VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

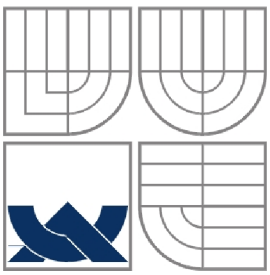
MONITOROVACÍ A ZABEZPEČOVACÍ SYSTÉM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

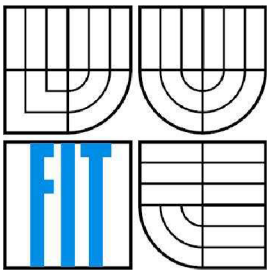
AUTOR PRÁCE
AUTHOR

BC. MARTIN FELIX

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

MONITOROVACÍ A ZABEZPEČOVACÍ SYSTÉM

MONITORING AND SECURITY SYSTEM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

BC. MARTIN FELIX

VEDOUCÍ PRÁCE
SUPERVISOR

ING. PAVEL OČENÁŠEK, PH.D.

BRNO 2010

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav informačních systémů Akademický rok 2009/2010

Zadání diplomové práce

Řešitel: **Felix Martin, Bc.**
Obor: Informační systémy
Téma: **Monitorovací a zabezpečovací systém**
Monitoring and Security System
Kategorie: Počítačové sítě

Pokyny:

1. Seznamte se s technologiemi koncových zařízení pracujících jak "wireless" tak "wired". Analyzujte možnosti monitorování různých vnějších událostí (kamerový systém, senzory a čidla).
2. Navrhněte vlastní bezpečený protokol pro obecnou komunikaci s koncovými prvky, zjišťování jejich aktivity a výstupů. Protokol implementujte jako bezpečnou službu na centrálním serveru (bráně), ke kterému jsou koncové prvky připojeny.
3. Navrhněte a implementujte webový portál využívající uvedeného protokolu a umožňující přístup a administraci z vnější sítě.
4. Analyzujte možnosti a informování uživatele (email, SMS/pager, ICQ, IP služba) včetně možností zjišťování stavu (aktivity) těchto výstupních kanálů (fronta). Na základě výsledků analýzy navrhněte a poté implementujte oznamování událostí (alarm) pro cílový systém.
5. Diskutujte možnosti dalšího rozšíření projektu.

Literatura:

- Tanenbaum, A.S.: Computer Networks. Fourth Edition, Prentice Hall, 2003
- Kurose J.F., Ross K.W.: Computer Networking, A Top-Down Approach Featuring the Internet. Addison-Wesley, 2003
- Fraden, J.: Handbook of Modern Sensors: Physics, Designs, and Applications, AIP Press, 2003

Při obhajobě semestrální části diplomového projektu je požadováno:

- Body 1 - 2.

Podrobné závazné pokyny pro vypracování diplomové práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva diplomové práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap, které byly vyřešeny v rámci ročníkového a semestrálního projektu (30 až 40% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním neprepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Očenášek Pavel, Ing.**, UIFS FIT VUT
Datum zadání: 21. září 2009
Datum odevzdání: 26. května 2010

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav informačních systémů
612 66 Brno, Božetěchova 2

L.S.

doc. Dr. Ing. Dušan Kolář
vedoucí ústavu

Abstrakt

Tato diplomová práce se zabývá návrhem a implementací systému pro monitoring a zabezpečení objektů. Celý systém slouží jako aplikační brána mezi klasickou TCP/IP sítí a heterogenní sítí obsahující různá koncová zařízení jako jsou kamery, mikrofony a čidla (teplotní, kouřové). Na základě zaznamenaných událostí (pohyb, hluk, požár) z těchto koncových prvků je možné odeslat upozornění uživatelům (SMS, e-mail). Systém je možné vzdáleně spravovat a je možné prohlížet aktuální data z koncových zařízení. Teoretická část této práce se zabývá rozborem druhů jednotlivých koncových zařízení a jejich využitím pro monitorovací systémy. Společně s tím je rozebrán popis jednotlivých komunikačních protokolů zařízení. Dále je provedena analýza kamerových systémů jako celku a jejich propojení s aplikační bránou tvořenou centrálním linuxovým serverem. Praktická část popisuje metody a techniky použité při implementaci systému a problémy s nimi spojené.

Abstract

This master's thesis deals with design and implementation of system for securing and monitoring objects. The whole system is serving as an application getaway between typical TCP/IP network and heterogeneous network containing different end devices such as security cameras, microphones and some sensors (e.g. for temperature measurement). In case of detected event, the notification is created, recorded and the user is informed via administrative front-end. System can be managed from remote location and data from devices can be shown by web interface. Theoretical part of this project concerns with the analysis of different types of connecting devices and sensors and the possibilities of their usage for the monitoring systems along with description of communications protocols for each end device. The next part deals with the cameras interfaces, content analysis and connectivity with central server. Practical part describes methods and techniques used for implementation of system.

Klíčová slova

Koncové zařízení, bezpečnostní kamera, webkamera, IP kamera, teplotní čidlo, detektor kouře, kamerový systém, monitorování, zabezpečovací systém, alarm, aplikační brána.

Keywords

End device, security camera, web camera, IP camera, heat sensor, smoke sensor, CCTV, monitoring, security system, alarm, application gateway.

Citace

Bc. Felix Martin: Monitorovací a zabezpečovací systém, diplomová práce, Brno, FIT VUT v Brně, 2010

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením Ing. Pavla Očenáška, Ph.D. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Bc. Martin Felix
26. 5. 2010

Poděkování

Tímto bych chtěl poděkovat mému vedoucímu práce Ing. Pavlu Očenáškovi, Ph.D. za vedení při tvorbě této práce a za cenné připomínky a rady. Dále bych chtěl poděkovat Mgr. Janě Skokanové za přístup k síťové kameře.

Obsah

1 Úvod

Od nepaměti mají lidé potřebu chránit svůj vlastní majetek před odcizením, znehodnocením a dalšími vnějšími vlivy. Původní zabezpečovací systémy byly velmi primitivní, ale jako spousta dalších věcí i zabezpečovací systémy prošly a neustále prochází postupným vývojem. Bezpečnost je v dnešní době velmi důležitým pojmem, se kterým se setkáváme v každodenním životě. Je nezbytnou součástí spousty oborů, a proto jsou na ni kladeny neustále větší a větší nároky. Nynější bezpečnostní systémy jsou velmi kvalitní a sofistikované, je to způsobeno především rozšířením internetu, mobilních sítí a integrací vysoce výkonných mikročipů. Umožňují nám nejenom zabezpečení objektů proti krádežím, poškozování, ale i proti přírodním katastrofám a mnoha dalším vnějším vlivům. Většina moderních systémů navíc podporuje vzdálené monitorování, zobrazování dat ze zařízení, a to vše z kteréhokoliv místa na světě. Aktuálně snímané dění je možno zaznamenávat a kdykoliv si jej prohlédnout. Jednou z největších výhod současných systémů je automatické informování uživatele o narušení bezpečnosti, ať už se uživatel nachází takřka kdekoliv na světě. Je tedy možno rychle a efektivně jednat při narušení bezpečnosti. Námi navrhovaný systém tedy bude sloužit jako aplikační brána mezi klasickou TCP/IP sítí a heterogenní sítí obsahující různá koncová zařízení jako jsou kamery, mikrofony a čidla (teplotní, kouřové). Systém bude možné vzdáleně spravovat a bude možné prohlížet aktuální data z koncových zařízení.

První kapitola (1) práce má název Úvod. Slouží k zasazení řešené problematiky do širšího kontextu a v podobě stručného obsahu jednotlivých kapitol definuje strukturu písemné práce.

Ve druhé kapitole (2) je proveden rozbor různých typů koncových zařízení, jejichž funkčnost se přímo či nepřímo dotýká monitorovacího anebo zabezpečovacího systému. Závěrem této kapitoly je vyhodnocení využití jednotlivých zařízení v systému pro ochranu před nežádoucími vlivy.

Třetí kapitola (3) popisuje komunikační protokoly pro práci s jednotlivými typy koncových zařízení. Zvláštní pozornost je věnována protokolu SNMP a knihovně pro komunikaci s webkamerami.

Kapitola čtyři (4) popisuje možné způsoby informování uživatele o narušení bezpečnosti. Jednotlivé varianty jsou důkladně rozebrány a popsány.

Pátá kapitole (5) pojednává o kamerových systémech jako celku, jejich propojení a umístění. Je zde probrána důkladná analýza jednotlivých druhů kamerových systémů.

Kapitola šestá (6) obsahuje návrh aplikační brány a webového portálu. Nejprve jsou definovány požadavky na celkovou funkčnost a chování systému. Z provedené analýzy je vytvořen předběžný popis systému soustav. Rovněž jsou zde vybrány konkrétní typy jednotlivých koncových zařízení, které budou použity jako testovací prvky při návrhu a implementaci systému. Následuje rozbor role aplikační brány v systému a požadavky na takovou bránu. Diagram případů užití s jeho specifikací zobrazuje, jak by se celý systém mohl v praxi chovat. Dále je zde vytvořen konceptuální diagram tříd a popsán návrh prototypu třídy zapouzdřující koncová zařízení.

V kapitole (7) se nachází popis implementace vytvořeného systému. Nejprve je krátce zhodnocen návrh a analýza monitorovacího systému a následně je popsáno, jakým způsobem celý systém pracuje. Jsou zde popsány nevýhody a výhody zvoleného řešení a kroky, které bylo třeba při implementaci podobně sofistikovaného systému řešit. Krátce je popsáno uživatelské rozhraní systému. Na závěr této kapitoly je provedeno vyhodnocení celé implementační části.

V závěru je vyhodnocena provedená analýza, návrh a implementace monitorovacího a zabezpečovacího systému. Jsou zde popsány klady a zápory takto fungujícího systému a směr, jakým by se celý systém mohl dále vyvíjet. V závěru kapitoly se nachází kompletní shrnutí dosažených výsledků.

Diplomová práce navazuje na semestrální projekt, ve kterém byla především provedena analýza využití koncových zařízení (kap. 2) a jejich zapojení do společného systému, který bude sloužit jako nástroj pro zabezpečování objektu (kap. 3). Dále v něm byl proveden předběžný návrh aplikační brány a způsob přístupu do uživatelské části aplikace z internetu (kap. 4). Diplomová práce tedy naváže doplněním a upravením analýzy a návrhu systému podle nabytých znalostí a zkušeností. Další část práce bude věnována samotnému popisu aplikace a hlavně kroků použitých pro její implementaci.

2 Analýza koncových zařízení

Koncové zařízení (koncový bod, prvek) je jednoznačně identifikovatelná entita stojící na jednom konci komunikačního toku mezi hostitelem a zařízením. V našem případě to budou kamery, mikrofony a čidla různých typů a vlastností. Avšak i samotný centrální server může být z abstraktního hlediska chápán jako koncové zařízení.

