít monitorovat – musíme předem stanovit a vymezit, zda se bude jednat o střežený prostor, kde bude vyžadováno střežení během dne či v noci, nebo zda bude objekt monitorován 24h denně.
3. KDE to budeme chtít monitorovat – musíme stanovit a vymezit, zda střežená plocha se bude nacházet vevnitř v objektu nebo se bude jednat o střežení perimetre objektu.

Tyto údaje při projektování tohoto systému jsou důležitou součástí, neboť tato vymezení stanoví a určí druh kamery pro použití v daném objektu. Samozřejmě v rámci komplexního řešení stanoví i více druhů kamer pro jednotlivé prostředí, ve kterých budou použity.

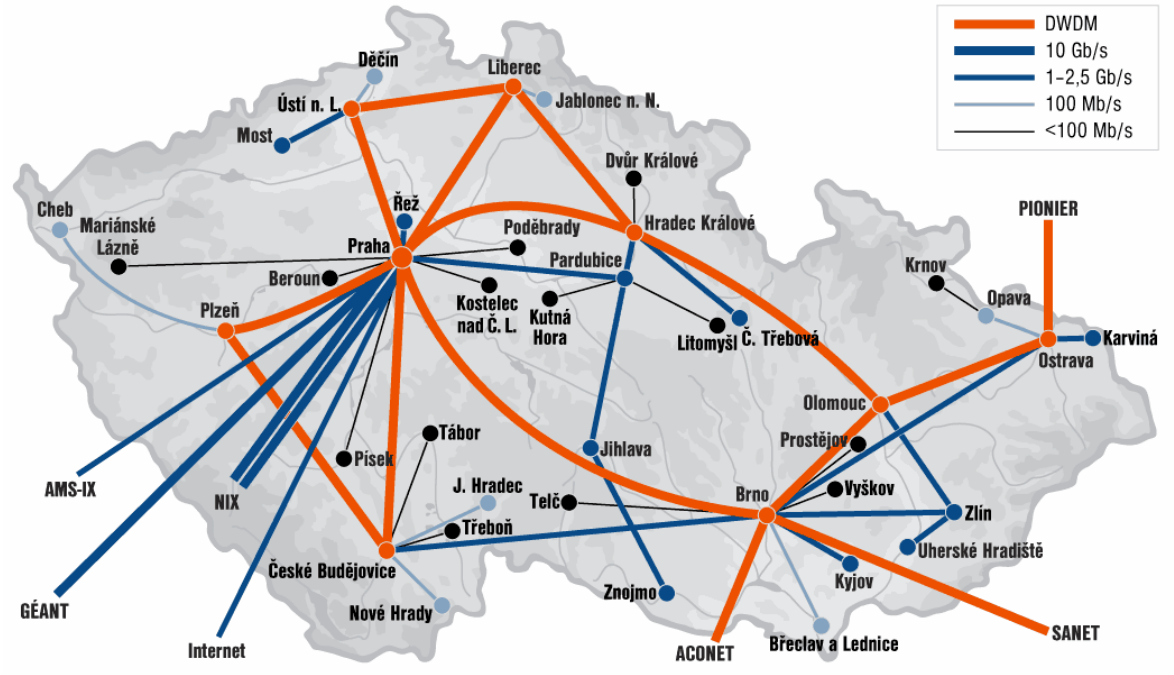
Pakliže dodržíme tyto obecné zásady, pak můžeme přejít k samotnému umístění, zapojení a nastavení kamery. V další kapitole bude ve zkratce rozebrána síť, ve které bude kamera umístěna, způsoby zpřístupnění kamery pro vzdálený přístup, technické parametry kamery, instalace kamery, nastavení kamery a v závěru předvedena ukázka.

13 INFORMACE O POČÍTAČOVÉ SÍTI UTB VE ZLÍNĚ



Obr. 27 Blokové schéma IP sítě a aktivních prvků

Jedná se o rozsáhlou počítačovou síť, kde základem je výkonný Router umístěn na jedné z budov (označen jako U2). Od ní je v hvězdicové struktuře sítě rozveden optickým vláknem rozvodná datová síť k ostatním budovám UTB ve Zlíně. Jedná se o objekty a budovy označené jako U1, U3, U4, U5, U6, U7, U10, U12, UH (umístěná cca 40 Km od Zlína). Propojení mezi budovy je zajišťováno pomocí optiky. Jednotlivé servery na jednotlivých budovách mají pod sebou páteřní switche dle počtu serverů a pod nimi lze naleznout ještě pod-switche na které jsou napojeny počítače a jiná zařízení. Celá sít je založena na technologiích CISCO Catalyst. V celé síti může naleznout až 2200 počítačů. Internetový poskytovatelem je CESNET. UTB ve Zlíně využívá síť CESNET 2. Její rozsáhlost a jednotlivou rychlost je možné vidět na obr. 28.



Obr. 28 Síť CESNET 2 a její rozsáhlost

14 TECHNICKÉ PARAMETRY KAMERY VIVOTEK PT 7135

Obecné vlastnosti

- přístup pomocí mobilních telefonů 2,5 a 3G
- otáčení 350° a naklápění 135°
- přístup pomocí internetového prohlížeče Microsoft Internet Explorer
- video v reálném čase, nastavení rozlišení a kvality
- přenos, případně záznam zvuku pomocí zabudovaného mikrofonu
- SW detektor pohybu ve třech nezávislých oknech
- SDK kit pro vývoj vlastních aplikací a integraci do WWW stránek
- Procesor Vivotek VVTK 1000
- RAM: 32MB SDRAM
- ROM: 4MB FLASH ROM

Síť

- automaticky přepínaný 10/100BaseT Ethernet
- protokoly TCP/IP, HTTP, SMTP, FTP, DDNS, UPnP, Telnet, NTP, DNS, DHCP, RTSP

Pohyb

- otáčením 350°
- naklápění 135°
- ovládání pomocí webového rozhraní, dodávané aplikace nebo mobilu

Video

- komprese videa MPEG4
- barevný snímací prvek CMOS 1/4“, citlivost 1,5Lux/F2,0
- až 25 snímků/s o rozlišení 640x480, 320x240 nebo 160x120 bodů
- AGC, AWB, AES, elektronická uzávěrka 1/60 až 1/15000s
- špičkový obraz i za velmi nepříznivých světelných podmínek

Audio

- komprese audia GSM-AMR/MPEG4 AAC

- audio 24kb/s
- zabudovaný všesměrový mikrofon

Napájení

- stejnosměrné 12V
- spotřeba asi 7W

Rozměry a hmotnost

- rozměry D100mm×Š110mm×V120mm
- hmotnost 270g

Obsah balení

- kamera s fixním objektivem 4,0mm, napájecí adaptér, adaptér pro montáž na zeď, CD se SW ST3402 pro záznam/přehrávání až 16 kamer/video serverů Vivotek řad 3xxx, 6xxx a 7xxx

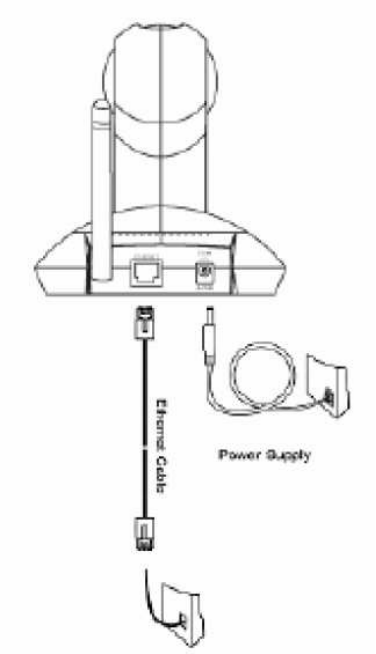
Obr. 29 IP kamera značky Vivotek PT 7135

15 PRVOTNÍ NASTAVENÍ IP KAMERY A PŘÍSTUP

Jde o nastavení IP kamery dané značky tak, aby byla tato IP kamera použitelná pro realizaci vzdáleného přístupu jak z vnitřní sítě LAN UTB, tak vzdáleně přes Internet.

15.1 Umístění IP kamery Vivotek PT 7135

Kamery Vivotek PT 7135 byla po dohodě s vedoucím práce umístěná v laboratoři číslo 309/54 v budově s označením U5 na Jižních Svazích. Kamera by měla monitorovat celou laboratoř a případně vyzkoušet její dovednosti respektive vyzkoušet, co kamera dokáže nabídnout za funkce.

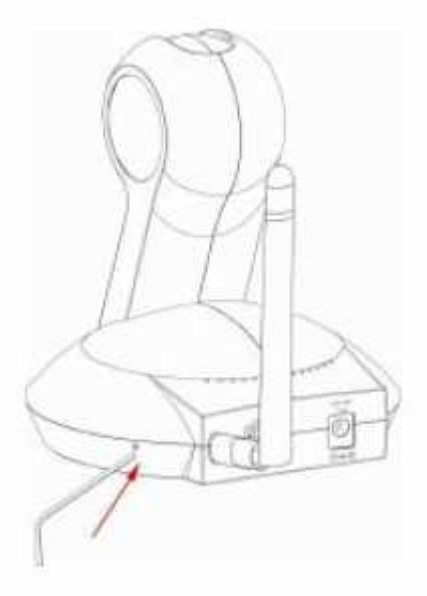


Obr. 30 Zadní strana IP kamery Vivotek PT 7135

Pro připojení IP kamery k počítači nebo do aktivní síťového prvku (switch) se používá Ethernet kabel kategorie UTP Cat. 5E, kde jeho délka by neměla přesáhnout 100m. Nejprve připojíme konektor napájecího zdroje do kamery a až pak připojíme adaptér do napájecí zásuvky. Vyhneme se poškození kamery v důsledku přepěťovým pulsem, který se může objevit. Jestliže připojíme IP kameru ke zdroji napětí, pak můžeme začít s nastavováním IP kamery (viz kapitola 3.6).

15.2 Přiřazení IP adresy pro kameru Vivotek PT 7135

Kamera má na výstupu speciální port pro konektor RJ-45. Tento port vytváří rozhraní pro kteroukoliv počítačovou sít (LAN) nebo umožňuje připojit kameru přímo k počítači nebo notebooku. Přímé připojení k počítači nebo notebooku se využívá jen tehdy, jestliže se požaduje kameře přiřadit pevnou IP adresu (na základě konzultace se správcem sítě v dané počítačové síti).



Obr. 31 Resetovací tlačítko IP kamery

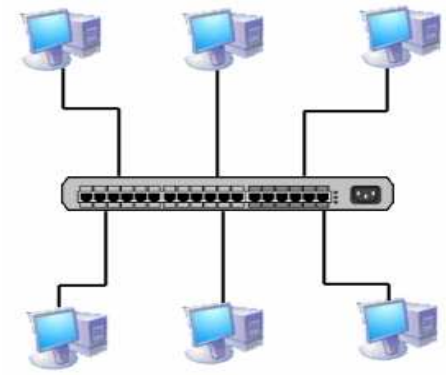
Kamera Vivotek 7135 se před uvedením do sítě doporučuje „resetovat“ do továrního nastavení. Provádí se resetovacím tlačítkem z boku kamery (viz obr. 31). Přiložením patřičného předmětu a podržením až do doby než se rychle rozblikají všechny LED diody (červená, modrá, zelená), pak dojde k obnovení továrního nastavení. Provádí se tehdy, když je potřeba změnit IP adresu nebo by se zapomnělo heslo pro přístup ze strany správce ke kameře.

Tovární IP adresa kamery Vivotek 7135 je 192.168.0.99.

Obr. 32 Přímé spojení IP kamery s počítačem

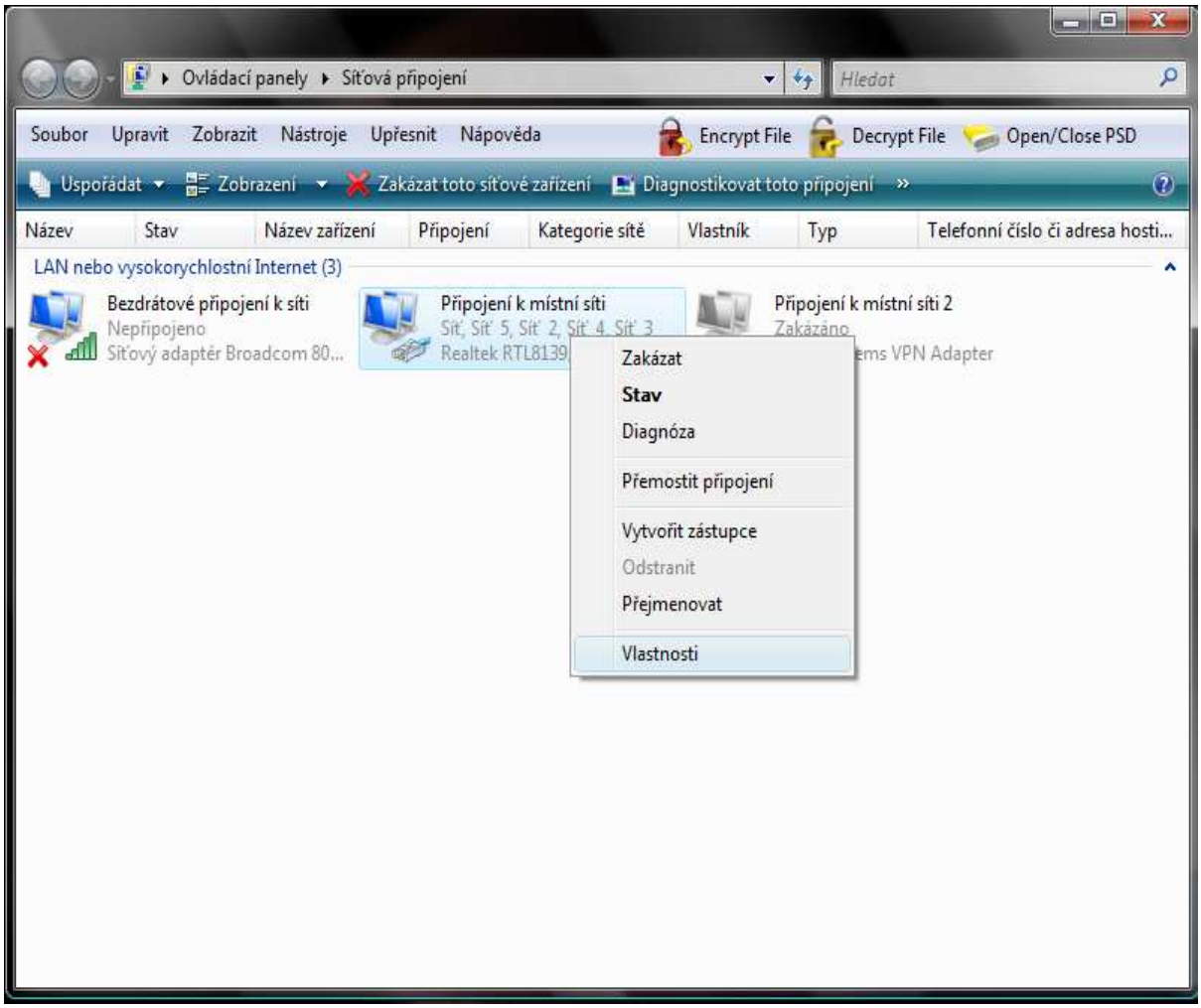
Pro připojení k jakékoliv počítačové síti je potřeba po konzultaci se správcem sítě přiřadit kameře danou IP adresu. Než se tak stane je potřebné zapojit IP kameru s počítačem (i notebookem) pomocí kříženého kabelu UTP Cat. 5E (viz obr. 32). Ten se používá pakliže se připojují mezi sebou dvě PC nebo dvě zařízení PC a kamera. Přímý kabel se používá pro připojení k HUBu nebo switchi (viz obr. 33 a obr. 34).