Z hlediska monitoringu a zabezpečení mají největší uplatnění koncová zařízení, jako jsou kamery, mikrofony a různé typy senzorů (čidel). O funkci *kamer* se není třeba dlouze rozepisovat, je zřejmé, že patří k nejlepším zabezpečovacím nástrojům, které zvládají jak detekci pohybu, tak je s nimi i případně možné detekovat stopy po kouři, ohni a dalších živlech. *Mikrofon* bývá běžnou součástí kamer a může sloužit jako další bezpečnostní prvek reagující na nadměrný hluk, kdy detekce pohybu může být podmíněna tím, že úroveň hluku stoupla o určitou hladinu. Senzorů neboli čidel je na trhu spousta, nás budou hlavně zajímat *čidla teplotní*, která umožňují kontrolovat teplotu monitorovaného subjektu. Tato vlastnost se nám může velmi hodit například při kontrole proti zamrznutí objektu (domu) anebo naopak hlídání proti vysokým teplotám.

V následujících podkapitolách si podrobněji popíšeme tři základní třídy koncových zařízení. Pro každou třídu si uvedeme různé podtřídy, které se od sebe většinou budou lišit interní softwarovou a hardwarovou výbavou a rozhraním, přes které jsou připojitelné k počítači.

2.1 Kamery

Kamera je přístroj používající se k zachycení pohyblivých obrázků. Původně byla vyvinuta pro televizní průmysl, ale v dnešní době se již používá běžně v mnoha různých odvětvích. Nás bude hlavně zajímat z hlediska *kamerových a zabezpečovacích systémů* viz kapitola 5.

Kamery můžeme rozdělit na *analogové* a *digitální*. Digitální kamery převádějí signál přímo na digitální výstup, jsou často menší než analogové, ale zato dražší. Analogové kamery jsou již v současné době částečně na ústupu, ale jejich zastoupení je stále nezanedbatelné. Proto budou zohledněny v navrhovaném kamerovém systému. Standardní kamery, ať už analogové či digitální, jsou obvykle vybaveny snímacím prvkem *CCD*. Levnější řešení je použití *CMOS* čipu, který se nachází především v nízkonákladových zařízeních. [1]

2.1.1 Průmyslové kamery

Díky technickému pokroku v oblasti vývoje CCD obrazových prvků jsou dříve výhradně používané černobílé bezpečnostní kamery postupně nahrazovány kamerami barevnými. V důsledku zvyšování integrace polovodičových čipů docházelo k postupnému rozšiřování řídící elektroniky kamer o nové vlastnosti, např. řízení expozice (elektronická závěrka) a přesné zahájení snímání. Trendem posledních let jsou tzv. inteligentní kamery, sdružující funkce klasické kamery a vyhodnocovacího systému s komunikačním rozhraním. Výstupem takové kamery nemusí být digitální ani analogový obrazový signál, ale analogová nebo digitální hodnota určující sledovaný stav nebo transformaci snímaného obrazu. [5], [23]

Bezpečnostní kamery se vyrábějí v nejrůznějších provedeních: standardní kamery s CS závitem (normalizovaná vzdálenost snímacího prvku od ohniskové roviny objektivu) pro výměnný objektiv, kompaktní kamery s vestavěným objektivem, polokulovité kamery pro montáž na strop, deskové kamery pro vestavbu do různých zařízení atd. Pro kamerové systémy s aktivní obsluhou (operátorem) je možné využít tzv. auto-dome kamery, které umožňují vzdálenou manipulaci (natáčení, naklápění a přibližování). Dnes se bezpečnostní kamery používají pro sledování nejrůznějších objektů a pozemků, k zabezpečení bank, muzeí, galerií, benzinových pump, parkovišť, letišť a v mnoha jiných zabezpečovacích aplikacích. [5], [8]

Obr. 2.1: Typické tvary průmyslových kamer. Zleva auto-dome, dome, standard [8]

2.1.2 Webkamera

Webová kamera (zkráceně webkamera) náleží do skupiny počítačových koncových zařízení, podobných videokameře či skeneru. K počítači se ve většině případů připojuje USB rozhraním. Snímky zachytávané z těchto kamer jsou obvykle ukládány na internetové úložiště. Takto pořízené aktuální snímky jsou dostupné mnoha uživatelům s počítačem a internetovým připojením kdekoliv na světě. Majitel webkamery s vysokou rychlostí internetového připojení může umožnit častější zachytávání snímků (a odesílání) a cíloví uživatelé mohou pak tyto snímky sledovat plynule podobně jako video. Z těchto důvodů se webkamera nejčastěji používá pro video-telefonování, video-konference apod.

Vzhledem k nízkým pořizovacím nákladům těchto zařízení nastal v poslední době jejich rozmach a mnoho dnešních domácích uživatelů i firem proto webkamery používá jak pro obrazovou komunikaci, tak pro ochranu majetku či osob. Velkým přínosem pro veřejnost je využití webkamer na důležitých dopravních tepnách, dálnicích a ulicích, kde každý řidič může sledovat aktuální stav dopravy takřka on-line. [8]

Obr. 2.2: Typický tvar webové kamery [17]

2.1.3 IP kamera

S technickým pokrokem, zejména v oblasti přenosových sítí a v oblasti digitalizace videosignálu, se začínají stále více prosazovat tzv. síťové IP kamery. *IP kamery* se používají v kamerových systémech, kdy se pro přenos dat a kontrolních signálů používá *internetový protokol* přes síťové vedení. IP kamery však udržují krok s moderními trendy a existují i v provedeních pro připojení k bezdrátovým sítím. IP kamery se také proto často nazývají síťové kamery. V pouzdře takové kamery je kromě standardní videokamery integrován rovněž *videoserver*, který zajišťuje komprimaci videosignálu a připojení videokamery k počítačové síti. Naprostá většina síťových IP kamer má zabudovaný *webový server*, který umožňuje sledovat obraz ze síťové IP kamery a provádět vzdálenou správu pomocí standardního webového prohlížeče z kteréhokoliv místa v lokální síti nebo internetu. Takový server poskytuje vývojářům zabezpečovacích systémů výborné komunikační rozhraní pro práci s kamerou. IP kamery jsou proto využívány mimo jiné pro video-monitoring a zabezpečení vzdálených objektů. [1], [8]

Součástí IP kamer jsou také dvoucestné audio kanály, které umožňují komunikaci mezi sledovaným objektem a osobou jej sledující. Kamery obsahují i LED diody, které zlepšují kvalitu obrazu za snížené viditelnosti a primárně tedy slouží pro pozorování v nočních hodinách. Díky tomu je kamera schopna snímat kvalitní obraz i za zhoršených podmínek. Většina IP kamer je schopna snímat obraz v minimálním rozlišení 640x480 obrazových bodů a za jednu sekundu zvládnout zachytit 30 snímků.

IP kamery se používají pro sledování stejným způsobem jako standardní průmyslové kamery. Součástí IP kamerového systému obvykle bývá například DVD rekordér nebo samotný stolní počítač pro zaznamenání obrazu zachyceného kamerami. Často se síťové kamery používají jako tzv. on-line kamery k přímému přenosu na internetu (sledování dopravy, průběhu stavby, sněhové zpravodajství ze zimních středisek apod.). Protože obraz z on-line kamery může sledovat kterýkoliv uživatel s připojením k LAN nebo internetu, stávající pojem *CCTV* (uzavřené televizní okruhy) přestává být výstižný. Proto se pro označení této techniky používají pojmy jako např. IP monitoring, network video monitoring nebo *OCTV* (otevřené televizní okruhy). [8]

Již ze specifikace síťových kamer je zřejmé, že jsou odlišné od standardních webkamer, které mají mnohem nižší cenu, nemají vestavěný videoserver a pro jejich připojení k síti je potřeba počítač vybavený USB rozhraním.

Obr. 2.3: Typický tvar síťové IP kamery [8]

2.1.4 GSM kamera

GSM kamera, jinak zvaná SimCam, představuje kompaktní mobilní dohledový a monitorovací systém, díky kterému je možné o případném narušení bezpečnosti okamžitě vědět. Díky možnostem okamžité reakce na pohyb jsou tyto kamery zajímavé pro využití v místech, kde není fixní připojení k síti anebo k centrálnímu serveru. Jakmile kamera tohoto typu zachytí pohyb, odešle MMS zprávu (snímaný obraz) nebo SMS zprávu z kamery přímo na mobil zadaný v nastavení kamery. Tato kamera rovněž nabízí vzdálený odposlech sledovaného prostoru a další funkce. Výhodou této kamery je téměř absolutní variabilita, co se týče jejího umístění. Stačí pouze pozice s mobilním signálem a elektřinou. GSM kamery obvykle bývají vybaveny pohybovým pasivním infračerveným senzorem, mikrofonem, infračerveným světlem a kvalitním snímačem. Kameru je možné ovládat a nastavovat pomocí SMS příkazů. Je například možné vyžádat si obrázek ukazující okolí kamery. [12]

Obr. 2.4: Typický tvar GSM bezpečnostní kamery [8]

2.1.5 Vyhodnocení

Z vlastností jednotlivých typů kamer, uvedených v tabulce 2.5 vyplývá, že každá kamera je určena pro jiné použití. Je proto komplikované zvolit nejvhodnější typy kamer pro náš systém. Vzhledem k tomu, že má být systém pokud možno co nejvíce univerzální, budeme uvažovat všechny kamery připojitelné k počítači přes standardní rozhraní. Konkrétně se tedy bude jednat o soustavu analogových kamer, IP kamer a webkamer. Webkamera se jeví jako nejperspektivnější, jelikož od navrhovaného systému nebudeme čekat monitorování nějakého velkého průmyslového objektu, ale spíše domácnosti apod. a cena takové kamery je oproti ostatním typům řádově nižší.

	Analogová kamera	IP kamera	Webkamera	GSM kamera
Formát videa	mpeg	mpeg-4 h.264	mpeg-4	JPEG
Mikrofon	výjimečně	ano	ano	ano
Pohyblivost	ano	ano	ne	ano
Přibližování	ne	výjimečně	ne	často
Noční vidění	často	ano	ne	často
Minimální rozlišení	510x490	640x480	640x480	320x240
Maximální rozlišení	750x590	1280x1024	1280x1024	640x480
Rozhraní	BNC konektor	Ethernet, Wi-fi	USB	GSM
Umístění	Venkovní i vnitřní	Venkovní i vnitřní	vnitřní	Venkovní i vnitřní
Zabudovaný detektor pohybu	ne	ano	ne	ano

Tab. 2.5: Přehled různých druhů bezpečnostních kamer

Standardní analogová průmyslová kamera - pro její použití bude třeba, aby centrální server obsahoval videokartu, která bude schopna převést analogový signál na digitální. Nedostatkem je, že běžně vybavené počítače takovou kartu neobsahují. Proto je nutné ji pořídit a zvyšuje se tak cena celého systému. Značnou nevýhodou může být, že při nutnosti videokarty se výrazně snižuje možnost využití notebooku (netbooku) jako centrálního serveru. Takový netbook by přitom kvůli své nízké ceně a příkonu mohl velmi dobře sloužit jako centrální server. Velkou výhodou videokaret je naopak integrace celé řady vlastností. Například komprimace dat do formátu MPEG-4 a detekce pohybu. Z hlediska napojení na centrální server na tyto kamery budeme nahlížet jako na webkamery, jelikož komunikační protokol je pro ně stejný.

Webkamera - díky nízké pořizovací ceně, poměrně dobrému rozlišení výstupního signálu a snadné připojitelnosti k počítači jsou webkamery dobrou volbou pro využití v navrhovaném kamerovém systému. Mezi další výhody patří fakt, že webkamera obsahuje mikrofon, který od bezpečnostních kamer v našem systému budeme standardně vyžadovat. Nevýhodou u těchto kamer je napájení z USB portu. Při použití na větší vzdálenosti může docházet ke ztrátám ve vedení, které mohou způsobit vady v přenosu signálu nebo zcela znemožnit správnou funkčnost kamery. Další nevýhodou je statické umístění a nemožnost natáčení. Kamera tak bude moci snímat pouze prostor v jejím manuálně nastaveném zorném úhlu. Největší nevýhodou oproti ostatním kamerám je absence detektoru pohybu, který je pro naše řešení velmi důležitý. Není však problémem k detekci pohybu využít nějaké volně šiřitelné softwarové řešení.

Síťová IP kamera - použití IP kamer v kamerovém systému bude velkým přínosem, jelikož repertoár integrovaných součástí těchto kamer je na velmi vysoké úrovni. Tyto kamery zvládají spoustu požadovaných vlastností, a proto je nebude třeba dále řešit. Výhodou bezdrátových IP kamer je možnost umístit je na jakékoliv místo. IP kamery jdou nastavovat vzdáleně a komunikace s nimi je řádně zabezpečená. Cena těchto kamer je několikanásobně vyšší oproti ostatním kamerám. Závažným problémem je neexistující standard pro IP kamery, každý výrobce tak má jiné programové rozhraní. V neposlední řadě je třeba zmínit, že nastavení takových kamer není jednoduchou záležitostí a je potřeba k tomu někoho s dobrou znalostí informačních technologií.

GSM kamera - tyto kamery nejsou pro nás vhodné, poněvadž nejsou standardně připojitelné k počítači. Pouze některé specializované typy podporují připojení k počítači přes USB rozhraní. Z abstraktního hlediska pak na tyto kamery můžeme pohlížet jako na webkamery.

2.2 Mikrofon

Mikrofon je akusticko-elektrický převodník konvertující zvuk na elektrický signál. První mikrofon byl vyroben v roce 1877. Dnes nachází uplatnění v mnoha nejrůznějších oblastech, jako jsou telekomunikace, televize, rádia a v neposlední řadě, pro nás nejzajímavějších, kamerových a bezpečnostních systémech. Nejpoužívanější mikrofony používají tenkou membránu, která vibruje v závislosti na tlaku vzduchu. Tento pohyb je pak následně převeden na elektrický signál. Existují i jiné způsoby konverze, např. elektromagnetická indukce, piezoelektřina a modulace světla k vytvoření signálu mechanických vibrací. [11]

Část bezpečnostních kamer má mikrofon zabudován. Nebude tedy třeba mít mikrofon umístěný zvlášť. Audio výstup bývá přístupný přes RCA konektor. Nutnost mikrofonu v kamerovém systému záleží na typu prostředí, které budeme sledovat. Pro jednoduchost budeme předpokládat, že kamery budou obsahovat zabudovaný mikrofon. Jak bude zmíněno v další podkapitole, různé senzory a čidla reagují na zaznamenání události alarmem, této vlastnosti lze využít a detekovat takový zvuk pomocí mikrofonu. Následně bude vyhodnoceno, které čidlo tento alarm způsobilo a bude o této události informován uživatel. Nebude třeba mít tyto senzory připojeny přímo na centrální server. Bude stačit mít připojený mikrofon, který bude reagovat na jejich zvukové signály.

Obr. 2.6: Typický tvar mikrofonu [11]

2.3 Čidla a senzory

Čidlo je zařízení, které měří určitou fyzikální veličinu a převádí ji na signál, který může být dále využit v měřicích a řídicích systémech. Jako příklad si můžeme uvést snímání teploty, vlhkosti, rosného bodu a mnoha dalších.

2.3.1 Teplotní čidlo

Digitální teplotní čidlo umožňuje snadným způsobem měřit údaje o teplotě a přenášet ji do počítače. K přenosu dat se většinou používá jednoduchý ASCII protokol. Teplota je udávána přímo ve stupních Celsia (°C). Jednotlivá čidla se liší pouze rozhraním, přes které se připojuje k počítači, mohou tedy být propojena přes USB, síťový nebo standardní sériový port RS232. Komunikace přes všechna rozhraní probíhá velmi jednoduše a pro USB a sériový port je téměř totožná. Síťová neboli IP teplotní čidla se od zbylých dvou liší svojí komplexností a poskytovanými vlastnostmi. IP teplotní čidla můžeme částečně srovnat s IP kamerami, pokud tedy pomineme různé snímané veličiny. Taktéž obsahují webový server a je s nimi možno komunikovat pomocí několika různých komunikačních protokolů.

2.3.2 Kouřové čidlo

Kouřové čidlo je určeno k detekci vzniku požáru. Pro lokální varování má zabudovanou akustickou sirénu. Elektronické relé poskytuje výstup poplachového signálu a detektor je vybaven volitelnou funkcí paměti poplachu. Pravidelně je prováděn interní automatický test detektoru. K detekci kouře se využívá principu rozptylu infračerveného světla na pevných částicích v optické komoře. Detektory velmi dobře reagují na viditelný kouř vznikající doutnáním např. dřeva, papíru, textilu apod. Méně vhodné použití je detekce požárů a otevřených ohňů s malým vývinem kouře a rychlým nárůstem teplot (líh apod.). Pro tento případ bývají detektory vybaveny pomocným teplotním senzorem aktivujícím poplach, pokud dojde k překročení teploty v určitém rozmezí (v závislosti na rychlosti teplotního nárůstu). [25]

2.3.3 Plynový snímač

Senzory obvykle detekují všechny typy hořlavých plynů (zemní plyn, svítiplyn, propan, butan, acetylen, atd.) a reagují ve dvou úrovních koncentrace. Charakteristickými vlastnostmi takových snímačů jsou vynikající stabilita, vysoká citlivost, dlouhá životnost a malé rozměry. Přístroj signalizuje únik plynu opticky a akusticky. [25]

2.3.4 Čidlo rozbití skla

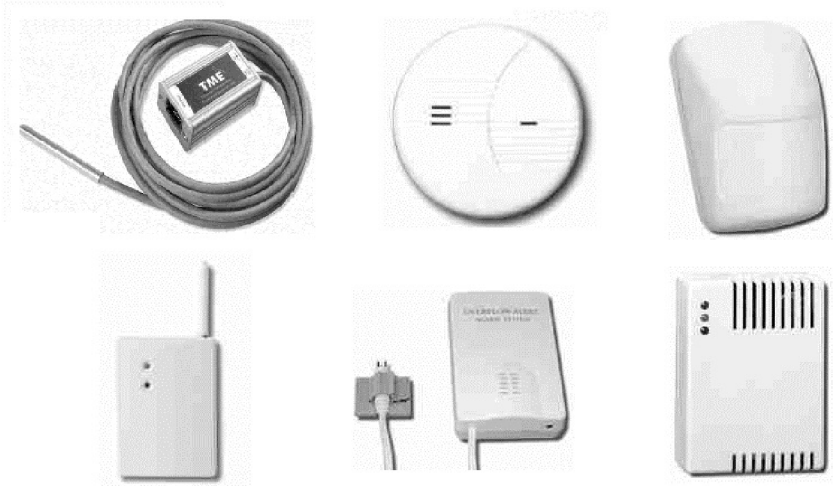
Čidlo slouží ke střežení prosklených ploch a detekuje jejich destrukci. K detekci užívá duální metodu, při které jsou vyhodnocovány nepatrné změny tlaku vzduchu v místnosti (náraz do skleněné výplně) a následné zvuky řinčení skla. Toto řešení vyniká vysokou spolehlivostí reakce při rozbití skleněné výplně. Citlivost detektoru lze často snadno nastavit podle vzdálenosti a rozměrů chráněných oken. Navíc bývá většina detektorů rozbití skla vybavena volitelnou paměťovou indikací. Připojují se k ústřednám poplachových systémů, ze kterých jsou napájeny. [25]

2.3.5 Čidlo pohybu

Pasivní infračervený snímač (PIR) pohybu osob je určen k prostorové ochraně objektů. Zpracovává signál metodou násobné analýzy signálu. Tím se dosahuje vynikající citlivosti a vysoké odolnosti proti falešným poplachům. [25]

2.3.6 Detektor zaplavení

Slouží k detekci zaplavení prostoru nebo překročení povolené výšky vodní hladiny. Indikace je akustická vestavěnou akustickou sirénou. Pro signalizaci do návazných systémů lze obvykle využít spínacího kontaktu. Vlastní sondy detektorů jsou vybaveny samolepící úchytkou s mechanickou aretací sond, umožňující její vyjmutí. Výrobek jde využít například v koupelnách, kuchyních a kotelnách. Případně při plnění nádrží, bazénů nebo akvárií. [25]



Obr. 2.7: Typické tvary čidel a detektorů. Zleva nahoře teplotní čidlo, kouřové čidlo, čidlo pohybu, čidlo rozbití skla, detektor zaplavení a plynový spínač [25], [19]

2.3.7 Vyhodnocení

Existuje velká řada různých čidel a senzorů. Některé senzory najdou využití v zabezpečovacím systému a jiné nikoliv. V této závěrečné podkapitole bude rozebráno, která čidla mohou najít využití v našem systému a která nikoliv. Použití čidel, která nejsou standardně připojitelná k počítači, je sporné. Využití mikrofonu jako prostředníka mezi těmito čidly není špatnou myšlenkou, ale v praxi obtížně realizovatelné.

Teplotní čidlo - v zabezpečovacím systému může mít podobné čidlo velmi důležitou roli. Budeme mít jistotu, že nedochází k zásadnímu výkyvu teplot, ať už jedním či druhým směrem. Můžeme například monitorovaný objekt chránit před zamrznutím.

Kouřové čidlo - je velmi spolehlivé zařízení pro detekci požáru apod. Místo tohoto čidla však lze jednoduše použít například čidlo teplotní i navzdory tomu, že účinnost takového čidla nebude zrovna nejvyšší. Velkou nevýhodou kouřového čidla je totiž nemožnost ho snadně připojit k počítači.

Plynový snímač - využití tohoto snímače je velmi diskutabilní. Pokud budeme v objektu skladovat nějaké hořlavé plyny, pak bude mít tento snímač praktické využití. Pro naše účely však o takovém čidle uvažovat nebudeme.

Čidlo rozbití skla a pohybu - použití podobných čidel je poměrně zbytečné, jejich funkce lze do jisté míry nahradit ostatními čidly a kamerami. Proto o nich v našem systému uvažovat nebudeme.