Obr. 33 Připojení křiženým kabelem mezi dvěmi PC



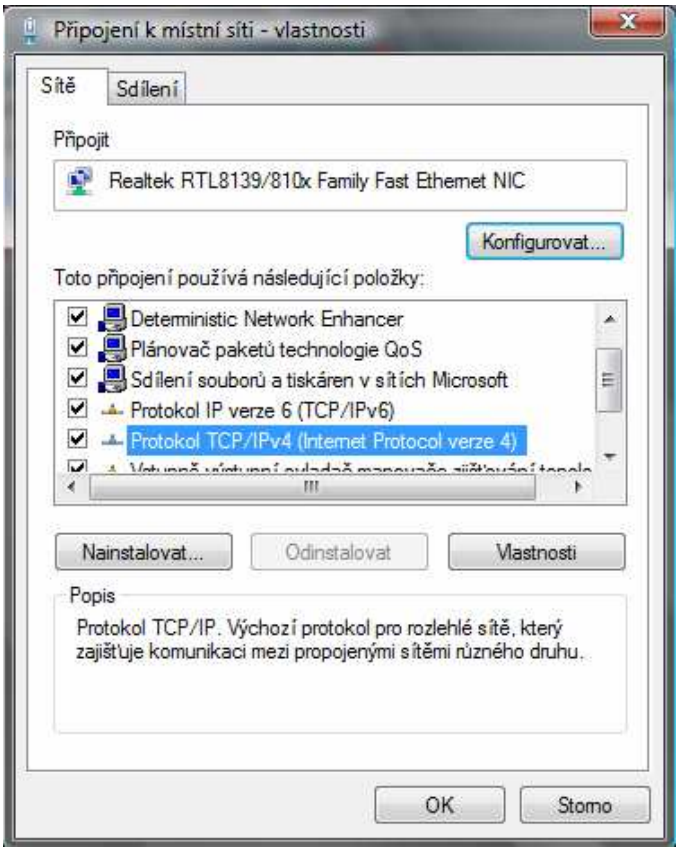
Obr. 34 Připojení přímým kabelem ke switchi

Pakliže jsem spojili správným kabelem počítač (i notebook) s kamerou, můžeme přejít k softwarovému nastavení počítače (i notebooku), tak aby bylo možné se spojit s kamerou. Proto je důležité otevřít „Ovládací panely“ a v „Síťovém připojení“ kliknout na „Vlastnosti dané sítě“ (viz obr. 35).



Obr. 35 Okno „Síťového připojení“

Po kliknutí se objeví okno „Připojení k místní síti“, můžeme najet na položku „TCP/IPv4“ a na „Vlastnosti“ této položky „TCP/IPv4“ (viz obr. 36).

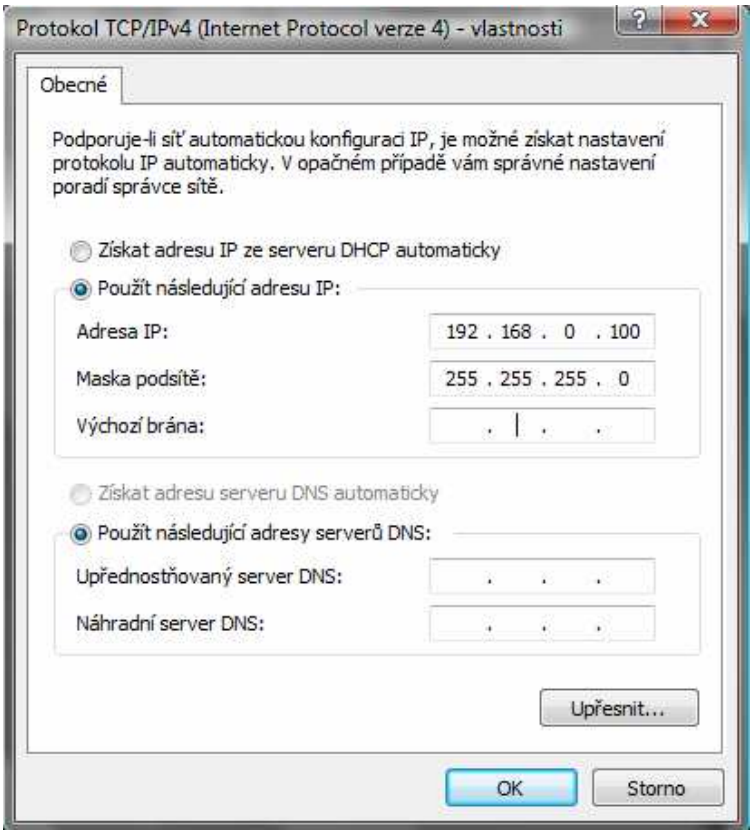


Obr. 36 Okno pro „Pro připojení k místní síti“

V následující tabulce (viz obr. 37) je potřeba zadat počítači (nebo notebooku) IP adresu. IP adresu volíme z intervalu IP kamery (dle tovární IP adresy). Nikdy nemůžeme přiřadit kameře stejnou IP adresu jako kamera, pak by komunikace nebyla zajištěna a nastavení by nemohlo probíhat. Došlo by ke kolizi při datovém přenosu.

Proto IP adresa počítače (i notebooku) se volí ve většině případů stejná jako IP kamera s výjimkou, že na konci přidáme např. o jedničku více. Tedy IP adresa počítače (nebo notebooku) pro komunikaci s kamerou nastavíme např. na 192.168.0.100. Následně potvrdíme „OK“.

Pak spustíme již nainstalovaný software ke kameře Vivotek PT 7135. V našem případě se jedná o software s názvem **Install Wizard**.



Obr. 37 „Vlastnosti“ protokolu IPv4

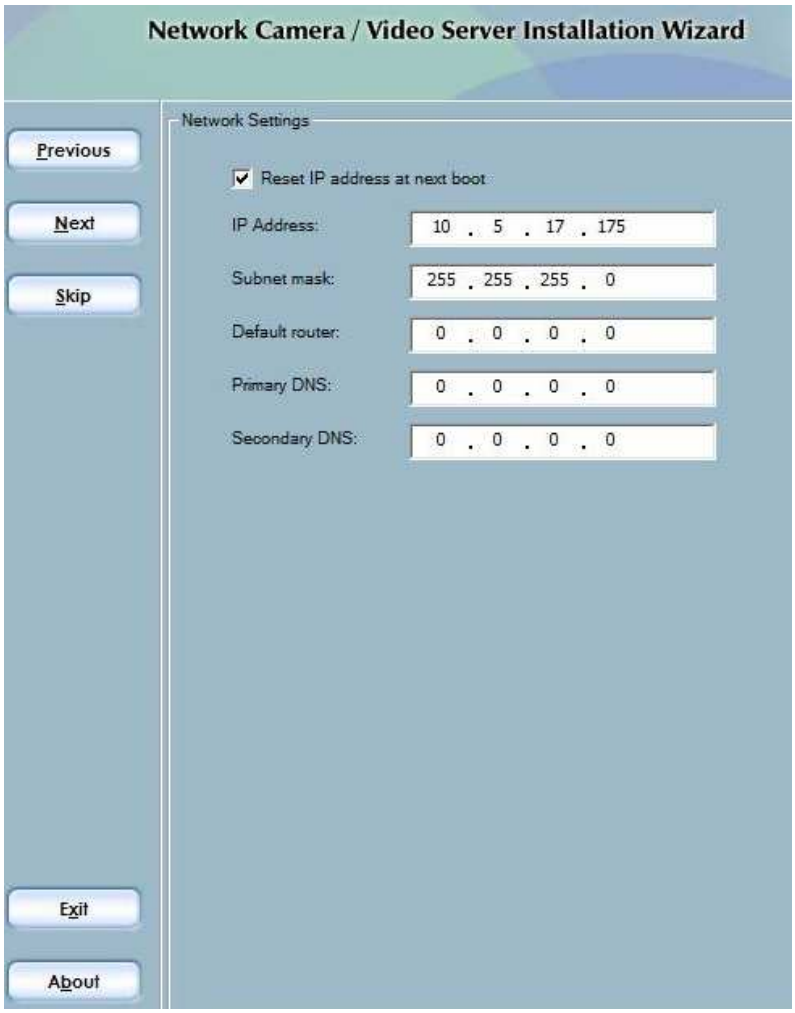
Od 30 sekund do 3 minut by kamera měla být softwarem zjištěna a my můžeme provádět nastavení – „Setup“ kamery (viz obr. 38). Zde můžeme nastavovat detailní konfiguraci pro příslušnou počítačovou síť.

Kamera umožňuje funkci automaticky resetovat IP adresu při každém spouštění (doporučení je nezatrhávat). V následující tabulce můžeme doplnit potřebné nastavení tak, aby kamera byla nastavena pro následující počítačovou síť, kde bude vykonávat funkci monitoringu.

V dialogovém okně je možnost nastaveni heslo pro správce kamery, které bude sloužit pro přístup ke kameře a její konfiguraci.

Pak můžeme přejít k přidělení vnitřní IP adresy, která po dohodě se správcem sítě je 10.5.17.175. Maska sítě se nastaví na 255.255.252.0. Adresa standardního routeru se nastaví na 10.5.16.1. Primární DNS server má adresu 195.178.88.66. Po dokončení tohoto nastavení stačí kliknout na „Apply“ a odpojit UTP kabel (křížený) od IP kamery.

Kdybychom nechali kabel propojený s IP kamerou, přestal by počítač (nebo notebook) s kamerou spolupracovat z důvodů jiného rozsahu IP adres.



Obr. 38 „Setup" kamery v programu Install Wizard

15.3 Vzdálený přístup k IP kameře ze sítě LAN

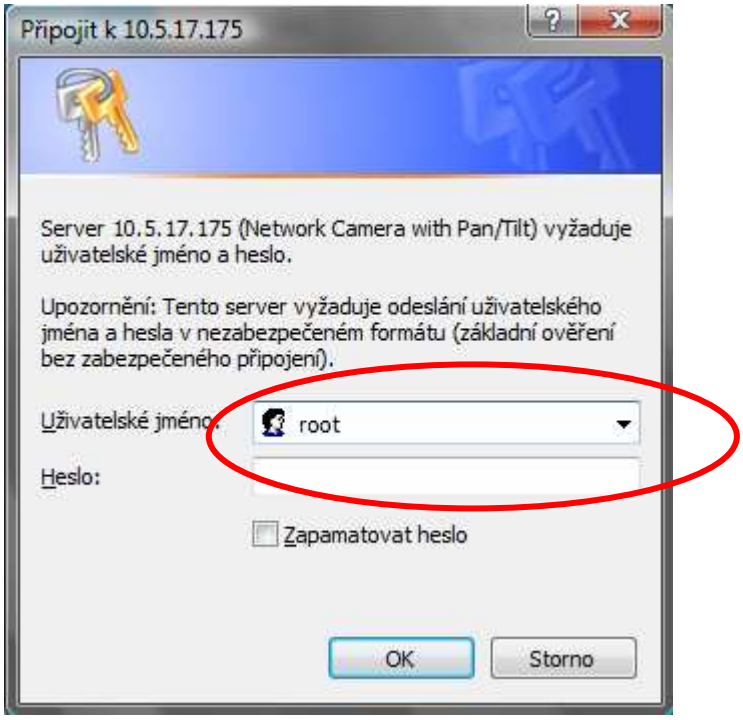
Následně připojíme IP kameru kříženým (i přímým) kabelem do aktivního prvku sítě (switch). Jestliže jsme zapojili správně, pak by z kteréhokoliv místa ze sítě LAN (jedno jaký PC umístěný v síti) bychom se měli dostat k IP kameře Vivotek.

A to tak, že otevřeme prohlížeč Internet Explorer a zadáme vnitřní IP adresu kamery (viz obr. 39), tedy 10.5.17.175. Dojde k otevření webového rozraní kamery Vivotek. Jen za předpokladu, že se k webovému rozhraní IP kamery dostáváme z vnitřní LAN sítě, kde je umístěná IP kamera. Jestliže se připojujeme poprvé k IP kameře, pak nám prohlížeč

(Internet Explorer) nabídne instalaci zásuvného modulu (tzv. plug-in). Tento modul je potřebný pro plynulé zobrazení videa v prohlížeči.

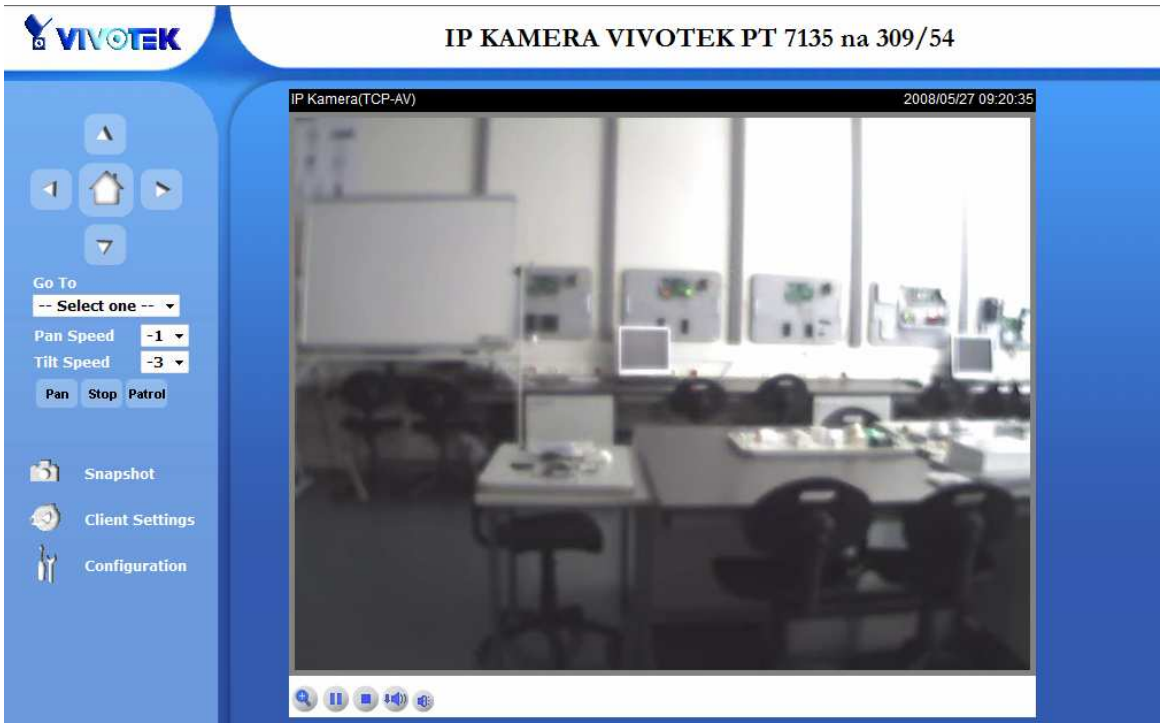
Obr. 39 IE a zadání adresy IP kamery

A následné se zobrazí přihlašovací okno (viz obr. 40). Pokud správce kamery nenastaví jinak, je přihlašovacím jménem slovo „root“ a heslo nastavené dle správce kamery.



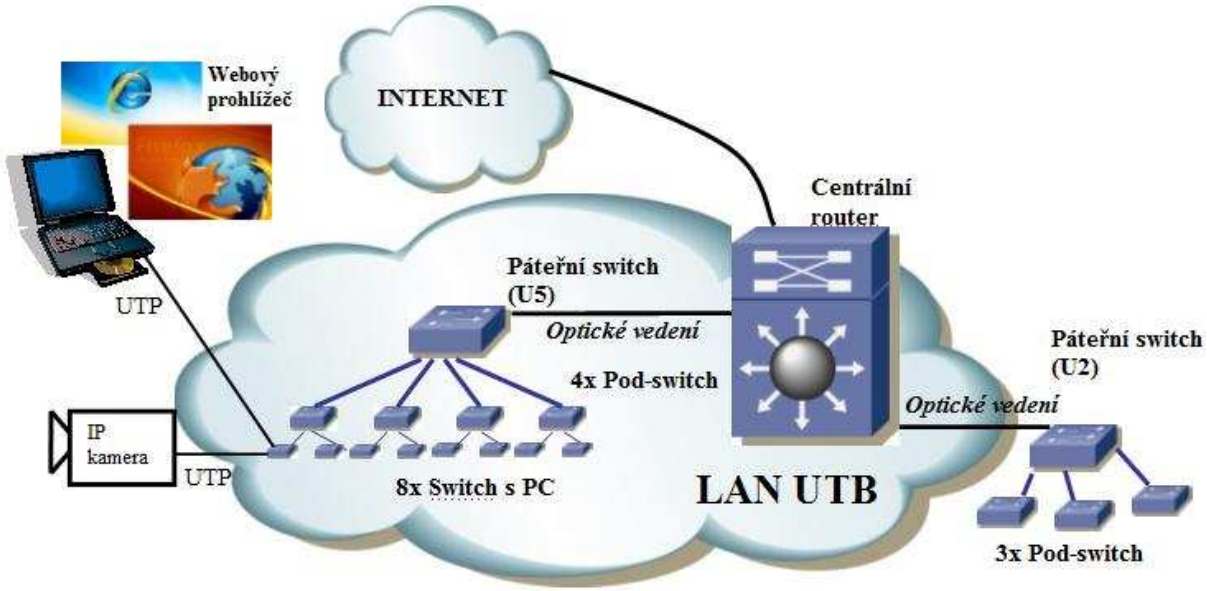
Obr. 40 Okno s přihlašovacími údaji

Následně už se zobrazí webové rozhraní IP kamery (viz obr. 41), kde je možno provádět kompletní správu IP kamery.



Obr. 41 Webové rozhraní IP kamery Vivotek

15.3.1 Schéma vzdáleného přístupu k IP kameře z podnikové sítě LAN



Obr. 42 Schéma vzdáleného přístupu k IP kameře přes síť LAN

Tento přístup je po připojení IP kamery do počítačové sítě LAN UTB ve Zlíně nejednodušší. Pakliže jsme na kterémkoli počítači (v síti jich je téměř 2200 PC), pak nám

k vzdálenému přístupu stačí pouze na počítači mít prohlížeč Internet Explorer a znalost IP adresy kamery (tedy 10.5.17.175).

15.4 Způsoby zpřístupnění IP kamery v síti LAN UTB ve Zlíně pro vzdálený přístup

Možnosti vzdáleného přístupu k síťovým kamerám se obecně odvíjí od sítě, ve které mají být zapojeny. Pro síť UTB ve Zlíně jsou tyto možnosti, jak se k zařízení připojit:

1. **Privátní pevná IP adresou (připojení přes VPN server a klienta)**
2. **Veřejnou pevná IP adresou**

Rozsah vnitřních IP adres podle modelu RFC 1918 jsou pro síť LAN UTB:

- 192.168.X.X
- 172.16.X.X – 172.31.X.X
- 10.X.X.X

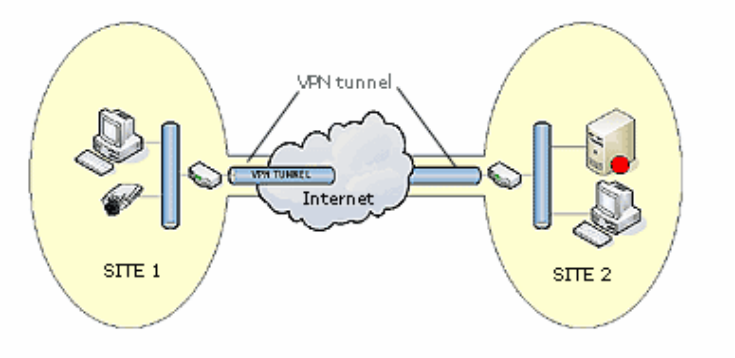
15.4.1 Výhody a nevýhody připojení přes VPN server

Výhody jsou:

- Šifrovaný datový přenos (IPsec)
- Možnost zabezpečeného přístupu do vnitropodnikové sítě z Internetu

Nevýhody jsou:

- Nejsou známy



Obr. 43 VPN tunel

15.4.1.1 IPsec (IPsecurity)

Je založen na vytvoření šifrovaného tunelu mezi dvěma koncovými zařízeními, které mohou představovat např. směrovač, firewall nebo koncovou stanici. Tento standard definuje nejen samotné šifrování, ale i standardní metody pro výměnu a správu klíčů.

Šifrované spojení zajišťuje následující vlastnosti:

- utajení (data jsou šifrována);
- integritu (přijímací strana ověřuje, zda nedošlo během přenosu k manipulaci s daty);
- ověření pravosti zdroje;
- anti-replay (přijímací strana rozpozná a odmítne opakované zasílání paketu – jedná se o případnou obranu proti replay útokům).

Před vytvořením šifrovaného tunelu je potřeba dohodnout parametry spojení:

1. šifrovací algoritmus (DES, 3DES);
2. hašovací funkci (MD5, SHA);
3. metodu autentikace;
4. dobu životnosti. [8]

15.4.2 Výhody a nevýhody Veřejných IP

Výhody jsou:

- přímá dostupnost počítače z venku z Internetu, například z práce, od kamarádů, a jiné
- možnost provozování veřejných serverových služeb, např. webové stránky, FTP, SSH
- přímá komunikace některých programů - například přenosy souborů přes ICQ
- vyžadováno některými síťovými hrami

Nevýhody jsou:

- nižší ochrana proti virům a útokům hackerů - každý si musí řešit sám
- ztráta anonymity - je jasné, kdo kam přistupuje
- riziko pro nezkušené uživatele

15.4.3 Výhody a nevýhody Privátních IP Adres

Výhody jsou:

- schovaná sít a je více chráněná před útoky zvenčí
- zbytečně se neplýtvá veřejnými IP adresami (IP adresy IPv4 je omezené počtem a je jich nedostatek)
- stejné adresy se lze používat v opakovaně v různých lokálních sítí (šetření veřejných).

Nevýhody jsou:

- provozovat službu NAT na Proxy serveru nebo routeru

Po dohodě se správcem sítě bylo navrženo, že k IP kameře Vivotek PT 7135 bude přistoupeno vzdáleně z jiného místa (přes Internet) přes VPN server a privátní IP adresu. Proto bude nutností na daném počítači, ze kterého se bude připojovat k IP kameře, instalace VPN klienta. Po vyplnění bezpečnostních údajů bude vytvořen šifrovaný tunel pomocí protokolu IP Security přímo do sítě UTB a po zadaní IP adresy zařízení do prohlížeče Internet Explorer bude ke kameře přistoupeno. Vycházelo se z předpokladu, že kamera je určena pro jednoho studenta a proto nebylo žádoucí přiřazovat veřejnou IP

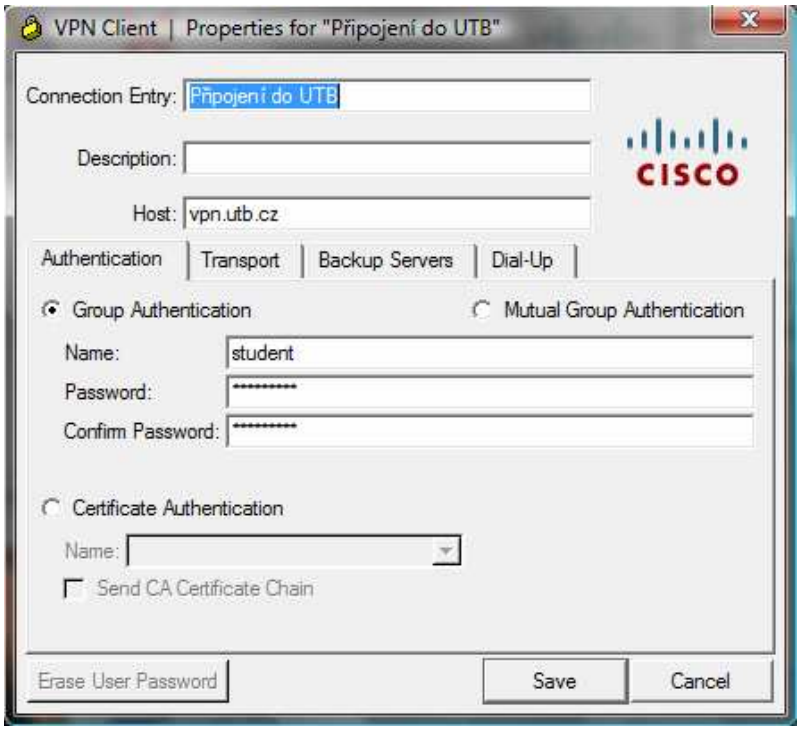
adresu. Tím by byl přístup ke kameře zajištěn komukoliv kdo zná IP adresu. A přenos by nebyl zabezpečen ani šifrován.

15.5 Vzdálený přístup k IP kameře přes Internet (přes server VPN)

Nejprve se musí na počítači (nebo notebooku) nainstalovat VPN klient. V mém případě jsem nainstaloval klienta od společnosti CISCO.

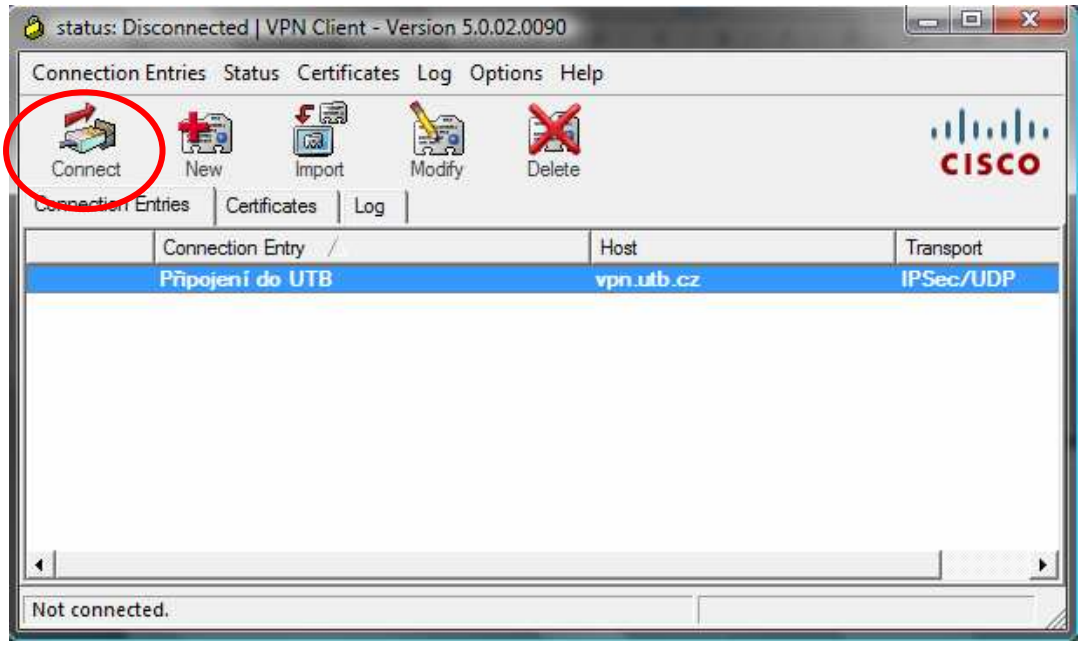
Pro počítačovou síť, do které se chci vzdáleně připojit, musím získat od správce sítě přihlašovací údaje a heslo pro VPN server. Na základě těchto získaných informací, se pak můžu z libovolného místa na Zemi, kde je počítač (nebo notebook) připojený do sítě Internet jednoduše připojit k IP kameře.

1) Otevřu VPN klienta a vytvořím nové VPN připojení (viz obr. 44). Do pole „Connection Entry“ vložím libovolný text. Do pole „Host“ zadám doménu od VPN serveru (v našem případě vpn.utb.cz), který zajistí připojení do vnitřní sítě LAN UTB. Pak jen stačí zadat „Name“ a „Password“ na základě informací získaných od správce sítě (ty jsou jedinečné). Následně stisknutím tlačítka „Save“ se vše uloží a připojení je vytvořeno.



Obr. 44 Okno pro vytvoření nového spojení

2) Nyní se objeví ve VPN klientovi již zřízené nové připojení a může se provést připojení tlačítkem „Connect“ (viz obr. 45).



Obr. 45 Okno již vytvořených připojení k VPN serveru

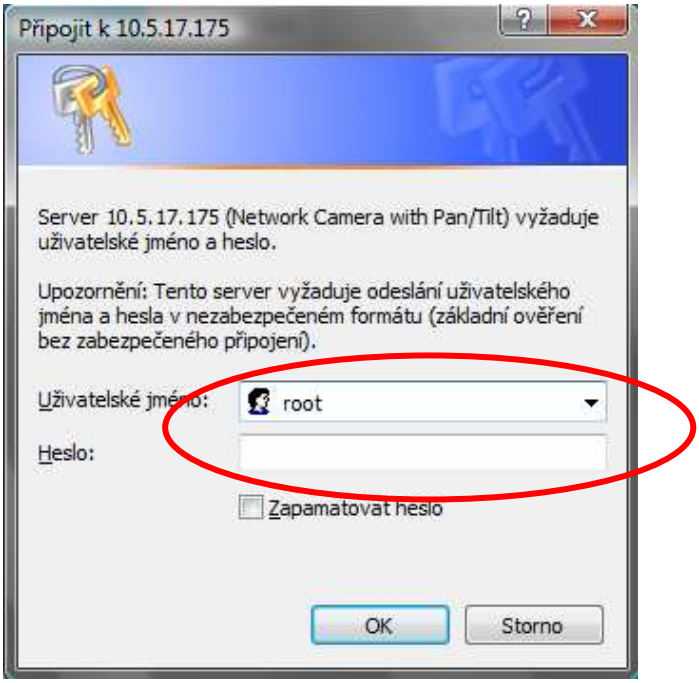
3) Po chvíli, kdy bude počítač navazovat spojení s VPN serverem v síti UTB ve Zlíně se po chvíli objeví okno, které si vyžádá síťový systém NOVELL v síti UTB ve Zlíně (viz obr. 46). V tomto okně vyplním přihlašovací údaje a heslo, které jsem získal již od začátku studia na UTB ve Zlíně pro připojení na můj síťový disk. Po zadání údajů počítač ze kterého se připojuji vzdáleně do sítě UTB ve Zlíně si ověří se servery sítě, zda uživatel je znám a zda má práva pro přístup do sítě. Jestli ano, pak se spojení uskuteční a objeví se ikona v pravém dolním rohu  se změní na  . Tím je spojení navázáno a počítač (nebo notebook) se chová jako by byl uvnitř v síti UTB ve Zlíně.

Obr. 46 Okno pro zadání přihlašovacích údajů do vnitřní sítě LAN UTB ve Zlíně

4) Otevřeme prohlížeč Internet Explorer a zadáme vnitřní IP adresu kamery (viz obr. 47), tedy 10.5.17.175.