Detektor zaplavení - ač se na první pohled může zdát poměrně zbytečný, mohl by dobře sloužit např. jako varování před záplavami, které nejsou v České republice ničím výjimečným. Samozřejmě jej půjde využít i pro funkce popsané v podkapitole 2.3.6.

3 Komunikační protokoly

Hlavním problémem současných komplexních monitorovacích a zabezpečovacích systémů je neexistence standardu pro komunikaci s různými koncovými zařízeními. Dokonce ani koncová zařízení stejného druhu, např. kamery, nemají jasně definovaný standard pro komunikaci, a proto si každý výrobce tvoří vlastní komunikační protokoly. Rozvíjející se možností pro sjednocení komunikace se zařízeními je protokol *SNMP*, který je původně navržen pro správu síťových prvků. Současné bezpečnostní prvky však většinou do této skupiny již patří, a proto je v tomto protokolu budoucnost. Blíže o tomto protokolu v následující podkapitole, vzhledem k jeho důležitosti mu věnujeme zvláštní pozornost.

3.1 SNMP

Zkratka SNMP značí „*Simple Network Management Protocol*“, tedy v překladu jednoduchý protokol pro správu sítě. V dnešní době rozsáhlých a komplexních síťových systémů je potřeba protokolu pro jednotnou komunikaci se síťovými prvky, zjišťování jejich stavu, vstupů a výstupů a nastavovaní jejich parametrů. Jádro SNMP se skládá z několika základních operací, které dávají uživateli možnosti spravovat tato zařízení. Protokol SNMP se skládá ze tří základních verzí:

- SNMPv1 je počáteční verze tohoto protokolu. Je definován v RFC 1157. Bezpečnost verze 1 je založena na tzv. komunitách, což jsou hesla, umožňující jakýmkoliv SNMP aplikacím znajícím toto heslo přístup k informacím zařízení. SNMP standardně obsahuje tři typy komunit, a to komunitu *read-only* (pouze pro čtení), *read-write* (čtení i zápis) a tzv. *trapy* (pasti na události). Ačkoliv je SNMPv1 již zastaralá, je neustále hlavní SNMP implementací, kterou podporuje většina výrobců. [7]
- SNMPv2 tato verze se správně technicky nazývá SNMPv2c a je definována v RFC 1901 až RFC 1908. Od předchozí verze se liší rozšířeným repertoárem podporovaných funkcí, které kontrolují doručení zpráv, aby nedocházelo k jejím ztrátám.
- SNMPv3 je nejnovější verzí SNMP protokolu. Její hlavním přínosem je šifrovaný přenos dat. Přidává autentizaci a privátní komunikaci mezi jednotlivými komunikujícími entitami. Je definována v RFC 3410 až RFC 3418. Ačkoliv je SMNPv3 plnohodnotným standardem, mnoho výrobců zatím neposkytuje jeho podporu. [7]

SNMP pracuje na aplikační vrstvě internetového protokolu. Agent přijímá požadavky na UDP portu 161. Manažer může agentovi zprávy odesílat z jakéhokoliv volného portu a agent mu bude odpovídat na stejný port. Manažer přijímá notifikace a trapy na UDP portu 162. Agent může vygenerované zprávy odesílat z jakéhokoliv portu. [7]

3.1.1 Entity v SNMP

Jak již bylo zmíněno dříve, ve světě SNMP existují různé entity a to konkrétně agenti a manažeři. Níže je popsáno, co přesně tyto entity představují.

Manažer je serverová softwarová aplikace, která obstarává správu úloh v síti. Manažeři jsou zodpovědní za odesílání dotazů a přijímání trapů od agentů za cílem získat požadované informace. Tato informace může být využita k detekci události. *Trap* (3.1.4) je způsob agenta, jak manažerovi říct, že se něco stalo. Trapy fungují asynchronně nehledě na aktuálně odesílané dotazy na agenta. Manažer je zodpovědný za provedení nějaké akce při příjmu trapu. [7]

Agent je software, který běží na nějakém síťovém zařízení, které spravujeme. Může to být oddělený program (daemon) nebo program integrovaný v operačním systému. V dnešní době má většina SNMP agenta zabudovaného, což velmi usnadňuje práci systémových administrátorů. Agent podává manažerovi proměnné operační aspekty zařízení. Manažer může sledovat stav zařízení jednotlivých zařízení, a pokud se s nimi stane něco neočekávaného, tak patřičně zareaguje na danou situaci. Obrázek 3.1 ukazuje komunikační vztahy mezi agentem a manažerem. Je důležité mít na paměti, že dotazy a trapy mohou probíhat ve stejný okamžik. [7]

Obr. 3.1: Komunikace mezi manažerem a agentem

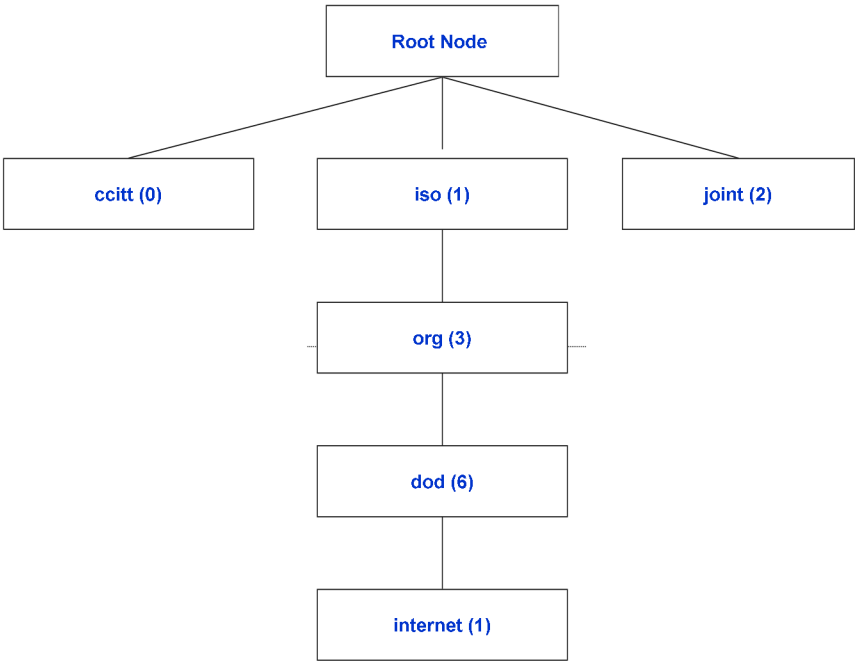
3.1.2 MIB databáze

Nyní je třeba vyřešit způsob, jak se bude přistupovat k jednotlivým informacím. Budeme k tomu využívat *SMI* (Structure of Management Information), což je struktura definující objekty a jejich chování. *MIB* (Management Information Base) je databáze těchto objektů, o kterých si agent vede záznamy. Jakákoliv statistická informace, která může být zpřístupněna manažerem, je uvedena v MIB. SMI nám říká, jakým způsobem deklarovat objekty, zatímco MIB jejich definici za použití SMI syntaxe. Objekt takové databáze má tři základní atributy: [7]

- *Jméno* neboli identifikátor objektu značený OID jednoznačně a unikátně definuje spravované objekty. Jména se obvykle objevují ve dvou podobách a to numerické a slovní. V obou případech jsou jména velmi dlouhá a je na aplikaci, aby poskytla uživateli příjemnější navigaci v těchto jménech. [7]
- *Typ a syntaxe* spravovaného objektu je definovaná za použití abstraktní notifikace syntaxe ASN.1. Je to způsob, jakým jsou reprezentována data mezi manažery a agenty v kontextu SNMP. Výhodou je, že tento způsob není závislý na použitém systému. [7]

- *Kódování* převádí jednu instanci spravovaného objektu na řetězec bytů použitím základních kódovacích pravidel (*BER*). BER definuje, jakým způsobem jsou objekty kódovány a dekódovány pro přenos přes transportní médium jako je síťové rozhraní. [7]

Spravované objekty jsou uspořádány do stromové hierarchie. Tento strom je základem pro pojmenovávání SNMP identifikátorů. Identifikátor objektu OID je složen ze série celočíselného typu, založených na jednotlivých uzlech stromu, oddělených tečkami. Existuje i přívětivější označení, kdy místo čísel jsou uváděny jmenné názvy uzlů, které jsou opět odděleny tečkami. Obrázek 3.2 ukazuje strukturu takového stromu, avšak pouze do určitého zanoření. Typický začátek OID pak vypadá následovně 1.3.6.1 neboli iso.org.dod.internet. [7]



Obr. 3.2: Ukázka stromové struktury MIB databáze

3.1.3 SNMP operace

Nejdůležitější částí SNMP protokolu jsou samotné operace, které nad tímto protokolem můžeme vykonávat. Jedná se o operace *GET, GETNEXT, GETBULK, SET, GETRESPONSE, TRAP, NOTIFICATION, INFORM* a *REPORT*. Škála podporovaných operací se liší podle jednotlivých verzí SNMP. Tyto operace jsou zabaleny do speciálního formátu, pomocí kterého manažeři a agenti komunikují. Tento formát se nazývá *PDU*. Nyní si popíšeme operaci GET, která pro nás má zvláštní význam. Zbylé operace využívat nebudeme, a proto se o nich dále zmiňovat nebudeme.

Operace *GET* je vyvolána manažerem, který ji odešle agentovi. Agent operaci přijme, a pokud je to možné, tak ji zpracuje. Pokud je agent přetížen, nemusí na tuto operaci odpovědět. Pokud ji však agent zdárně zpracuje, odešle zpět manažerovi zprávu s operací *GET RESPONSE* a ten ji zpracuje. Tento pochod je zobrazen na obrázku 3.1. Nedílnou součástí zprávy musí být i identifikátor *OID* v podobě vázané proměnné, což je vlastně OID a jemu přiřazená hodnota. [7]

3.1.4 SNMP trap

Trap je způsob, jak může agent říci manažerovi, že se něco stalo. Postup komunikace již byl nastíněn na obrázku 3.1. Trap zpráva je poslána na cílovou adresu, která musí být agentovi zadána. Tato adresa je typicky IP adresa manažera. Manažer neodesílá agentovi zpět žádnou potvrzovací zprávu. Jelikož však SNMP protokol pracuje na UDP, není zaručeno, že trap na cílovou adresu dojde. Nicméně při správně navržené síti by to neměl být problém. Obsahem trap zprávy je již zmíněné OID, které manažer musí znát, aby dokázal správně určit, jaká data přišla. To je většinou vyřešeno MIB tabulkou, kterou má manažer volně přístupnou. [7]

3.1.5 SNMP paket

Na závěr této kapitoly je popsáno, jak vypadá SNMP paket typu dotaz a odpověď viz obrázek 3.3. Společně s příkladem (obrázek 3.4) konkrétního příkladu jak by paket vypadal zaplněný hodnotami. Obrázek 3.5 ukazuje paket trap zprávy.

verze	název komunity	PDU typ	ID dotazu	error status	error ID	OID	hodnota

Tab. 3.3: Struktura SNMP paketu typu dotaz a odpověď

1	public	GET (0)	8	no error (0)	0	1.3.6.1.4.1.18248.1.1.1.0	NULL

Tab. 3.4: Příklad paketu směr manažer k agentovi

verze	název komunity	PDU typ	enter-prise	IP adresa agenta	gen. trap	spec. trapu	čas	objekt 1 hodnota 1	…