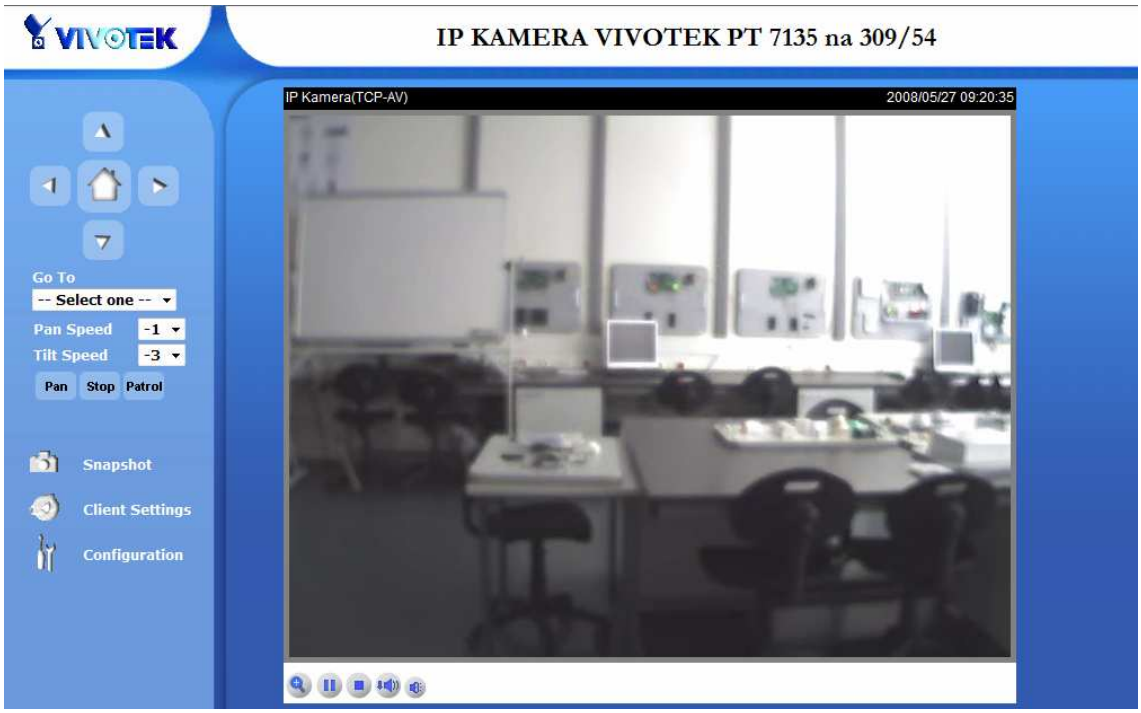
Obr. 47 IE a zadání adresy IP kamery

5) A následné se zobrazí přihlašovací okno (viz obr. 48). Pokud správce kamery nenastaví jinak je přihlašovacím jménem slovo „root“ a heslo nastavené dle správce kamery.



Obr. 48 Okno s přihlašovacími údaji

6) Po zadání správného uživatelského jména a hesla směrem ke kameře dojde k ověření přístupu a otevření webového rozraní kamery Vivotek (viz obr. 49). Pak můžeme využívat všechny funkce a nastavení (viz kapitola 3.7).

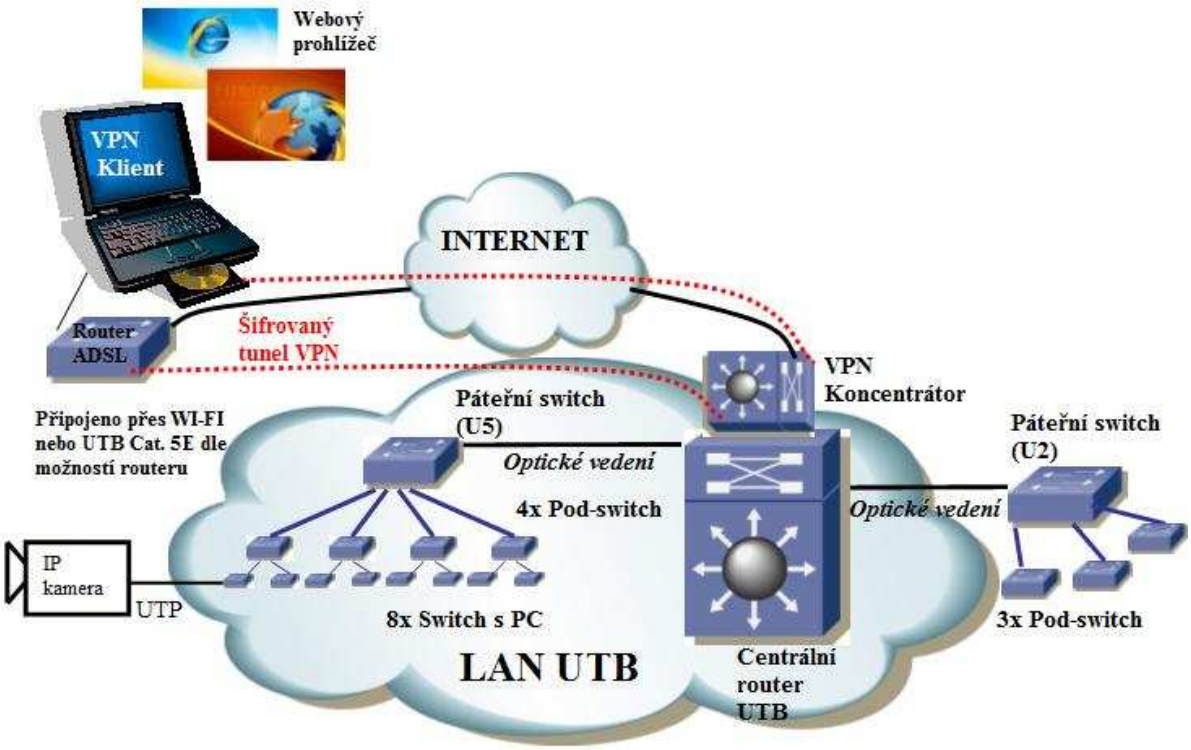


Obr. 49 Webové rozhraní IP kamery Vivotek

15.5.1 Schéma realizovaného vzdáleného přístupu k IP kameře přes Internet (typ ADSL) a VPN do vnitřní podnikové sítě LAN

Blokové schéma vytvářeno na základě připojení z rodinného domu s Internetovým připojením do sítě LAN UTB ve Zlíně přes klienta VPN pro Windows Vista.

V rodinném domě je používán Internet ADSL s rychlosti 3056kbps pro download a 256kbps pro upload. Už na první pohled upload je pro ovládání kamery důležitou položkou a z osobní zkušenosti mohu potvrdit, že tato rychlost pro odesílání dat do sítě je pro IP kameru Vivotek malá. Proto dochází v rámci agregace sítě, která je 1 ku 50 uživatelům k poklesu rychlosti dle připojeného počtu.

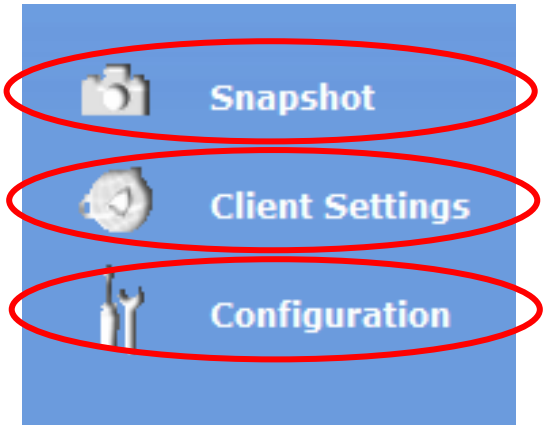


Obr. 50 Schéma pro připojení ze vzdáleného místa s připojením k Internetu přes ADSL a pomocí VPN klienta

16 FUNKCE A DOVEDNOSTI IP KAMERY OVLÁDANÉ VZDÁLENĚ PŘES LAN SÍŤ A INTERNET

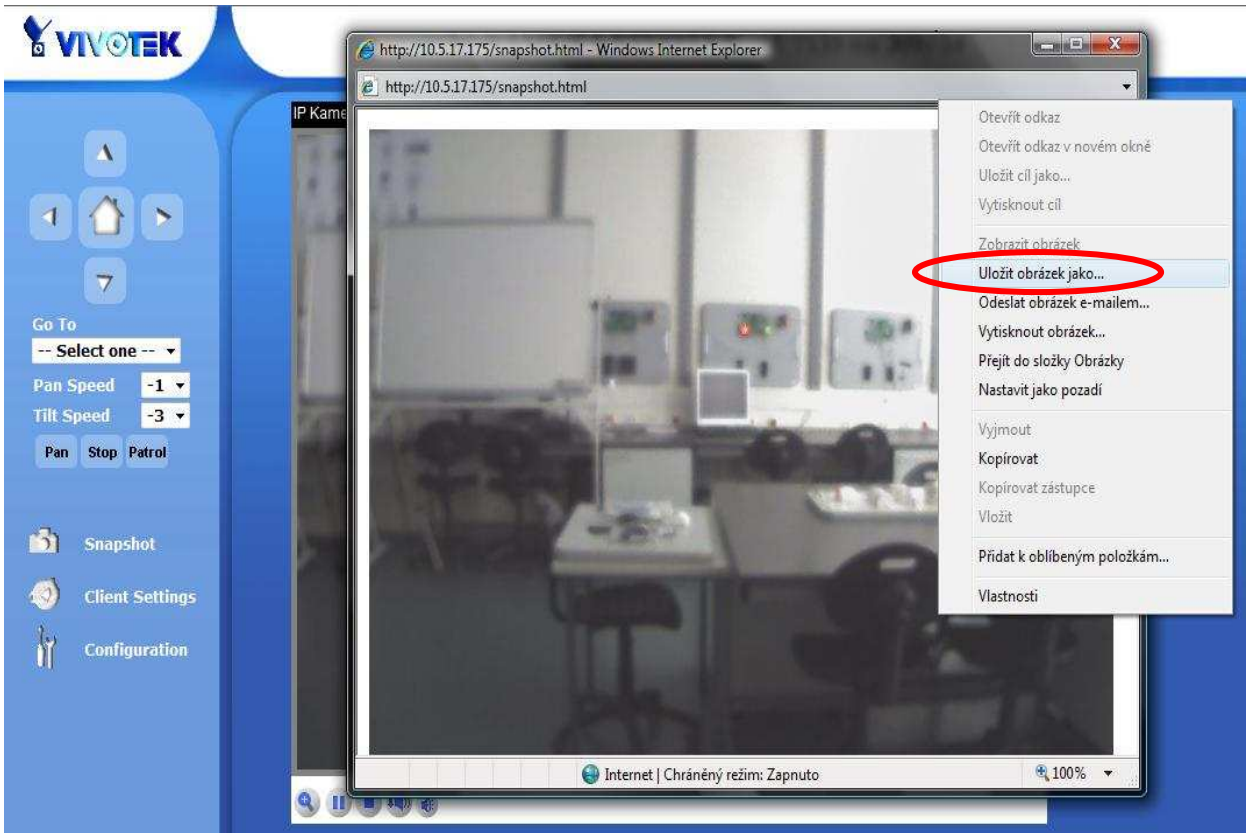
Po správném vyplnění přihlašovacích údajů se dostaneme do celkového nastavení z pohledu správce.

Nyní můžeme ovládat otočnou IP kameru dle libosti a nastavení (viz obr. 51).



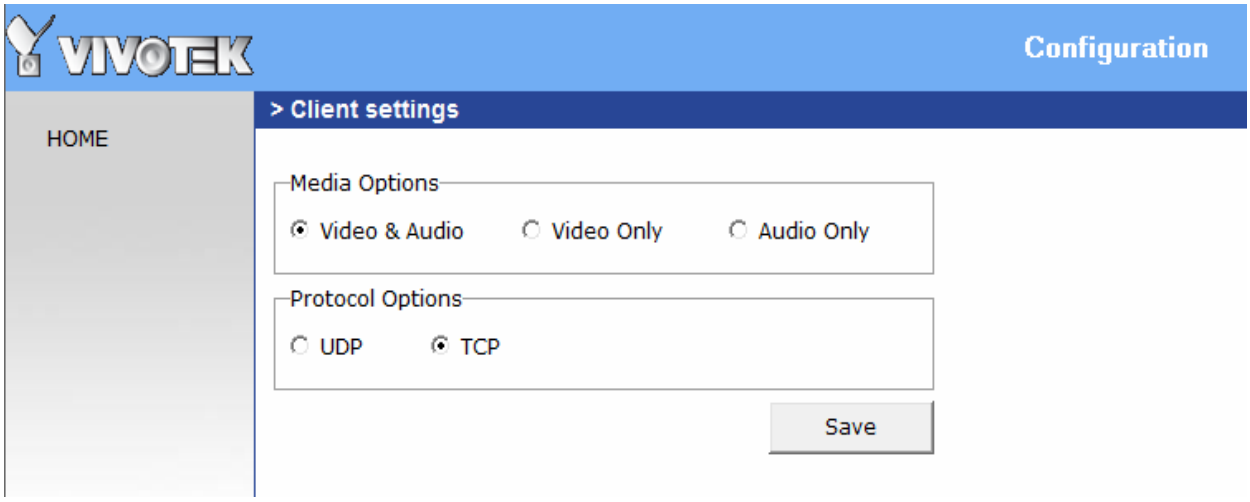
Obr. 51 Důležitá tlačítka pro nastavení a snímání obrázků

Pro nás jako správce jsou důležité tlačítka Snapshot a Client Settings. Po kliknutí myši na tlačítko „Snapshot“ (viz obr. 51) nám vyjede dialogové okno s obrazem pořízeného právě v momentě kliknutí myší na tlačítko „Snapshot“. Tento jeden obrázek můžeme uložit na paměťové médium a to tak, že najedeme myši na obrázek do libovolného místa a stiskneme pravé tlačítko myši. Vyjede nám nabídka, kde zvolíme „Uložit obrázek jako…“ (viz obr. 52). Následně vybereme úložiště a snímek ve formátu JPEG (či BMP) bude uložen na námi zvolenou paměť (HDD, USB či jiné).



Obr. 52 Okno pro zaznamenaní snímku „Snapshot“

Po stisknutí na tlačítko „Client Settings“ (viz obr. 51) se nám objeví dialogové okno (viz obr. 53). Zde můžeme nastavit přenosové protokoly, a zda kamera bude pořizovat pouze audio, nebo pouze video nebo obojí současně.



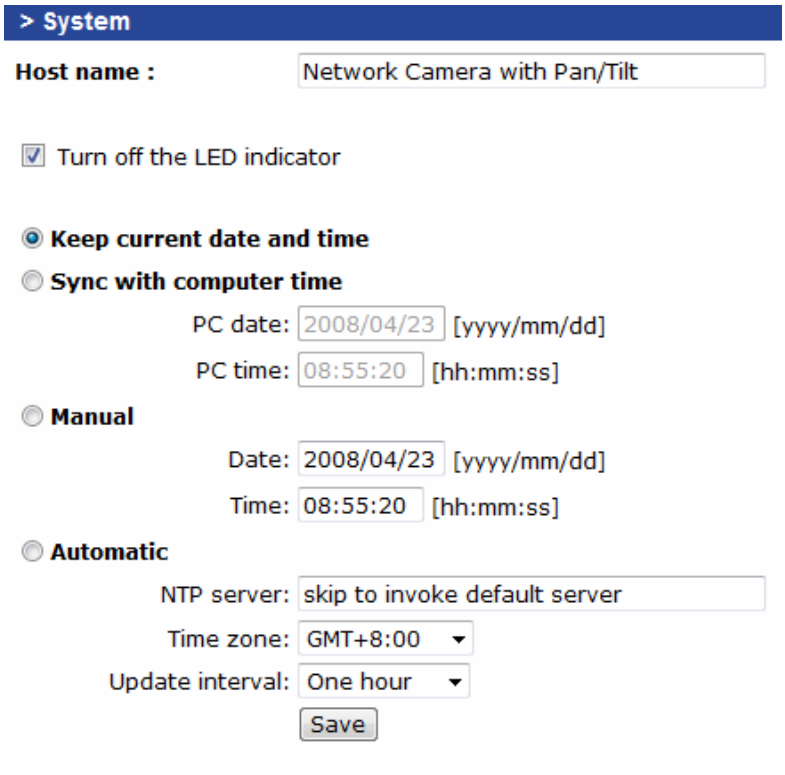
Obr. 53 Dialogové okno pro „Client Settings“

Po kliknutí myší na tlačítko „Configurations“ (viz obr. 51) se nám webové rozhraní rozdělí na sekce (viz obr. 54).

Obr. 54 Rozdělní webového rozhraní kamery do jednotlivých sekcí

16.1 System

V této sekci nastavuje „Host name“ tedy název, který se zobrazí jako nadpis na titulní straně. Dále můžeme nastavit, že kamera se bude jevit jako ve vypnutém stavu a nebudou svítit všechny tři LED diody (pro použití je potřeba zatrhnout funkci „Turn off the LED indicator“). A pro správný chod a monitoring v reálném čase je potřeba nastavit datum a čas (automaticky, manuálně nebo sychronizovaně s počítačem). Po jakékoliv změně je potřeba stisknout tlačítko „Save“.



Obr. 55 Sekce „Systém“

16.2 Security

V této sekci je možné nastavovat heslo pro správce kamery nebo zřizovat či odstraňovat až dalších 20 účtů pro jiné uživatele s omezenými právy.

Obr. 56 Sekce „Security“

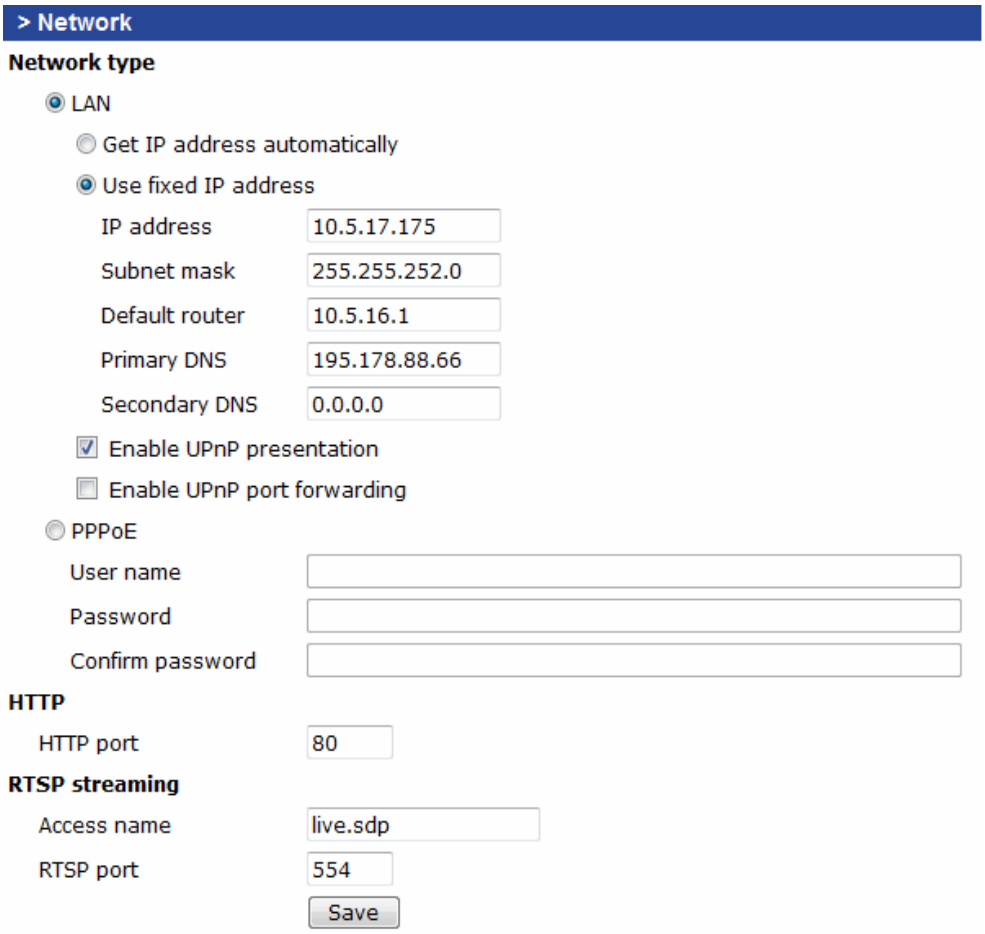
16.3 Network

V této sekci lze nastavovat síť. Při jakékoli změna může způsobit restart kamery, proto je doporučení před opuštěním této sekce a uložením tlačítkem „Save“ zkontrolovat případně zaspat hodnoty uvedené v editačních polích.

V nastavení sítí „Network type“ pro LAN připojení (PPPoE zapnout jen v případě, že kamera je přímo připojená na ADSL) se můžeme setkat s nastavením IP adresy a to jako automaticky přiřazována od DHCP severu, nebo zvolit pevnou IP adresu (nutná znalost počítačových sítí nebo prokonzultovat se správcem sítě).

Pro nastavení HTTP protokolu můžeme nastavit i jinou hodnotu než standardní číslo 80. Pří zadání jiného čísla portu (jiné než 80) musí uživatel při zadávání IP adresy do prohlížeče (IE) za IP adresu připsat dvojtečku a právě nové číslo portu. Tedy jestliže jsme změnili port na číslo 8080, pak při přihlašování bude adresa v prohlížeči vypadat v našem případě jako http://10.5.17.175:8080.

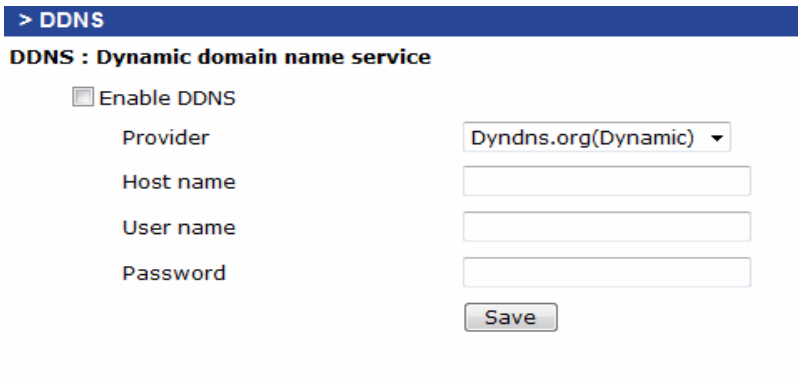
Lze nastavit přístupové jméno „Access name“ a číslo portu jiné než 554. Jedná o nastavení pro připojení ke kameře přes klienta a protokol RTSP pro mobilní telefony.



Obr. 57 Sekce „Network“

16.4 DDNS

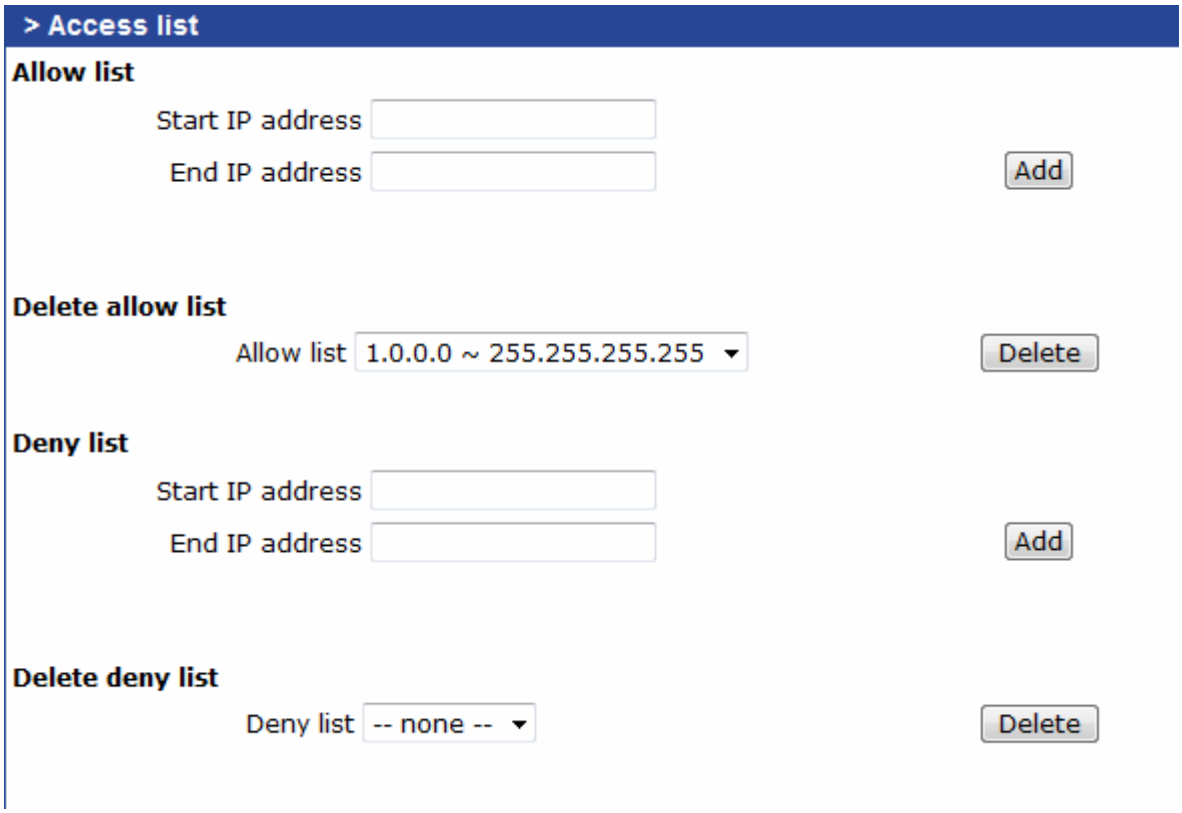
V této sekci je nutno nastavit jen v případě, že používáme více připojení k Internetu. V poli „Provider“ jsou vypsány poskytovatelé, kteří nabízejí tuto službu. Pro více informací o poskytování této služby musí správce navštívit WWW stránky daných poskytovatelů.



Obr. 58 Sekce „DDNS“

16.5 Access list

V této sekci se nastavuje přístup ke kameře z určité IP adresy. Správce má možnost omezit přístup ke kameře uživatelům. Stránka obsahuje dva seznamy. Jeden seznam povolených „Allow list“ a seznam zakázaných „Deny list“. Oba dva seznamy mohou obsahovat až 20 položek a intervalů IP adres.

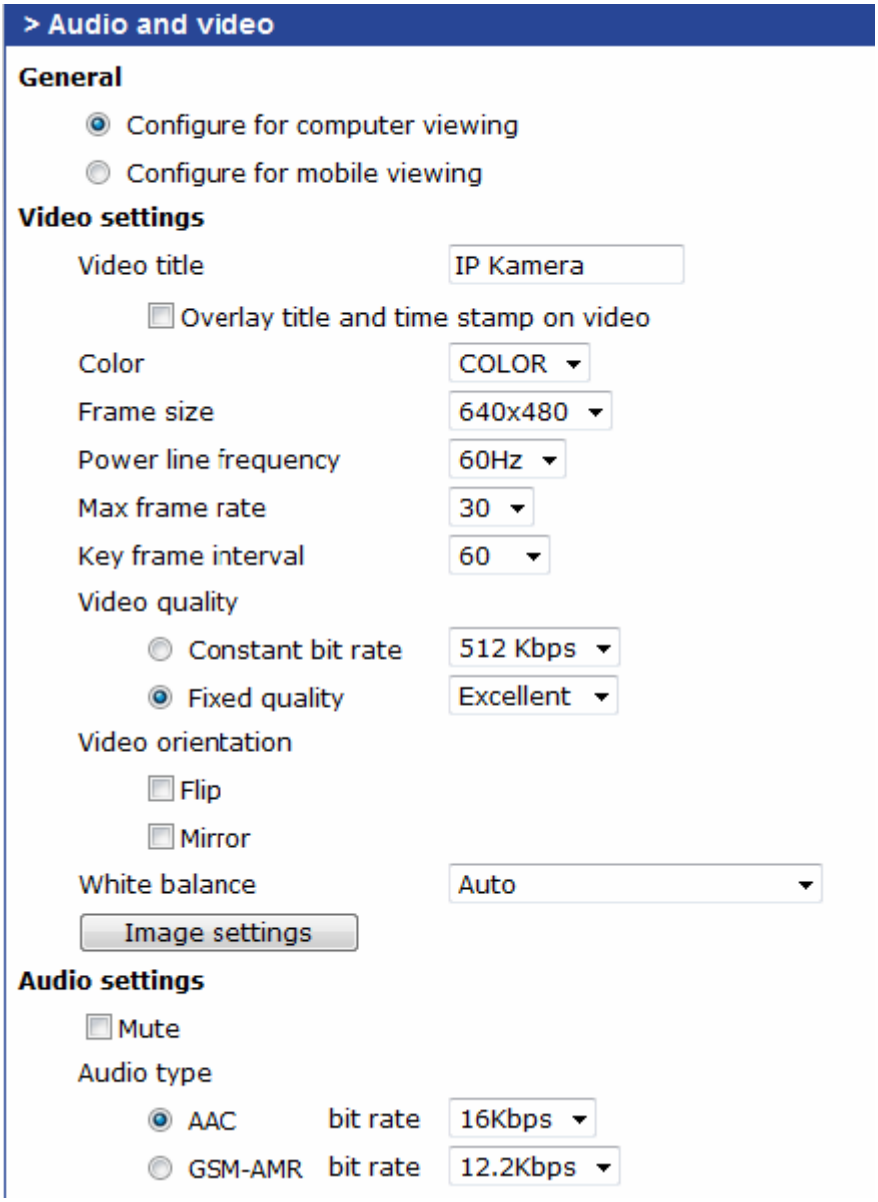


Obr. 59 Sekce „Access list“

16.6 Audio and video

Na této stránce v hlavní sekci „General“ můžeme nastavit prohlížení pro počítač nebo pro mobilní telefon. Podle zvolení se pak nastavují další parametry. Jeden z parametrů je text, který bude zobrazen spolu s datem a časem nad obrazem videa (černý pruh). Další možností je barevný režim „Color“, kde můžeme zvolit barevné zobrazení obrazu nebo černobílé zobrazení. Kamera dále nabízí tyto čtyři rozlišení: 160x120; 176x144; 320x240; 640x480. Nastavení frekvence napájení je závislá podle země, kde kamera vykonává službu. Pro ČR, SR a ostatní země EU musíme zvolit 50Hz. Kvalita zobrazení snímku je závislá na nastavení třech voleb. První volba „Max frame rate“ nastavuje maximální obnovovací frekvencí snímků. Ve volbě „Video quality“ můžeme nastavit „Constant bit

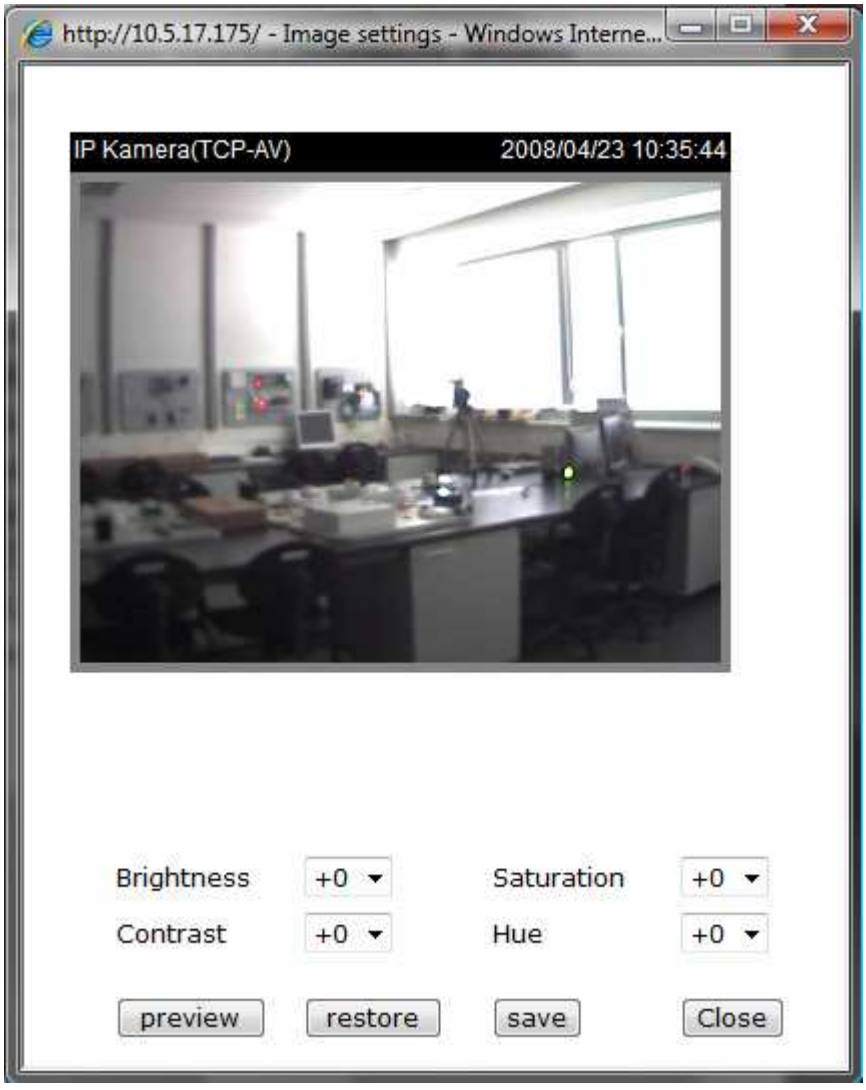
rate“, která se nastavuje v případě, že uživatel plánuje využít plně dostupnou šířku pásma. Pokud dojde k rychlým změnám obrazu a pokud nebude dostupná dodatečná šířka pásma, pak se může stát, že obraz v krátkých časových intervalech vypadne nebo dojde ke zhoršení kvality. Naopak funkce „Fixed quality“ umožní odesílat data v maximální nastavené kvalitě bez ohledu na šířku přenosového pásma. Toto nastavení se doporučuje pro lokální sítě (LAN) nebo pro rychlé připojení.