Tab. 3.5: Příklad paketu trap zprávy

3.2 Video for Linux

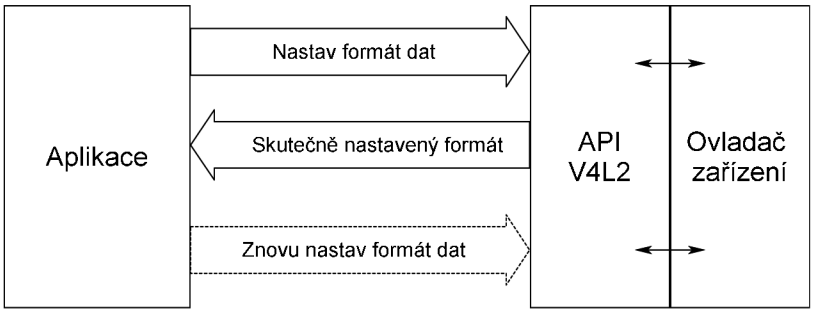
Tato podkapitola obsahuje popis knihovny sloužící pro komunikaci s video zařízeními pod systémy Linux. Navázání spojení se zařízením podporujícím V4L2 (*Video for Linux version 2*) pomocí API (aplikační rozhraní) probíhá v několika základních krocích. Níže uvedené kroky jsou volitelné a nemusejí být nutně prováděny v uvedeném pořadí. Záleží na typu zařízení a požadavcích na komunikaci. [6]

- Otevření zařízení
- Nastavení vlastností zařízení, jasu, standardu apod. a výběr audio / video vstupu
- Vyjednání formátu dat
- Vyjednání vstupně / výstupních metod
- Smyčka vstupů a výstupů
- Uzavření zařízení

Obecně mohou být zařízení podporující V4L2 otevřeny více než jednou. Uživatel může například nastavovat parametry spojení a mezitím již zachytávat snímky. Tohoto by se dalo využít v případě, kdy by uživatel používal kameru k detekování pohybu a současně pro nějakou jinou funkci. [6]

3.2.1 Formát dat

Formát dat se nastavuje vyjednáváním mezi aplikací, knihovnou a zařízením. Celé vyjednávání funguje na principu odeslání požadavku pro nastavení formátu dat API. API se pokusí nastavit formát dat. Pokud se to nepodaří, vyhledá nejbližší podobné nastavení a pokusí se je nastavit. V případě úspěšného nastavení se odešle zpět struktura obsahující skutečně nastavená data. Pak záleží na programátorovi, zda mu podobné nastavení vyhovuje anebo celý proces zopakuje s odlišným nastavením. Konkrétně můžeme chtít nastavit určité rozlišení snímaných dat. Pokud bude hodnota rozlišení nesmyslná nebo ji nebude podporovat zařízení, API rozhraní zvolí nejbližší podporované rozlišení. Celý proces je zobrazen na obrázku 3.6. [6]



Obr. 3.6: Vyjednávání formátu dat mezi aplikací a V4L2

3.2.2 Čtení/zápis dat

API definuje několik různých metod pro čtení a zápis ze / na zařízení. Zařízení samozřejmě musí alespoň jednu z těchto metod podporovat, jinak není možné čtení a zápis úspěšně provést. Standardními vstupně výstupními metodami jsou funkce `read()` a `write()`. Pokud však zařízení zmíněné funkce nepodporuje, může dojít kdykoliv k neočekávanému ukončení aplikace. Ostatní metody se musí vyjednat. To se provádí pomocí funkce `ioctl()` a je možné tímto způsobem vyjednat proudový přenos I/O dat s namapovanou pamětí nebo s uživatelskou vyrovnávací pamětí. Existují ještě další způsoby, ale ty pro naše cíle nemají žádný význam. Obecně je tedy každému souborovému deskriptoru zařízení přiřazena jedna metoda. Jedinou výjimkou jsou aplikace, které žádné data od kamery nevyžadují. [6]

Z hlediska našeho systému by bylo zřejmě nejjednodušší použít standardní funkce `read()` a `write()`. Bohužel však tuto metodu stejně jako metodu uživatelských bufferů spousta zařízení nepodporuje. Budeme proto využívat I/O metodu namapovaných pamětí. Tato metoda je pro navrhovaný systém velmi důležitá, a proto si ji nyní popíšeme blíže.

3.2.3 Mapovaná paměť

Kamera tuto I/O metodu podporuje, pokud podporuje proudový přenos dat. Kontrola podpory se provádí pomocí definovaných struktur. Celá problematika je přesněji popsána ve specifikaci [6]. Vzhledem k tomu, že existují dvě metody proudového přenosu dat, je ještě třeba ověřit, zda jsou dostupné vyrovnávací paměti pro odesílání požadavků. Proudový přenos dat je I/O metoda, kde jsou mezi aplikací a zařízením předávány pouze pointery na vyrovnávací paměti a data samotná nejsou kopírována. Toto chování je výhodné, jelikož šetří čas i prostor. Primárním účelem mapování je namapování vyrovnávacích pamětí v celé paměti zařízení na adresový prostor aplikace. Pamětí zařízení je v našem případě video paměť s uloženými daty z kamery. Ačkoliv je tato I/O metoda dlouhodobě tou nejefektivnější, spousta dalších zařízení podporuje proudový přenos dat pomocí alokovaných vyrovnávacích pamětí v hlavní paměti s přímým přístupem do paměti. [6]

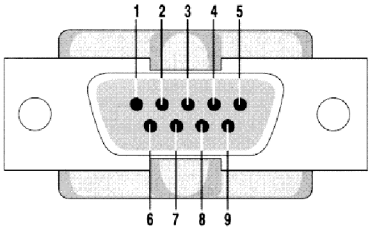
Zařízení může podporovat mnoho různých sad vyrovnávacích pamětí. Každá sada je identifikována jednoznačnou typovou hodnotou vyrovnávací paměti. Tyto sady jsou na sobě nezávislé a každá sada může obsahovat různé typy dat. Pro přístup k různým sadám ve stejný čas je třeba mít pro každou sadu různý deskriptor zařízení. [6]

Pro alokaci vyrovnávacích pamětí zařízení musí aplikace odeslat požadavek na tyto paměti, a to konkrétně na počet těchto pamětí a jejich typ. Stejným způsobem je možno i uvolnit alokovanou paměť, za předpokladu, že žádná z vyrovnávacích pamětí již není namapovaná. Předtím než aplikace může zpřístupnit vyrovnávací paměti, je třeba je namapovat do adresového prostoru aplikace pomocí `mmap()` funkce. Umístění vyrovnávacích pamětí v celé paměti zařízení může být určeno pomocí dotazu. Následně je v podobě struktury vrácena délka dat a jejich offset. Offset a délka nesmí být modifikovány. Vyrovnávací paměti jsou alokovány ve fyzické paměti na rozdíl od virtuální paměti, která může být odložena na disk. Aplikace by měla uvolnit vyrovnávací paměti, jakmile je to možné, pomocí `munmap()` funkce. [6]

3.3 Teplotní čidla

3.3.1 Sériový a USB port

Na obrázku 3.7 je zobrazen sériový port s očíslovanými piny. V tabulce 3.8 jsou popsány piny portu, které budeme využívat pro komunikaci s čidlem.



Pin	Signál v PC	Funkce
2	RxD	Přijímání dat z čidla
4	DTR	Napájení a ovládání čidla
5	GND	Signálová zem

Obr. 3.7, tab. 3.8: Znázornění využití pinů portu RS232 [18]

Nyní si popíšeme samotný protokol, se kterým budeme komunikovat se zařízením. Teplotní čidlo je napájeno ze sériového / USB portu, do kterého je připojeno. Jakmile je na portu nastaven signál DTR, čidlo změří teplotu a pošle ji do počítače v ASCII formátu jako textový řetězec. Pokud je signál DTR stále aktivní, čidlo měří a odesílá teplotu v pravidelném intervalu. Každý odměr je signalizován červenou kontrolkou na konektoru čidla. Měřící konec je v jednoduchém provedení určen zejména pro měření teploty vzduchu. [18] Výše popsané je zobrazeno v přehledné tabulce 3.9.

Nastavení v PC	Funkce	Formát dat
Nastavení signálu DTR	Aktivace čidla, okamžité odeslání dat	<znaménko><3 znaky – celé><.> <1 znak – desetiny><C> Např.: +025.3C
Signál DTR trvale nastaven	Periodické posílání dat	

Tab. 3.9: Popis komunikace mezi počítačem a čidlem

3.3.2 Síťové rozhraní

Komunikace se síťovými čidly je založena na protokolu SNMP, který je popsán v kapitole 3.1. Důležitým parametrem tohoto spojení je OID zařízení, pod kterým se nachází sledovaná hodnota. Identifikátory OID hodnot teplot v MIB databázích jsou uvedeny v tabulce 3.10. Jsou uvedeny OID pouze nejčastěji dostupných čidel.

OID	Formát dat
1.3.6.1.4.1.18248.1.1.1.0	Teplota krát 10
1.3.6.1.4.1.22626.1.5.2.3.0	
1.3.6.1.4.1.18248.18.5.2.1.1.6.1	

Tab. 3.10: Identifikátory do MIB databáze na hodnotu aktuální teploty

3.4 Kamery

Následující podkapitola obsahuje názorný popis komunikace počítače s kamerami připojenými přes různá rozhraní. Bohužel neexistuje jednotný způsob, kterým by se toho dalo dosáhnout. Proto si tento problém můžeme rozdělit podle provedené analýzy na dvě základní skupiny. Do jedné skupiny patří kamery připojitelné pomocí PCI a USB rozhraní a druhé IP kamery. Vzhledem k jisté náročnosti získávání dat z první skupiny využijeme linuxové specifikace verze 2 (V4L2) [6] pod licencí GNU pro komunikaci s těmito zařízeními. Druhá skupina bude využívat komunikace na protokolu TCP/IP s aplikačním programovým rozhraním (API) typickým pro každého výrobce. Taková komunikace bude založena na protokolu HTTP (hypertextový přenosový protokol).

3.4.1 PCI a USB kamery

Kamery tohoto typu se pod linuxovými systémy nachází ve složce `dev` a pojmenovávají se `video0` až `video255`. Pro využití specifikace V4L2, a s ním spojeného aplikačního rozhraní je třeba, aby zařízení tuto specifikaci podporovalo. Tato specifikace však zvládá celou řadu zařízení napříč různými výrobci a různými typy a verzemi. Proto je mezi vývojáři velmi oblíbená a vůbec nejrozšířenější mezi specifikacemi tohoto druhu. Podrobný popis komunikace pomocí specifikace V4L2 se nachází v kapitole 3.2.

Koncepčně zařízení podporující proudový přenos dat udržují dvě fronty vyrovnávacích pamětí, příchozí a odchozí. Oddělují synchronní zachycení snímku nebo omezují zpoždění jinými procesy, čímž snižují pravděpodobnost ztráty dat. Fronty jsou organizovány jako FIFO (první dovnitř, první ven), vyrovnávací paměti budou dány na výstup v pořadí, v jakém přišly do FIFO. [6]

Zařízení může vyžadovat minimální počet bufferů pro její chod. Mimo to neexistuje žádná hranice, která by limitovala počet vyrovnávacích pamětí. Vyrovnávací paměti mohou být zpracovány v jiném pořadí, než v jakém byly zaplněny a zařízení uvolněné vyrovnávací paměti může plnit v jakémkoliv pořadí. Index vyrovnávací paměti má tedy pouze funkci jako identifikátoru. Pro zachytávání snímků je obvyklé nejdříve zařadit do fronty všechny namapované vyrovnávací paměti, pak začít zachytávat snímky a začíst číst data. Tady aplikace čeká, dokud nemůže být naplněná vyrovnávací paměť vyjmuta z fronty. Jakmile data nejsou potřebná, zařadí paměť znovu do fronty. [6]

Pro spuštění nebo zastavení zachytávání aplikace volá metody pro spuštění či zastavení proudového přenosu dat. Zastavení proudového přenosu dat jako vedlejší efekt odstraní všechny vyrovnávací paměti ze všech front. [6]

3.4.2 IP kamery

Různé druhy kamer podporují různé protokoly, příkladem si můžeme uvést protokoly HTTP(S), SNMP, TCP, UDP. Vzhledem k co možná nejobecnějšímu návrhu využijeme aplikační programové rozhraní založené na HTTP protokolu. Nastává problém, kdy drtivá většina kamer sice HTTP protokol podporuje, ale každý výrobce kamer má jinak postaven systém HTTP status kódů. Pro názornost a jednoduchost si uvedeme pouze aplikační rozhraní IP kamer AXIS, které jsou na trhu zastoupeny v největší míře [4]. Počítač komunikuje s integrovaným HTTP serverem, a to pomocí předávaných parametrů. Ty jsou předávány v hlavičce HTTP metodou GET nebo POST. Syntaxe hlavičky s parametry je uvedena níže:

GET /axis-cgi/param.cgi?<argument>=<value>[&<argument>=<value>...] HTTP/1.1

param.cgi	- typ brány přes kterou budeme přistupovat k datům
argument	- platný parametr brány
value	- hodnota parametru

Pomocí těchto parametrů je kameru možno nastavovat, upravovat její vlastnosti a hlavně získat aktuálně snímaný obraz (případně i zvuk) z kamery. Z hlediska bezpečnosti není podobný způsob zrovna ideální, a proto jsou zavedeny tři druhy přístupových práv. Ve zkratce se jedná o práva na prohlížení, nastavování a administrátorský přístup k zařízení. Po úspěšném zpracování parametrů kamerou je odeslána odpověď, která je dána status kódem a má tvar:

HTTP Code: <code>	*code*	- HTTP status kód
Content-type: <type>	*type*	- typ hodnoty v těle
Body:		
<text>	*text*	- přenášená data

3.4.2.1 Příjem snímku z kamery

Ukážeme si, jak bude vypadat komunikace mezi počítačem a kamerou za účelem získání jednoho či více snímků z kamery. Využijeme znalosti a popis z předchozího odstavce. Uvedený příklad vyžaduje kameru s podporou kódování snímků do formátu JPEG. Před zahájením příjmu snímku je třeba se autorizovat pomocí jména a hesla. Parametry je nutno odesílat metodou GET, syntaxe pak tedy bude následující:

GET /axis-cgi/jpg/image.cgi?camera=1&resolution=640x480 HTTP/1.1

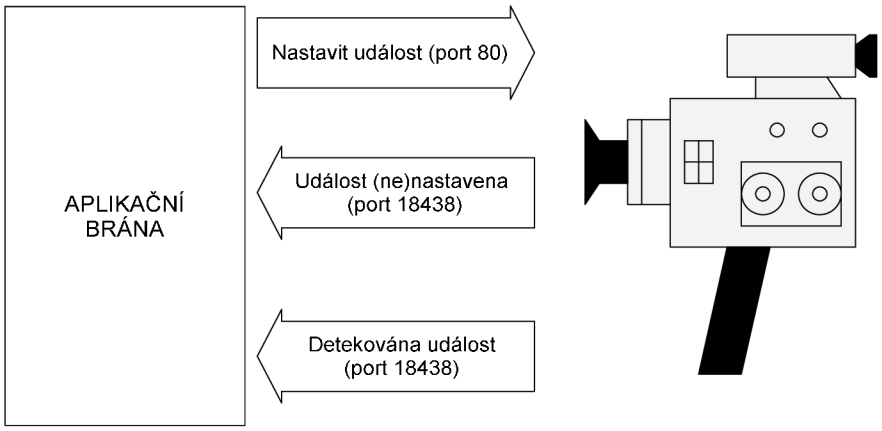
Pokud byl požadavek úspěšně zpracován, je vrácen jeden snímek ve formátu JPEG. Obsah zprávy je typu „*multipart/x-mixed-replace*“ a každý obrázek je ohraničen kódovým řetězcem „*<boundry>*“. Přijatá zpráva by tedy vypadala následovně:

HTTP Code: 200 OK
Content-Type: multipart/x-mixed-replace; boundary=<boundary>
Body:
--<boundary> <image>

kde pole *<image>* je:
Content-Type: image/JPEG
Content-Length: <image size>
<JPEG image data>
--<boundary>
<image>

3.4.2.2 Nastavení událostí

Pro detekci pohybu, překročení hladiny šumu apod. je třeba nastavit na IP kameře událost. Kamera při detekci pohybu odešle na zadanou síťovou adresu a port zprávu o nastalé události. Celý postup komunikace je zobrazen na obrázku 3.11. Brána nejprve předá kameře parametry pro nastavení události. Kamera následně odešle potvrzení nebo zamítnutí o vytvořené události. Pokud je událost úspěšně nastavena a kamera detekuje pohyb, je odeslána asynchronní zpráva na aplikační bránu obsahující informace o události. Přesný popis parametrů pro nastavení událostí je uveden zde [3].



Obr. 3.11: Komunikace mezi IP kamerou a aplikační bránou

4 Analýza informování uživatele

Tato kapitola pojednává o možnostech informování uživatele o narušení bezpečnosti. Existuje celá řada možností. Vybereme si pouze typické zástupce a o každém si něco v následujících podkapitolách napíšeme.

4.1 E-mail

Zasílání e-mailu zadanému adresátovi je pod linuxovými systémy bezproblémové, využijeme k tomu řešení třetí strany. Knihoven či programů pro posílání e-mailů je velmi mnoho. Můžeme si je rozdělit do dvou skupin podle potřeby externího účtu pro odesílání e-mailu. Uvedeme si typického zástupce z každé skupiny dostupného pod GPL licencí.

- *sendmail* - typicky součástí linuxových distribucí, není třeba externího účtu, ovládání z příkazové řádky, složitá konfigurace.
- *jwsmtp* - robustní knihovna napsána v jazyce C++ pro posílání e-mailů z jakékoliv platformy, odesílání skrze externí účet, autentizace, bezpečné spojení.

Pro poslání e-mailu se na první pohled jeví aplikace `sendmail` jako vhodnější volba, jelikož není třeba e-mail posílat přes externí účet. Na druhou stranu to může být nevýhodou, protože takový e-mail může být v mnoha případech označen jako nevyžádaná pošta. Dále zapojení již hotové aplikace do zdrojového kódu není zcela ideální možností. Proto byla zvolena knihovna `jwsmtp`, která je pro naše požadavky sice příliš komplexní a všechny parametry nebudou využity, ale pro bezchybný chod programu, lepší přehlednost řešení atd. bude výhodnější zapojení této knihovny.

4.2 SMS zprávy

Existuje několik způsobů, jakými lze odeslat SMS zprávu z počítače. Uvedeme si tři základní způsoby, jakými je toho možno dosáhnout.

- *Webové SMS portály* - zprávy z těchto portálů lze posílat zdarma přímo z počítače.
- *GSM modul k počítači* - externí zařízení obsahující simkartu s nabitým kreditem. Zprávy se z počítače posílají skrz tento modul.
- *Mobilní e-mail* - někteří operátoři podporují tzv. mobilní e-maily, každému telefonnímu číslu přiřadí unikátní e-mailovou schránku. Pokud na tuto schránku přijde e-mail, je automaticky přesměrován a uživateli přijde onen e-mail v podobě SMS zprávy.

První možnost nabízí velmi zajímavé řešení, jelikož stačí pouze připojení k internetu a posílané SMS zprávy jsou zdarma. Překážkou tohoto řešení ale je přílišná náročnost na implementaci, protože by bylo třeba stahovat obsah tohoto portálu a využívat některou z aplikací pro detekci čísel v obrázku, které je třeba zadat pro odeslání zprávy. Možné řešení se nabízí v podobě využití komplexního softwaru třetí strany. Bohužel většina těchto softwarů jsou komerční a proto pro nás nepoužitelné.

Využití GSM modulu je reálnou variantou, která by si v našem systému jistě našla své místo pro případné rozšíření. Pro náš systém budeme uvažovat nejjednodušší variantu a tou je mobilní

e-mail. Využijeme řešení obstarávající odesílání e-mailů. Nevýhodou tohoto řešení je doba doručení e-mailů posílaných na mobil. Doba doručení velmi kolísá. Může se dokonce jednat až o desítky minut, střední doba se však pohybuje okolo 20 sekund.

4.3 Okamžité posílání zpráv

V našich zeměpisných šířkách jsou využívány především dva systémy pro okamžité posílání zpráv. Patří mezi ně komerční *ICQ* a volně šiřitelný *JABBER*, založený na otevřeném protokolu *XMPP* (Extensible Messaging and Presence Protocol). Komerční systém je pro náš systém nevhodný, a proto se budeme zabývat pouze systémem XMPP.

Existuje řada knihoven pro práci nad XMPP protokolem systému JABBER. Nejvýhodnějším kandidátem se zdá být knihovna Gloox naprogramována v jazyce C++, založená na událostech. Nebude problém takovou knihovnu zapojit do návrhu a systému pro ohlašování událostí.

4.4 Webové požadavky

Další možnost jak informovat uživatele je pomocí tzv. webových požadavků. Celá komunikace probíhá na aplikační vrstvě pomocí HTTP protokolu. Principiálně tento způsob funguje tak, že se vytvoří spojení mezi zabezpečovacím systémem a vzdáleným počítačem (serverem). Serveru se odešle GET požadavek obsahující parametry reprezentující informace o nastalé události. Záleží pak na vzdáleném serveru, jakým způsobem parametry zpracuje a vyhodnotí. Požadavek dodržuje syntaxi protokolu *CGI* (Common Gate Interface), který je přímo určen k propojení externích aplikací a webových serverů. Níže vidíme přesnou syntaxi odesílaného požadavku, následovanou názornou ukázkou konkrétního požadavku odesílaného webovému serveru.