Obr. 60 Sekce „Audio a Video“

Dále lze nastavit parametry pro obraz. Otáčení obrazu okolo svislé osy či vodorovné („Flip“, „Mirror“). Vyvážení bílé barvy, která bude závislá na umístění a množství světla

v místnosti. Pokud rozkřikneme tlačítko „Image settings“, pak se nám objeví okno pro nastavování Jasu, kontrastu, odstínu, sytosti obrazu (viz obr. 61). Naše změněné nastavení si můžeme nejprve prohlídnout tlačítkem „Preview“ a následně uložit tlačítkem „Save“ nebo obnovit tyto parametry tlačítkem „Restore“.



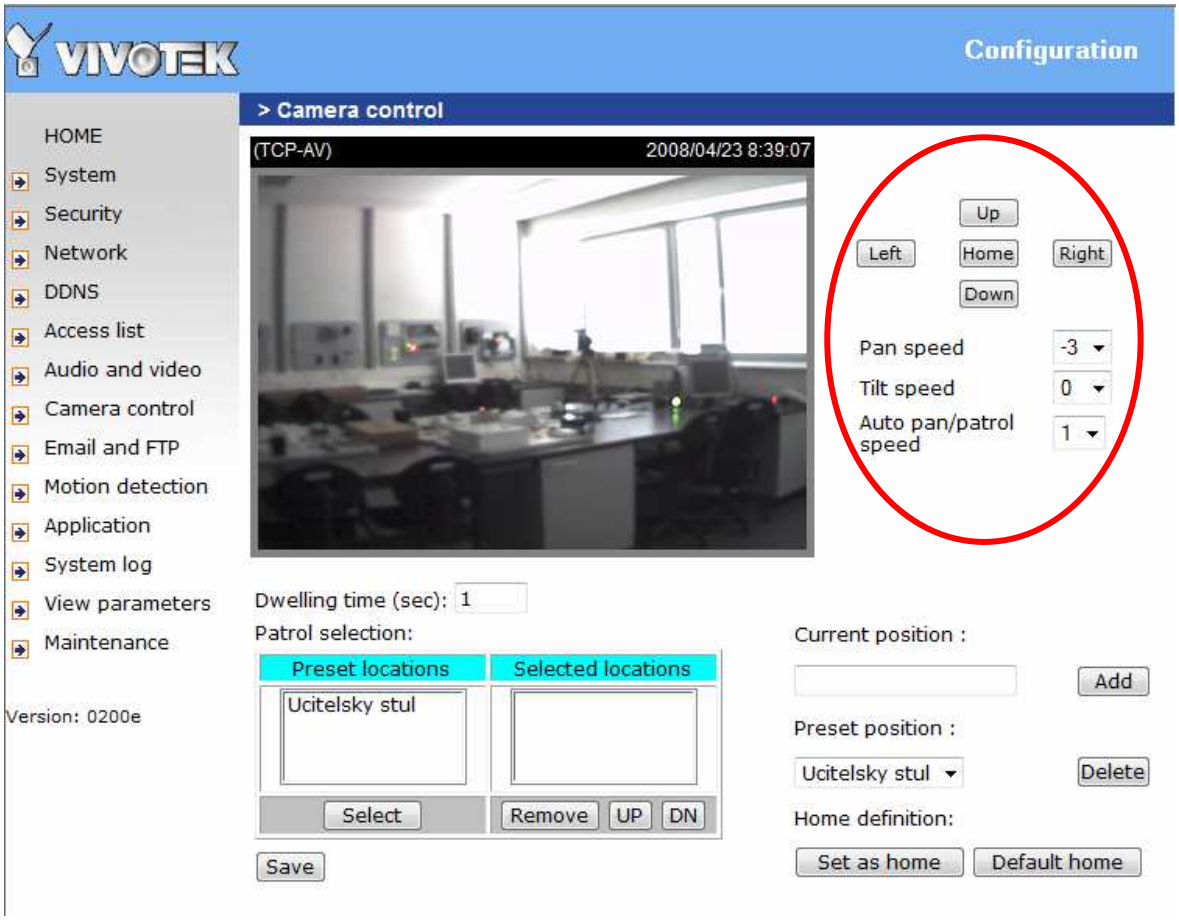
Obr. 61 Okno „Image settings“

Také v oblasti „Audio settings“ lze vypnout zvukový mikrofon „Mute“ a nastavit zvukové kodeky pro přenos zvuku (zpravidla není třeba měnit).

16.7 Camera control

V této sekci je možné provádět otáčení kamerou až o 350° a také naklápění kamery o 125°. Kameře lze nadefinovat rychlost otáčení („Pan speed“), což znamená o kolik dílku se

kamera otočí v horizontální směru při jednom kliknutí na myš, ale také rychlost naklápění („Tilt speed“) kamery ve vertikálním směru. Kamera umožňuje nastavení rychlosti otáčení v režimu panoramatického snímání nebo v režimu patroly („Auto pan/patrol speed“). Jestliže bychom chtěli aktuální záběrovou plochu uložit, postačí přidat název („Current positron“) a stisknout tlačitko „Add“. Pokud bychom požadovali zvolit si novou pozici pro tlačítko „Home“, pak po dosažení požadované pozice stiskneme tlačítko „Set as home“. Pro funkci patroly nebo panoramatického snímání lze zvolit určitý počet prepozic, které musíme nastavit do tabulky „Selected locations“ a tato uložená a pojmenovaná pozice bude jednou za zastávek patroly.

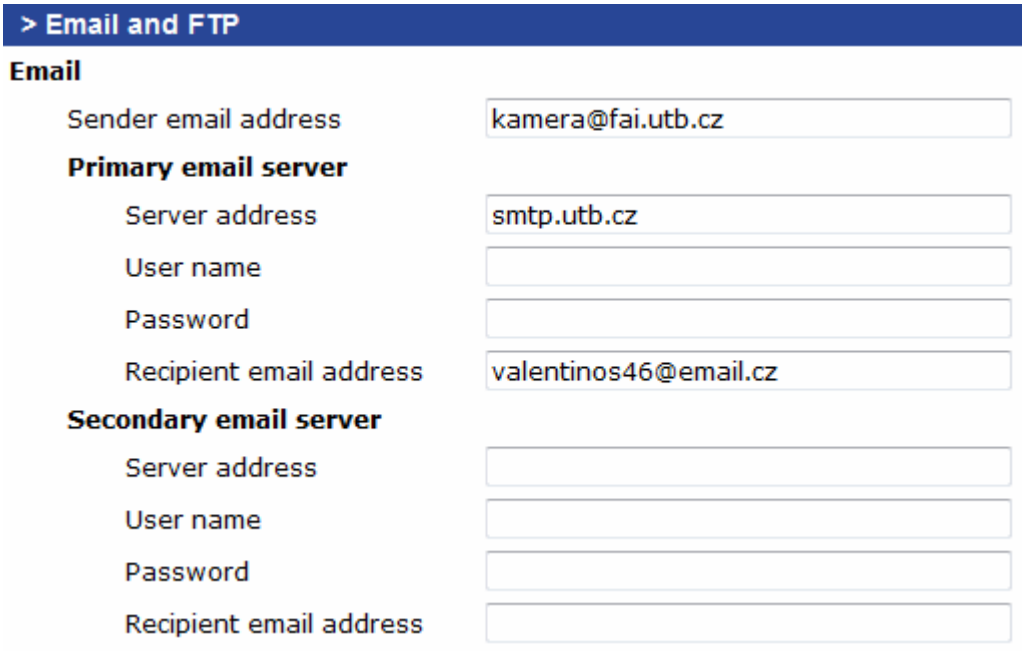


Obr. 62 Sekce „Camera control“

16.8 E-mail and FTP

V této sekci lze nastavit odesílání obrázku pořízených z IP kamery na E-mail nebo FTP server. Nastavení odesílání snímku na E-mail či FTP se odvíjí od množství zaslaných snímků a o velikosti kamerového systému. Odesílání snímku na E-mail můžeme použít jen

v případech, kdy chceme zaslat malé množství snímků (E-mailová schránka má menší kapacitu než FTP server). Většina SMTP serverů vyžadují autentifikaci, proto je třeba zadat jméno a heslo pro připojení k serveru. Do editačního pole „Sender email address“ je potřeba napsat libovolnou emailovou adresu pro identifikaci odesílatele. Pak lze zadat dva emailové servery nezávislé na sobě. Je to výhoda v tom případě, když primární server nebude dostupný, pak se kamera pokusí data odeslat přes sekundární server. Do editačního pole „Server address“ napíšeme IP adresu externího SMTP nebo doménový název. Do pole „User name“ vložíme uživatelské jméno pro přístup k SMTP serveru. Do pole „Password“ vložíme heslo pro přístup k SMTP serveru. Do pole „Recipient email address“ vložíme emailovou adresu příjemce snímků.

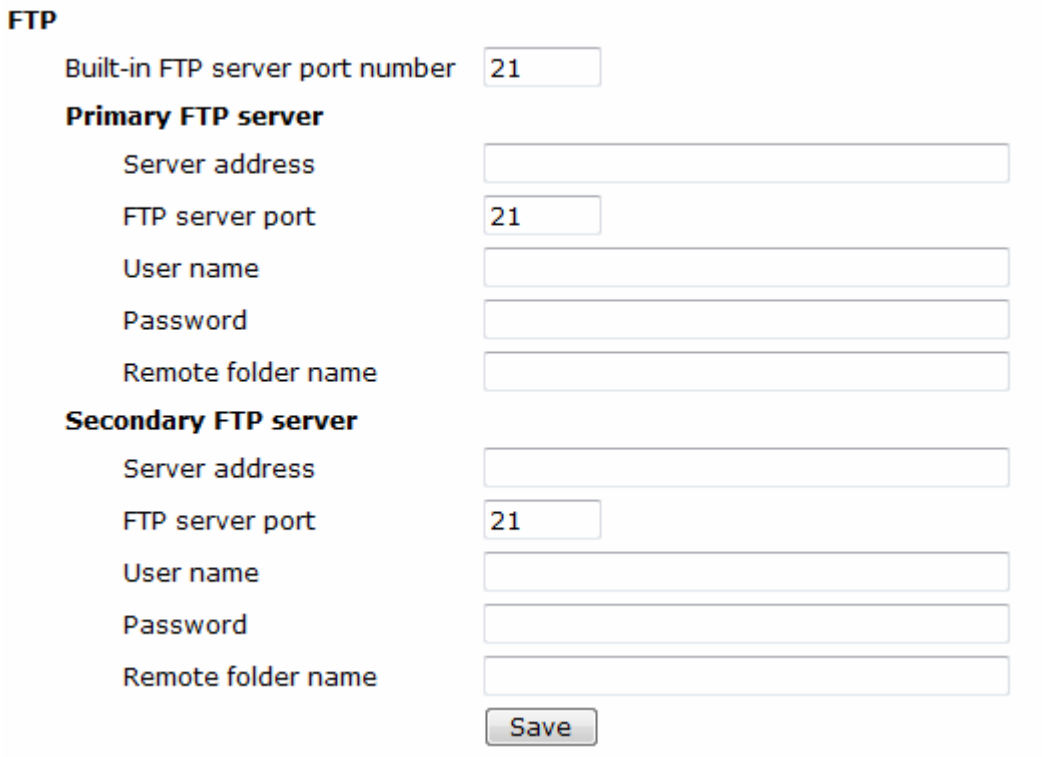


Obr. 63 Sekce „Email“

Pro FTP přenos se musí nastavit správný port pro příjemce („Bulit-in FTP server port numer“). Zpravidla jde o číslo 21. Lze zadat i jiné čísla z rozsahu 1025 až 65535. V případě změny se musí změnit číslo i v FTP klientovi.

Opět lze zadat jeden hlavní server FTP a jeden sekundární server FTP. V případě nedostupnosti hlavního serveru FTP se pokusí kamera odeslat snímek(y) na sekundární FTP server. Do editačního pole „Server address“ se napíše doménový název nebo IP adresa FTP serveru. U FTP se navíc zadává i uživatelské jméno a heslo. Do pole „User name“

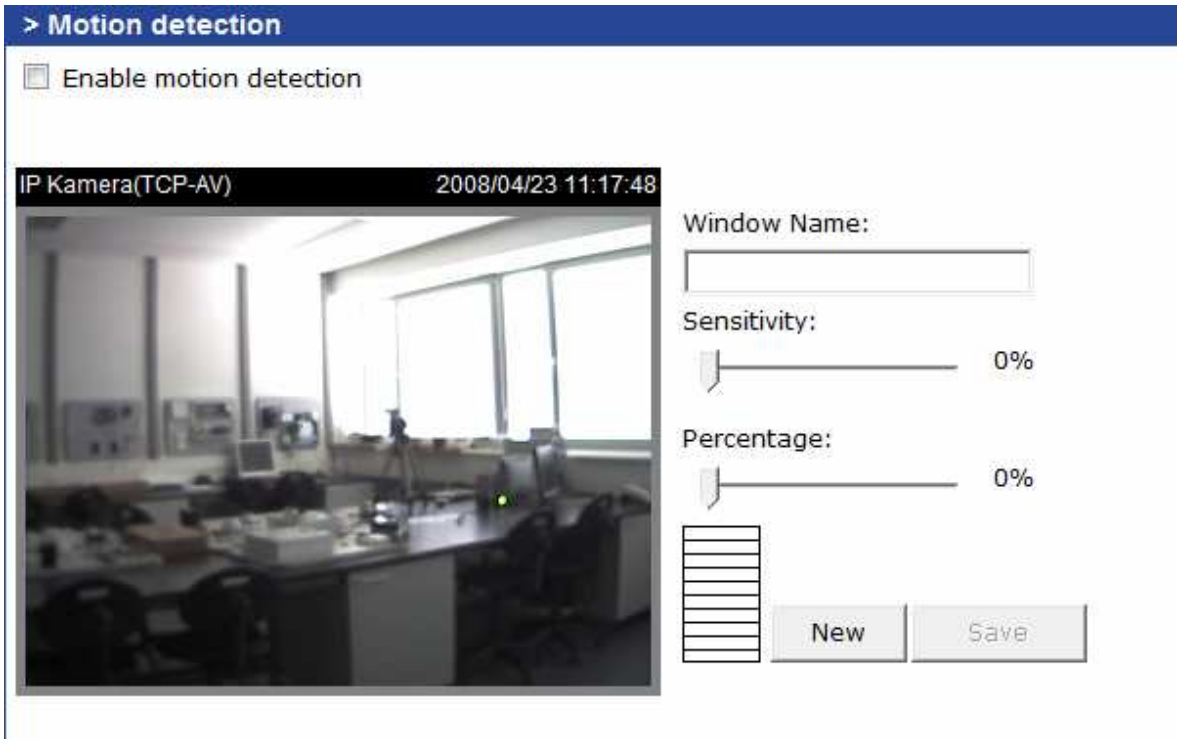
vložíme uživatelské jméno pro přístup k FTP serveru. Do pole „Password“ vložíme heslo pro uživatelský učet u FTP serveru. A posledního pole „Remote folder name“ se určí adresář FTP serveru pro ukládání snímku. Tento typ kamery Vivotek podporuje pouze pasivní režim přenosu obrazu na FTP server.



Obr. 64 Sekce „FTP“

16.9 Motion detection

V této sekci se seznámíme se speciální inteligencí této IP kamery. Jedná se o detekci pohybu. Jedná se o nejzajímavější vlastnost a umění kamery. Pro použití musíme nejprve zatrhnout „Enable motion detections“, tím se aktivuje detekce pohybu v obraze. Po stisknutí tlačítka „New“ získáme nové detekční okno. Lze vytvořit až tři nezávislá okno s možností překrývání. Při omylu stačí detekční okno zavřít pomocí malého tlačitka „X“. Jednotlivým oknům můžeme přiřadit název v poli „Windows name“ a citlivost v poli „Sensitivity“. V poli „Percentage“ lze nastavit detekovanou velikost objektu procentuálně k velikosti detekčního okna. Pokud nastavíme velkou citlivost a malou velikost objektu, pak dosáhneme velmi intenzivní a efektivní úrovně detekce pohybu.



Obr. 65 Sekce pro „Motion detection“

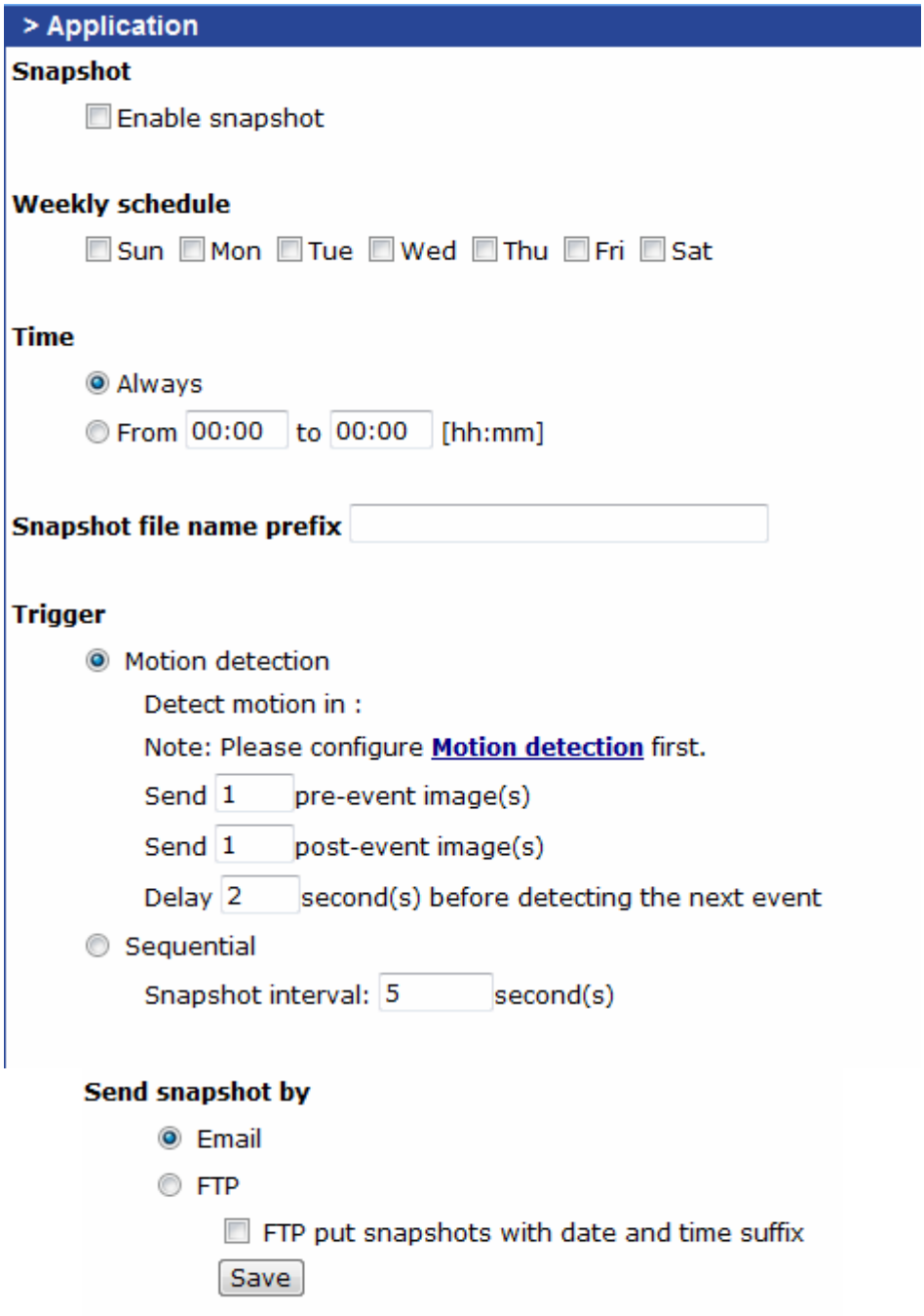
Tato funkce byla vyzkoušena a realizována zasláním snímku na E-mail schránku. Snímky se v případě překročení nastavené citlivosti odesílaly každých 5 sekund na zvolený E-mail.

16.10 Application

V této sekci se nastavují aplikace kamery. Jedním ze základních aplikací je zapnutí nebo vypnutí posílání snímku v poli „Enable snapshot“. Pakliže jsem povolili zasílání snímků, pak můžeme nastavit, ve které dny je žádoucí tyto snímky posílat nebo lze nastavit zasílání snímků každý den. Nyní lze zvolit časový interval a to buď zatržením „Always“ se snímky dle potřeby budou zasílat vždy nebo nastavíme časový interval. Dny v týdnu a čas je závislý dle nastavení v sekci „System“. Do pole „Snapshot file name“ můžeme uvést předponu, která bude použita pro začátek názvu odesílaných souborů JPEG.

Nejprve nastavíme v sekci „Motion detection“ zóny pro detekci pohybu, pak bychom mohli nastavit v této sekci počet snímků pořízených před událostí („Send pre-event image(s), které se pošlou v případě detekce pohybu. Jsou uloženy v paměti kamery. Rovněž je možné nastavit počet snímků pořízených po události („Send post-event image(s)“), které se pošlou v případě detekce pohybu. Jestliže chceme zadat časový odstup pro další detekci pohybu od současné detekce, pak hodnotu vložíme do pole „Delay

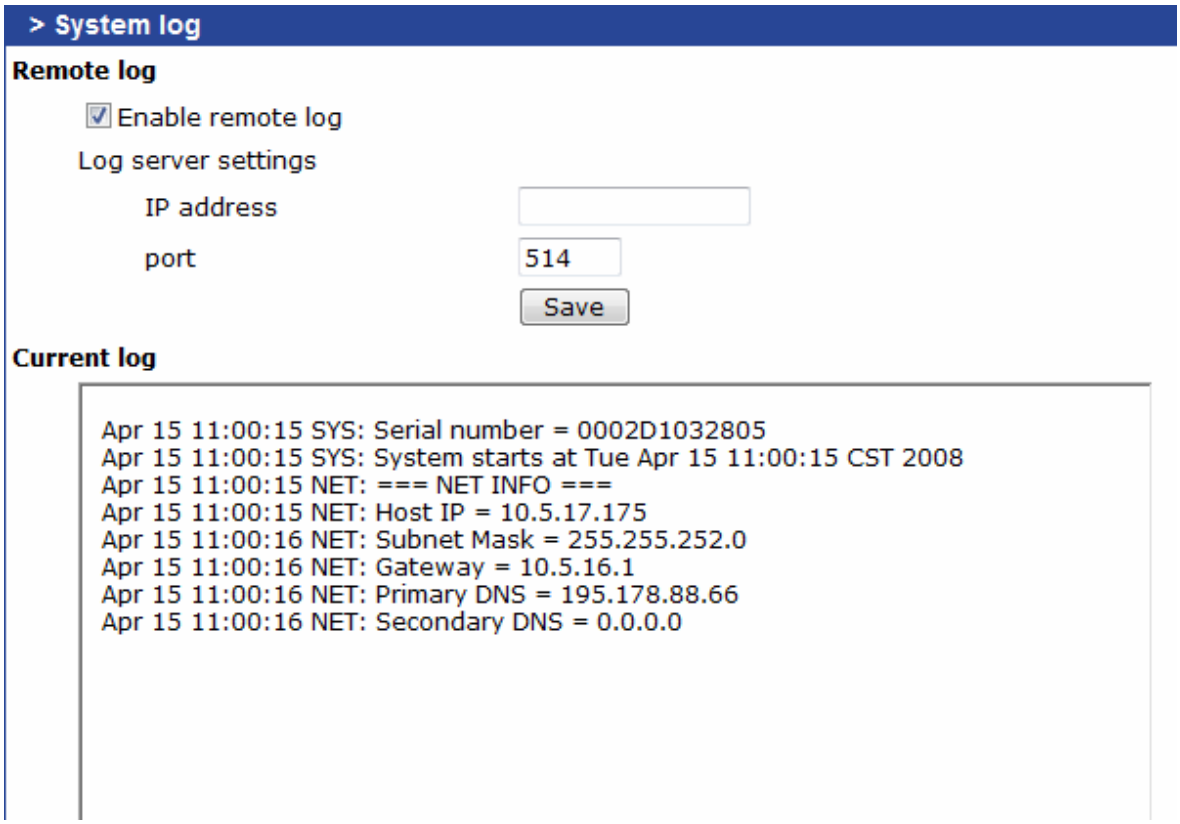
second(s) before detection next event“ v sekundách. V dalším případě lze nastavit místo zasílání snímků před a po události v intervalu, který si zvolíme v sekundách v poli „Snapshot interval“. V poslední kroku můžeme nastavit odesílaní snímku na Email nebo FTP. V případě zatrhnutí nabídky „FTP put snapshots with date and time suffix“ se snímky po sobě jdoucí nepřepisují, ale přidává se k nim přípona data a času. Kdyby funkce nebyla zatrhnutá tak se v časovém intervalu snímky přepisují následujícími.



Obr. 66 Sekce „Application“

16.11 System log

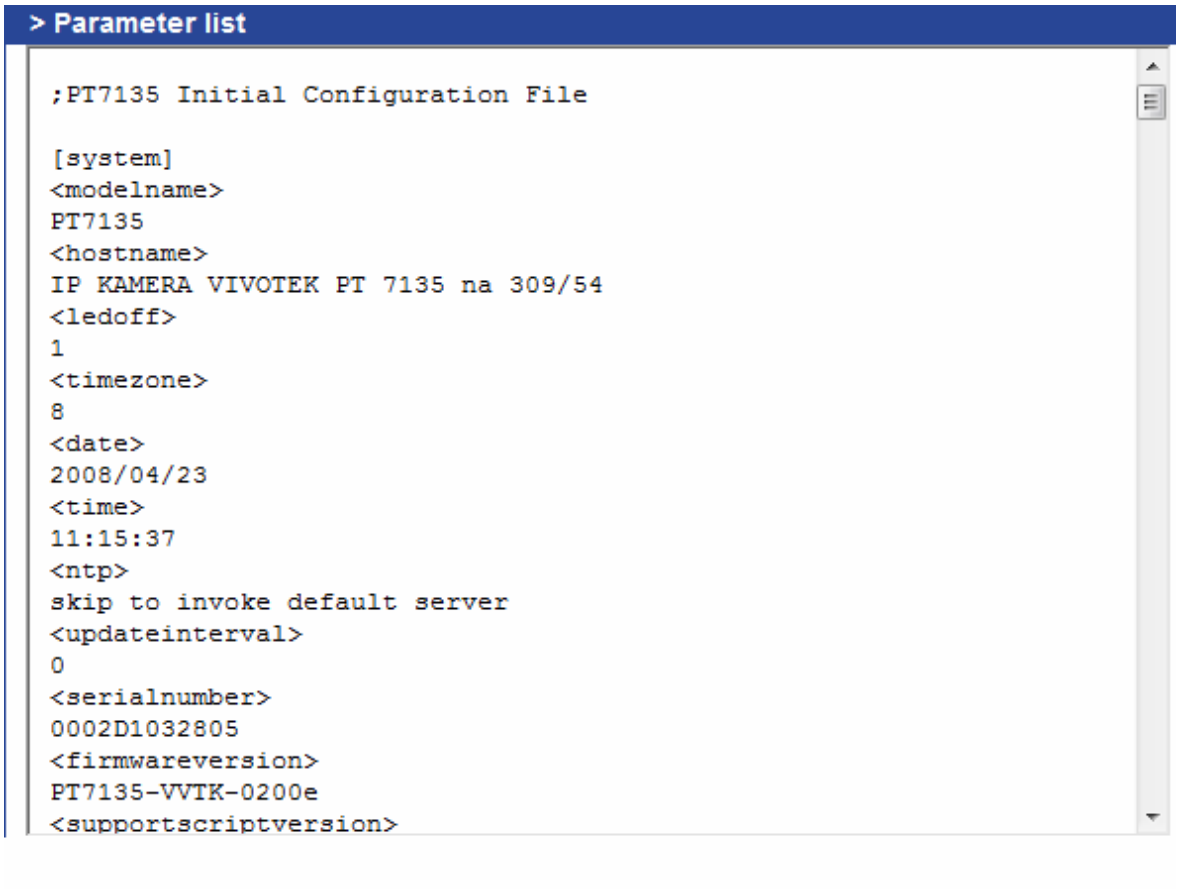
Tato sekce obsahuje užitečné události a informace v souvislosti s provozem kamery. Lze zasílat v případě potřeby tyto události na vzdálený server v tomto případě je nutné zatrhnout „Enable remote log“ a do pole „IP address“ zadat adresu externího serveru a do pole „Port“ zadat číslo portu. Nemusí to být 514.