GET /mass/?<parametr>=<hodnota>[&< parametr >=< hodnota >...] HTTP/1.1
GET /mass/?nazev=dev/video0&cas=6.5.2010&data=94.228.25.16/detect/cap.mjpeg HTTP/1.1

4.5 Vyhodnocení

Možnosti informování jsou různé. E-maily a okamžité posílání zpráv jsou z hlediska přístupnosti a jednoduchosti nejvýhodnější. Zvolené varianty je možno různě kombinovat. Např. je-li adresát on-line, lze použít okamžité posílání zpráv, v opačném případě raději e-mail. Pokud není e-mail doručen dostatečně včas, je vhodné ještě poslat SMS zprávu. Jednoduchou a přitom velmi zajímavou možností jsou již zmíněné webové požadavky. Další zajímavou možností by mohlo být prozvánění, které je zdarma a uživatele zastihne víceméně kdekoliv. Naopak posílání zpráv na pager se již v dnešní době jeví jako poměrně zastaralá záležitost.

Ať už použijeme jakoukoliv variantu informování uživatele, obsah posílané zprávy bude významově vždy stejný. Zpráva bude obsahovat informaci o tom, které koncové zařízení tuto událost vyvolalo a odkaz na data s tím spojená.

5 Bezpečnostní sítě

Bezpečnostní sítě jsou úzce spjaty s pojmem CCTV, což je odvozenina z anglického pojmu „*Closed Circuit Television*“. Tomuto názvu odpovídá český ekvivalent uzavřené televizní okruhy. Obraz z CCTV okruhu je přístupný pouze těm, kteří jsou připojení přímo do okruhu. Protikladem je veřejné televizní vysílání, kdy je obraz dostupný všem, kteří mají ve vlastnictví televizor.

Často se pro CCTV kamerové systémy používá rovněž starší pojem průmyslová televize nebo průmyslové kamery, což vyjadřuje původní použití CCTV kamer převážně pro průmyslové aplikace. Postupně se však začala průmyslová televize používat rovněž ve školství a zdravotnictví, ke sledování dopravy, ke kontrole výrobních procesů atd. Největší uplatnění nalezly CCTV kamerové systémy při zabezpečení nejrůznějších objektů. Proto se můžeme často setkat rovněž s pojmem bezpečnostní kamery nebo zabezpečovací kamery. Kamerové systémy jsou využívány při zabezpečení vnějších i vnitřních prostor, k zabezpečení velkých firemních objektů nebo v soukromé sféře (např. zabezpečení rodinného domu pomocí video-vrátného). Často jsou bezpečnostní kamery nasazovány jako doplněk klasického elektronického zabezpečovacího systému, čímž se zjednodušuje a zefektivňuje zabezpečení objektu. [8], [21]

Pod pojmem kamerový systém si v praxi můžeme představit několik kamer většinou stejného typu (typy kamer viz kapitola 2.1), které tvoří jistou soustavu kamer. Ta je pak připojena k nějakému zařízení zpracovávající data viz další kapitola. Taková zařízení se pak většinou liší jen svou vybaveností a na tom závislou cenou.

5.1 Zpracování dat z koncových zařízení

5.1.1 Záznam dat

CCTV kamerové systémy používají speciální videorekordéry umožňující dlouhodobý bezobslužný záznam obrazu z bezpečnostní kamery. Dříve používané analogové páskové videorekordéry jsou postupně vytlačovány digitálními videorekordéry, které ukládají obrazová data na pevný disk. Digitální videorekordéry bývají často vybaveny video-serverem, který umožňuje vzdálený přístup k rekordéru přes LAN / Internet. [8], [21]

Jinou možností digitálního záznamu je standardní PC vybavené videokartou a příslušným softwarem. Tyto kamerové systémy pro počítače sestávají obvykle z 4kanálové PCI videokarty a speciálního software, který umožňuje sledování a záznam kamer na pevný disk počítače. Videokarty jsou obvykle modulární, takže např. při instalaci čtyř 4kanálových videokaret lze na počítači sledovat a nahrávat až 16 kamer.[8]

5.1.2 Konverze dat

Další možností je snímky z kamer vůbec nezaznamenávat. Velkou výhodou tohoto řešení je odstranění nutnosti zařízení pro záznam dat. Pokud má být systém smysluplný, je třeba zachycená data okamžitě zpracovávat. Mohou být například ihned převáděny do výstupního zařízení, jako je monitor. Nebo je možné pořízený záznam předat na vstup programu pro rozpoznání podoby apod. A na základě toho reagovat příslušnou akcí, nejspíše informováním uživatele. Úskalím takového způsobu je však relativní náročnost na počítač zpracovávající taková data. Případné zpracování několika signálů z několika kamer ve stejném čase by mohlo být velmi náročné a z celkového hlediska i zbytečně obtížné. Jako nejvýhodnější se tedy jeví získávání dat z jednotlivých koncových zařízení v určitém časovém intervalu několika sekund a jejich následným zpracováním. Lze předpokládat, že i spotřeba při podobném získávání dat bude nižší, což je v dnešní době jistě nezanedbatelné hledisko. Při narušení bezpečnosti by tento přístup znamenal velké množství zaznamenaných snímků, a proto se v tomto případě jeví jako výhodnější pořizovat nepřetržitý záznam dat, ale po omezenou (uživatelem danou) dobu.

Použitá čidla na rozdíl od různých typů kamer neposkytují žádnou obrazovou hodnotu. Jejich výstupem je buď hodnota naměřené fyzikální veličiny anebo spuštění alarmu. Zaznamenat taková data, vzhledem k jejich velikosti, na harddisk počítače není žádným problémem.

5.2 Existující řešení

Na trhu existuje spousta různých řešení monitorovacích nebo zabezpečovacích systémů. Patří mezi ně mechanické zábranné systémy, elektronické zabezpečovací systémy, elektrická požární signalizace a hlavně z našeho pohledu nejzajímavější kamerový systém, který již byl rozebrán v úvodu kapitoly. Monitorovacích kamerových systémů je na trhu celá řada. Každá firma zabývající se tímto oborem má vytvořen vlastní systém. Je proto velmi těžké se v těchto systémech orientovat. Podobné systémy mají velmi dobrou podporu všech různých druhů kamer. Pomocí některých systémů je možno kamery vzdáleně ovládat a využít tak plné funkčnosti těchto kamer. Nevýhodou většiny těchto systémů je přílišné zaměření na kamerové systémy. Náš systém se tento nedostatek snaží odstranit podporou různých typů čidel a detektorů.

Mechanické zábranné systémy (*MZS*)

Úkolem mechanických zábranných systémů je narušitele při jejich překonávání co nejvíc zdržet. Nejlépe do doby, kdy je možno provést například fyzický zásah. Všechny mechanické zábranné systémy jsou v konečném čase překonatelné. Tato doba závisí především na jejich kvalitě a umístění. Určitý vliv na ni má rovněž znalost konstrukce ze strany pachatele, druh použitých nástrojů při překonávání nebo například možnost použít elektřinu. [15]

Elektronický zabezpečovací systém (*EZS*)

Elektronický zabezpečovací systém EZS slouží k upozornění na narušení hlídaného objektu. Děje se tak pomocí akustické a optické signalizace, tj. poplachové sirény. Siréna umístěná uvnitř objektu působí na narušitele psychicky, zatímco venkovní siréna dá o poplachu vědět širokému okolí. Samotný zabezpečovací systém EZS tedy nezabrání narušení objektu a měl by proto být použit jako doplňková ochrana k prvkům mechanických zábran. Právě tyto zábrany hrají rozhodující roli v zabezpečení majetku. Je důležité, aby pachateli co nejvíce zkomplikovaly průnik a prodloužily tak dobu narušení. [15]

Elektrická požární signalizace (*EPS*)

Úkolem elektrické požární signalizace je upozornit na vznikající požár v objektu. Reaguje na jevy charakteristické pro požár, tj. kouř, nárůst teploty a plameny. Existuje velké množství typů lišících se principem detekce (optické, tepelné, kombinované) a provedením. [15]

Monitorovací systémy (*MS*)

Monitorovací systémy poskytují uživateli přehled o aktuálním dění v zobrazovacím poli kamer. Tyto systémy jsou většinou dány aplikací běžící na centrálním serveru. Tato aplikace poskytuje obraz z jedné či více kamer a umožňuje uživateli tyto kamery nastavovat. Zvláštním případem MS jsou síťové kamery, které mají všechny tyto součásti integrované a poskytují tak vynikající dohledový systém a jejich snadnou správu.

6 Návrh

Návrh monitorovacího a zabezpečovacího systému vychází z provedené analýzy. Nejprve je třeba specifikovat požadavky na celkové chování systému. Bude nutné navrhnout systém, který zvládne komunikaci s různými typy koncových zařízení a poskytne uživateli jednotný a jednoduchý přístup k těmto zařízením. Rovněž budou vybrány konkrétní typy zařízení, na kterých bude systém stavěn. Při návrhu je třeba zvláště dbát na celkovou výkonnost systému, snadnou instalaci a jednoduchou možnost rozšíření.

6.1 Požadavky

Hlavním bodem návrhu jakéhokoliv systému je určení požadavků na jeho funkčnost. Celý systém má sloužit jako aplikační brána mezi klasickou TCP/IP sítí a různorodou sítí obsahující různá koncová zařízení jako jsou kamery, mikrofony a čidla (teplotní, kouřové atd.). Na základě zaznamenaných událostí (pohyb, hluk, požár) z těchto koncových prvků je možné odeslat upozornění uživatelům (SMS zpráva, e-mail, JABBER, webový požadavek) a zaznamenat data ze zařízení, které událost vyvolalo. Každé zařízení bude možno umístit do libovolné místnosti s tím, že zařízení v jedné místnosti budou tvořit jednu skupinu. Systém musí být možné vzdáleně spravovat a musí existovat možnost, jak prohlížet aktuální data z koncových zařízení. Zaznamenaná data bude potřeba ukládat a je tedy vhodné, aby existovala podpora pro dostupný druh databáze, ve které budou data uložena.

Systém musí minimalizovat nežádoucí stavy, jako jsou falešné alarmy. Tyto alarmy vznikají v případě nesprávného vyhodnocení narušení bezpečnosti. Falešný pozitivní alarm nastává v případě, že systém detekuje narušení i v případě, kdy k žádnému nedošlo. Falešně negativní alarm nastane v opačném případě, kdy systém nedetekuje problém při narušení bezpečnosti. Při návrhu a implementaci bude dbáno na obecnost systému vzhledem k možným rozšířením systému. Je důležité, aby byl návrh objektově orientovaný a modulární. Systém bude zaměřen na linuxové platformy.

6.2 Soustavy kamer nebo čidel

Pod soustavou koncových zařízení (kamer, čidel) si můžeme představit skupinu jednoho či více zařízení stejného typu. V následujících podkapitolách rozebereme výhody a nevýhody použití různých typů zabezpečovacích soustav.