Obr. 67 Sekce „Systém log“

16.12 View parameters

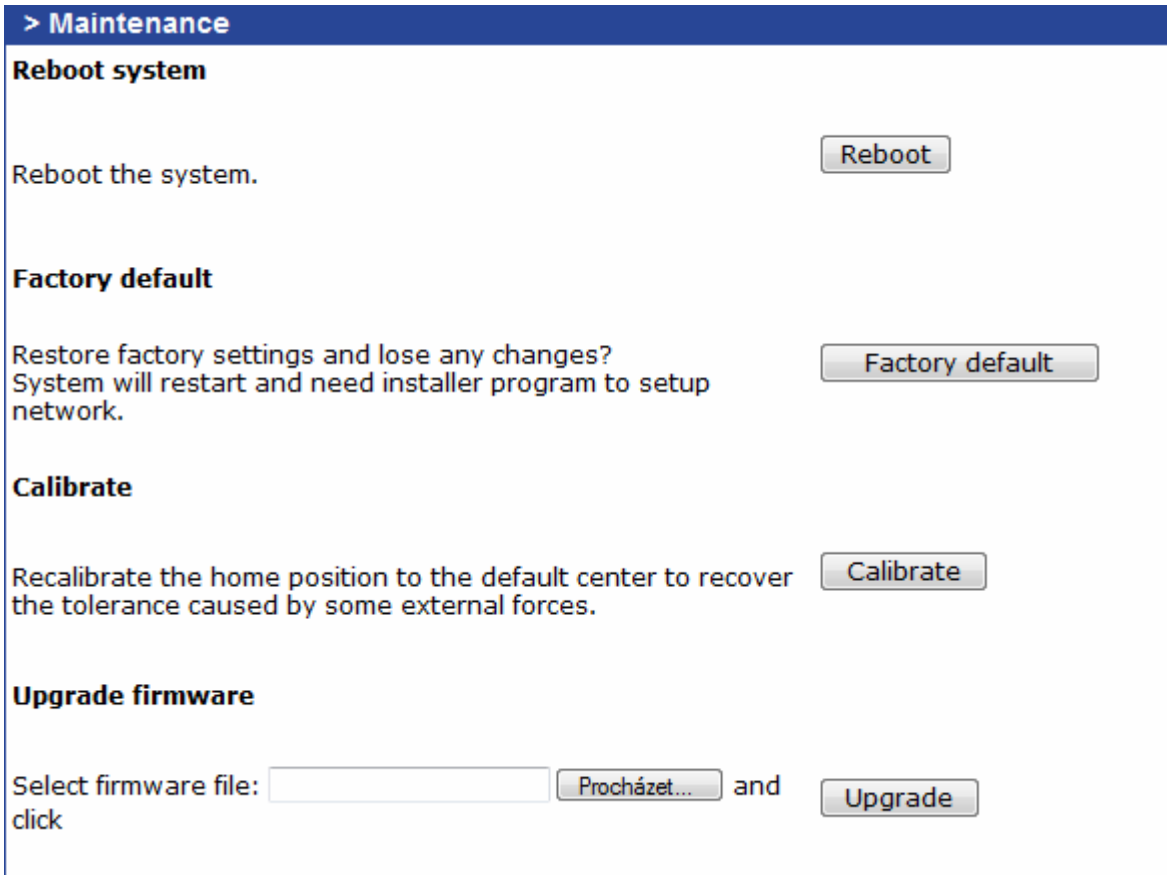
V této sekci se nám zobrazí stránka s kompletním nastavením parametrů kamery.



Obr. 68 Sekce „Parametr list“

16.13 Maintenance

Tato sekce je základem pro údržbu kamery. Nalezneme zde tlačitko „Reboot“, které způsobí restart kamery a to stejným způsobem jako bychom vyndali z kamery napájecí kabel. Stisknutím tlačítka „Factory default“ se smažou všechny parametry kamery a kamera bude resetována do počátečního stavu z výroby. Stisknutím tlačítka „Calibrate“ se kamera okamžitě mechanicky resetuje do středové polohy. V poslední možnosti v této sekci se setkáme s tlačítkem „Upgrade“, kde můžeme aktualizovat programové vybavení pomocí nového firmwaru.



Obr. 69 Sekce „Maintenance“

17 VÝVOJ A BUDOUCNOST

Přístup k BT spadá do moderních možností, které jsou v dnešní době ze strany firem nabízené. Přeci jenom je rozdíl u zabezpečovacích systémů a požárních systémů, které jsou instalované do RD nebo do firem. U RD si jen tak někdo kompletní požární systémy i s napojením na PCO HZS ČR nedovolí. Bude to řešit maximálně speciálním hlásičem, který bude komunikovat s ústřednou EZS. EZS systémy už jsou více viditelné u RD. U firem především většího rozsahu se už EPS systémy používají a můžu říct, že by měly být samozřejmostí. Přece jenom aktiva firmy jsou podstatné a to především lidský faktor, který je přímo součástí výrobního procesu a bez něho by se firmy neobešly. Přístupem do BT přes počítače a Internet má své výhody, ale mnohdy se ještě můžeme setkat s názorem, že má své nevýhody. Veškeré přístupy a možnosti s tím spojené směřují v této technice především k integraci BT a systémů do takové podoby, kde budou vytvářený sekce, kde každá bude plnit jeden článek celého komplexu ochrany zdraví a majetku. V první řadě mám tedy na mysli, že postupem času vzniknou univerzální moduly a komunikátory, které budou komunikovat přes určitý univerzální protokol pro všechny zařízení a budou obsahovat všechny programovatelné vstupy a výstupy od různorodých sběrnic. V druhé řadě mám na mysli SW vývoj, neboť komunikátory resp. převodníky už dneska jsou dostupné, ale mnohdy vyvinutý SW pro aplikace není kompatibilní s ostatními prvky v systému nebo není kompatibilní s odlišnými BT.

Proto bychom se jednou mohli dočkat SW, který bude schopen efektivně, spolehlivě a bezpečně přistupovat k jednotlivým BT pomocí jediného programu pro komplexní systém. Vzorem pro takové řešení instalace bezpečnostních, požárních, přístupových a monitorovacích systémů je pojem inteligentní budova. Její podoba představuje vysoký rámec integrace v podobě:

- Centralizovaná správa a údržba budov
- Integrace slaboproudých technologií se světem IT
- Náhrada některých řídících prvků slaboproudých systémů pomocí SW
- Snadné ovládání technologií pro každého uživatele
- Automatizace procesů bezpečnosti, údržby a provozu
- Jednotná instalace technologií po konvergované IP síti

ZÁVĚR

Mít přehled a umět získat cenné informace je důležitým prvkem pro osobní vzdělávání. Díky veškerým poznatkům jsem se mohl vzdělávat v oblasti, která vyplývá z názvu zadání bakalářské práce. Internet a jeho možnosti jsou dneska na takové úrovni, že i v oblasti BT jsou vyráběny jednotlivé komunikační moduly, které jsou schopny komunikace po Ethernetových sítích a tím docílit převod signálů (elektrických) na datové pakety, odpovídající struktuře TCP/IP protokolu.

V teoretické části práce jsem nastínil jednotlivé druhy bezpečnostních technologií. Specifikoval jsem jejich účel a jaké zaujímají místo v ochraně majetku a zdraví. Navrhnul jsem jednoduchou skladbu a popsal jednotlivé prvky systému. Největší důraz jsem kladl na přístup k těmto bezpečnostním technologiím přes Internet. V jednotlivých kapitolách jsem využíval schémat, která mají sloužit jako představa, jak a na jakém principu bezpečnostní systém pracuje. Jedná se o jeho strukturu, zařazení jednotlivých prvků v systému a objasnění funkcí jednotlivých zařízení a komunikačních modulů. Nakonec z toho vyplynulo, že přístup k dnešním moderním BT je reálný. Musí splňovat určité podmínky a apelovat na bezpečnost a přenos dat tak, aby bylo zabráněno neoprávněné manipulaci. Tuto neoprávněnou manipulaci zajišťují většinou SW bezpečnostní nadstavby anebo přímo komunikační moduly, obsahující šifrování pomocí klíčů. Některé komunikační moduly či převodníky, která zajišťují jednak komunikaci po Ethernetu a zároveň i šifrovanou komunikaci, jež jsou zmíněny v práci.

V praktické části jsem si měl vybrat jednu z existujících BT. V mém případě se jednalo o IP kameru, která spadá do kategorie CCTV (Close Circuit Television). IP kameru značky Vivotek, jsem zapojil, nastavil pro danou síť a zprovoznil tak, aby k ní byl přístup vzdálený, z kteréhokoliv místa v síti. Navíc jsem IP kameru zpřístupnil i přes Internet. Pro ověření funkčnosti jsem byl schopný se připojit ke kameře z mého bydliště, které je velmi vzdálené z místa instalace IP kamery. Proto v oblasti kamerových uzavřených systémů (CCTV) se mi podařilo objasnit vzdálený přístup přes Internet a rovněž názorně zobrazit (pomocí schémat) tento přístup. V oblastech zabezpečovacích a požárních systémů se mi podařilo pouze zpracovat teoreticky pomocí schémat vzdálený přístup. Požární systémy nenabízejí přes Internet takové možnosti jako BT CCTV, EZS, ACCESS CONTROL,

neboť systémy EPS chrání především zdraví před požárem a pomocí těchto systémů lze vzdáleně provádět pouze diagnostiku, správu či dohled, nikoliv konfiguraci.

Cílem bakalářské práce bylo prokázat, zda přístup přes Internet je k BT reálný. Věřím, že se mi podařilo splnit úkol dle zadání a taktéž objasnit možnosti Internetu v technologiích určených k ochraně majetku a zdraví.

ZÁVĚR V ANGLIČTINĚ

To posses a view and know how to obtain information is a important element for personal education. Thanks all piece of knowledge I could rear in the area, which results from title setting baccalaureate work. Internet and his possibilities are today on of such level, that and in the area BT are producing individual communications moduli, that are competently communication after Ethernet nets thereby reach for transmission signals (electric) on datal faggot corresponding structure TCP/IP record.

In theoretic parts work I foreshadowed individual sorts security technology. Specifyed I their purpose and what seat seat on protection possession and health. Suggested I simple composition and described individual elements system.Suggested I simple composition and described individual elements system. Biggest emphasis I laying on access to this security technologies over Internet. In single chapters I derive benefit from schematics, which have serve as image, how and on what tenet security system works. Acts of his structure, enlistment single elements in system and illumination function single arrangement and communications modulus. In the end of it follow on, that access to today's modern BT is real. Must answer definite conditions and invoke safeness and data transmission so, to was hamper unqualified handling. This unqualified handling interlock mostly SW security superstructure or directly communications moduli containing encryption by the help of keies. Some communications moduli or inverter, which interlock partly communication after Ethernet at the same time as well as in code communication, which are mentioned in work.

In practical parts I had choose some from going BT. Biggest emphasis I laying on access to this security technologies over Internet. In single chapters I derive benefit from schematics, which have serve as image, how and on what tenet security system works. Acts of his structure, enlistment single elements in system and illumination function single arrangement and communications modulus. In the end of it follow on, that access to today's modern BT is real. Must answer definite conditions and invoke safeness and data transmission so, to was hamper unqualified handling. This unqualified handling interlock mostly SW security superstructure or directly communications moduli containing encryption by the help of keies. Some communications moduli or inverter, which interlock

partly communication after Ethernet at the same time as well as in code communication, which are mentioned in work.

In practical parts I had choose some from going BT. In mine case dealt about IP camera, which coincides to the caregory CCTV (Close Circuit Television). IP camera brands Vivotek, I gear, set for given to net and open so, to to her was access distant, from any seats in net. In addition I IP camera make accessible and over Internet. For check functionality I was able add to camera from of my domicile, which is very distant from seats installation IP cameras. Therefore in the area camera reserved systems (CCTV) me managed clear up distant access over Internet and as well clearly display (by the help of schematics) this access. In the area preventive and fire systems me managed only work up abstractedly by the help of schematics distant access. Fire systems no offer over Internet of such possibilities like BT CCTV, EZS, ACCESS CONTROL, because systems EPS saves above all health before fire and by the help of these systems can be far do only diagnosticians, repair or sight, no configuration.

Aim baccalaureate work was evidence, whether access over Internet them to BT real. I trust, that me managed realize imposition according to setting and likewise clear up possibilities internet in technologies intended to protection possession and health.

SEZNAM POUŽITÉ LITERATURY

[1] KŘEČEK , Stanislav. *Příručka zabezpečovací techniky / Stanislav Křeček a kolektiv* . 3. aktualiz. vyd. [s.l.] : [s.n.], 2006. 313 s. ISBN 80-902938-2-4.

[2] UHLÁŘ , Jan. *Technická ochrana objektů II. díl : Elektrické zabezpečovací systémy II.*. Olga Ryšánková. 1. vyd. Praha : [s.n.], 2005. 229 s. ISBN 80-7251-189-0.

[3] KREISER, Jiří. *Vyvážené smyčky* [online]. 2002 [cit. 2008-05-20]. Dostupný z WWW: <http://www.jablotron.cz/info.php?pid=smycky>.

[4] ČANDÍK, Marek. *Objektová bezpečnost II. : Univerzita Tomáše Bati ve Zlíně*. Marek Čandík, 2004. 100 s. ISBN 80-7318-217-3.

[5] *Www.sezam.cz : EMZ* [online]. [cit. 2008-05-20]. Dostupný z WWW: <http://www.sezam.cz/produkty/emz/>.

[6] Elektronický katalog od firmy PROBIN, s.r.o., [cit. 2008-05-20]. Dostupný z reklamního CD.

[7] *Www.netcam.cz : Co je to IP kamera?* [online]. [cit. 2008-05-20]. Dostupný z WWW: <http://www.netcam.cz/encyklopedie-ip-zabezpeceni/co-je-sitova-kamera.php>.

[8] LUHOVÝ , Karel. *VPN (7) - šifrování na síťové vrstvě* [online]. 2003 [cit. 2008-05-20]. Dostupný z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=203>.

[9] ODVÁRKA, Petr. *Principy komunikace, média, rozsah : Rozsah* [online]. 2000 [cit. 2008-05-20]. Dostupný z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=13>.

[10] ODVÁRKA, Petr. *Ethernet* [online]. 2000 [cit. 2008-05-10]. Dostupný z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=18>.

[11] *Ethernet* [online]. [cit. 2008-05-10]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Ethernet>.

[12] *Co je to video server (enkodér)* [online]. [cit. 2008-05-10]. Dostupný z WWW: <http://www.netcam.cz/encyklopedie-ip-zabezpeceni/co-je-to-videoserver.php>.

[13] *Výhody IP kamer oproti analogovým a PC kamerám : Výhody oproti systému analogových (CCTV) kamer* [online]. 2007 [cit. 2008-05-22]. Dostupný z WWW: <http://www.netcam.cz/encyklopedie-ip-zabezpeceni/vyhody-sitovych-kamer.php>.

[14] *Zabezpečení sítě* [online]. 2007 [cit. 2008-05-24]. Dostupný z WWW: <http://www.netcam.cz/encyklopedie-ip-zabezpeceni/zabezpeceni-site.php>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Access Control - Přístupový systém
Bit	Jednotka informace
BMP	Microsoft Windows Bitmap – Formát pro rastrovou grafiku
BNC	Bayonet Neill-Concelman - Bajonetový konektor
BT	Bezpečnostní technologie
CCTV	Close Circuit Television - Uzavřené televizní okruhy
CD	Collision Detection – Kolizní detekce
CSMA	Carrier Sense Multiple Access – Vícenásobný přístup
ČSN	Česká státní norma
DHCP	Dynamic Host Configuration Protocol – služba pro automatické přídělování IP adres
DVR	Digital video recorder – Digitální video rekordér
EN	Evropská norma
EPS	Elektronická požární signalizace
EZS	Elektronická zabezpečovací signalizace
HDD	Hard disk drive – Úložiště dat
HTTP	Hypertext Transfer Protocol – Hypertextový přenosový protokol
HTTPS	Hypertext Transfer Protocol Security – Hypertextový přenosový protokol
HW	Hardware – zařízení
HZS	Hasičský záchranný sbor
IP	Internet Protocol – Internetový datový protokol
ISP	Internet service provider – Poskytovatel připojení
JPEG	Joint Photographic Experts Group – Formát ztrátové komprese obrázků
kbps	Jednotka přenosové rychlosti - Kilobit za sekundu

KTPO	Klíč trezoru požární ochrany
LAN	Local Area Network – Lokální sítě
MAN	Metropolitan Area Network – Metropolitní síť
NVR	Network video recorder – Síťový video rekordér
OPPO	Obslužné pole požární obsluhy
OS	Operační systém
PAN	Personál Area Network – Osobní síť
PC	Personal computer – Osobní počítač
PIR	Passive Infra – Red detector – Pasivní infračervený detektor
PTZ	Pan, Tilt, Zoom – Otáčení, naklápění, přiblížení
RD	Rodinný dům
SHZ	Stabilní hasící zařízení
SOZ	Samočinné odvětrávací zařízení
SW	Software – Programové vybavení
TCP	Transmission control protocol – Transportní protokol
USB	Universal Serial Bus – Univerzální sériové sběrnice pro přípojení periferií k PC
UTP	Unshelded Twisted Pair – Kroucený dvoupár
VPN	Virtual private network **–** Virtuální počítačová síť
WAN	Wide Area Network – Rozsáhlé sítě
Wi–Fi	Wireless fidelity – Bezdrátové připojení
ZDP	Zařízení dálkového přenosu

SEZNAM OBRÁZKŮ

SEZNAM TABULEK