6.2.1 Soustava webkamer

První soustava je tvořena webkamerami. Tato soustava je pro nás nejzajímavější. Limitem takové soustavy je počet dostupných USB konektorů na centrálním serveru. Není však problémem rozšířit hardwarovou výbavu serveru o rozšiřující USB kartu, která většinou obsahuje další čtyři USB konektory. Pro naše řešení budeme uvažovat menší počet webkamer, než je počet dostupných USB konektorů na serveru.

Víme tedy, přes jaké rozhraní budeme s webkamerami komunikovat, nebude tedy problém využít již popsaného komunikačního protokolu (kap. 3.2) pro získání zobrazovaných dat. Aplikace postavena na tomto protokolu by měla být nezávislá na druhu použité webkamery. Pro náš systém budeme předpokládat soustavu tvořenou z webkamer Logitech Webcam C200, která poskytuje dostačující technické parametry [17].

6.2.2 Soustava detektorů kouře a zaplavení

Tyto soustavy se budou poněkud lišit od ostatních soustav. Nejsou totiž standardně připojitelné k počítači. Propojení s počítačem by bylo možné docílit za pomoci volně použitelných párových svorek (GBS). Podobný způsob by se však spíše hodil pro elektronický zabezpečovací systém. Pro nás je tento způsob propojení nevhodný. Proto využijeme toho, že každá naše kamera bude obsahovat i mikrofon. Podobná zařízení totiž obsahují akustickou sirénu, která v případě detekce události začne vydávat zvuk. Na tento zvuk pak bude reagovat mikrofon kamery. Takové zařízení může být tedy umístěno prakticky kdekoliv v slyšitelném poli některého z mikrofonů. Problém nastává při samotné detekci zvuku akustické sirény. Může docházet k různým rušivým vlivům, např. šumu apod.

Takto navržená soustava by měla být zcela nezávislá na typu jednotlivých detektorů. Popsané řešení by se spíše mohlo týkat dalšího vývoje systému. Při návrhu budeme s touto variantou počítat a usnadníme tím případné rozšíření systému. Pro náš systém si zvolíme běžně dostupné detektory. Kouřový detektor SD-280 je určen pro domy a menší prostory, je vhodný pro použití v našem systému. Přesná specifikace tohoto detektoru je uvedena zde [13]. Obdobně zvolíme i detektor zaplavení, tedy konkrétně typ LD-63HS se specifikací zde [14].

6.2.3 Soustava teplotních čidel

Další soustavou jsou teplotní čidla využívající k propojení s počítačem sériový port, síťové rozhraní nebo USB. Současné počítačové sestavy již standardně sériový port neobsahují. Jedním z možných řešení tohoto problému je zapojení rozšiřující RS232 karty do serveru, jedna taková karta obvykle obsahuje alespoň dva takové porty. Stejně tak by mohl být problémem nedostatek USB portů, vzhledem k tomu, že pomocí nich budou připojovány jak čidla, tak webkamery.

Úskalím této soustavy je mnoho různých druhů rozhraní, přes které je možno se připojit k serveru. Komunikace tedy bude muset být oproti jiným čidlům komplexnější. Pro konkrétní návrh systému musíme vzít tedy v úvahu několik různých druhů čidel. Nejčastěji používané teplotní čidlo typu TM [18] se vyrábí v několika provedeních právě podle typu rozhraní. Data přicházející z takových čidel budou tedy stejná, což nám velmi usnadní práci s čidly.

6.2.4 Soustava analogových kamer

Soustava analogových kamer se k počítači připojuje pouze pomocí videokarty, která musí být součástí centrálního serveru. Omezením takové karty je, že k ní lze připojit současně maximálně čtyři analogové kamery. Současným omezením také je, že standardní počítače mohou obsahovat „pouze“ čtyři takové videokarty. Dostáváme se tedy k číslu šestnáct, které nám omezuje maximální počet připojitelných kamer k serveru.

Z hlediska získávání dat z analogové kamery je pro nás důležitější typ videokarty a její funkce než typ samotné kamery. Proto tedy zvolíme standardní analogovou kameru, která bude obsahovat i mikrofon. Tyto požadavky splňuje barevná kamera YK-564K [9]. Videokartu volíme dle schopnosti detekovat pohyb, tedy VGUARD-RT4 [24], která dokonce podporuje i kompresi videa v reálném čase.

6.2.5 Soustava IP kamer

Poslední soustavou je soustava bezdrátových a síťových kamer. Tato soustava je z hlediska navrhovaného systému tou nejzajímavější a do budoucna rozhodně nejperspektivnější. Výhody takových kamer již byly zmíněny v předchozích kapitolách. K vytvoření fungující soustavy bezdrátových a síťových kamer je potřeba zvážit hlavně jejich propojení s centrálním serverem. Prvotní možností by bylo připojit každou síťovou kameru zvlášť k centrálnímu serveru. Podobné řešení by se v praxi vyplatilo pouze při velmi malém počtu kamer. Vytvářet podobnou bezdrátovou síť by bylo takřka nemožné.

Další možností by mohlo být použití jednoho či více síťových *směrovačů,* do kterých by byl zapojen jak centrální server, tak síťové kamery. Bezdrátové kamery by pak mohly být připojeny k centrálnímu serveru, který by tvořil přístupový bod. Toto řešení se zdá být vcelku bezproblémové, nevýhodou takového řešení by však byla nutnost nastavit statické IP adresy jednotlivých koncových zařízení. Tuto variantu uvažovat nebudeme, ale z hlediska funkčnosti celého systému by neměla představovat problém.

Využijeme možnosti propojení kamer se serverem, jak je uvedeno na obrázku 6.2. Mezi kamery, ať už síťové či bezdrátové, a centrální server umístíme bezdrátový směrovač, který vytvoří jednotnou síť bezdrátových a síťových kamer. Společně s kamerami se na směrovač připojí i server. Toto řešení nám poskytne dynamické přidělení adres. Nebude tedy třeba nastavovat síťové adresy jednotlivých kamer zvlášť.

Stejně jako u ostatních kamer, požadujeme integrovaný mikrofon v kameře. Částečně nás tato podmínka limituje při výběru vhodné kamery. Zvolíme tedy síťovou IP kameru AXIS Q1755 se specifikací uvedenou zde [2].

6.2.6 Vyhodnocení

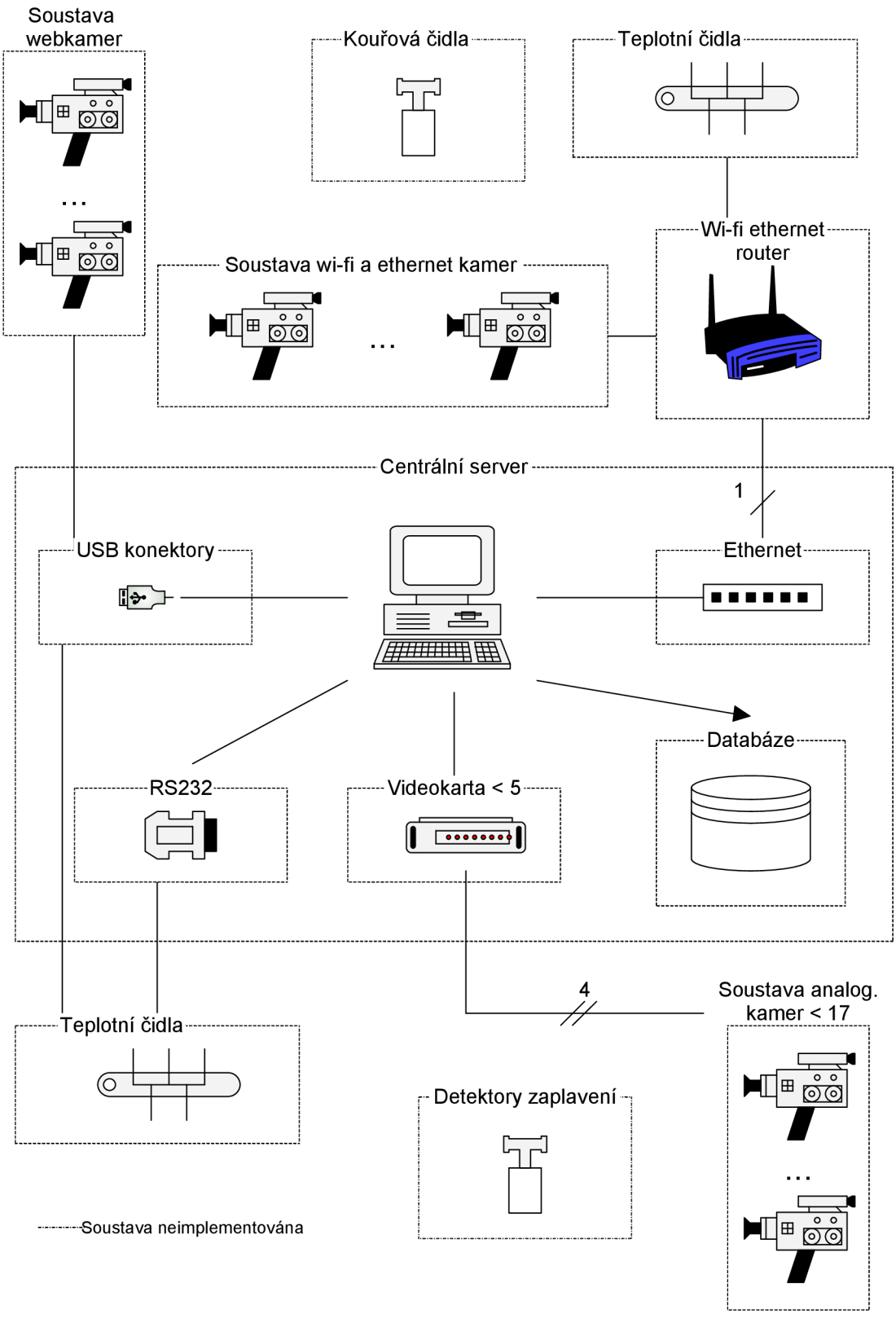
Byly rozebrány různé typy soustav koncových zařízení, jejich výhody a nevýhody. Následně byly vybrány konkrétní typy zařízení patřící do daných soustav. Tato zařízení budou použita při návrhu a implementaci systému. Nejedná se však rozhodně o jediná podporovaná zařízení. Jedná se pouze o názornou ukázku několika zařízení, která mají šanci najít své uplatnění v našem systému. Jednotlivá zařízení a jejich vlastnosti jsou přehledně znázorněna v následující tabulce.

Soustava	Typ	Rozhraní	Formát dat	Technická specifikace
Anal. kamery / videokarty	YK-564 / VGUARD-RT4	PCI	Mpeg-4	[9] / [24]
Webkamery	Logitech Webcam C200	USB	VGA	[13]
IP kamery	AXIS Q1755	LAN	Mjpeg / h.264	[2]
Teplotní čidla	Čidlo TM	RS232 / USB / LAN	ASCII (℃)	[18]
Detektory kouře	SD-280	Mikrofon	Zvukové vlnění	[13]
Detektory zaplavení	LD-63HS	Mikrofon	Zvukové vlnění	[14]

Tab. 6.1: Přehled konkrétních typů zařízení použitých v systému

Pro názornou ukázku propojení soustav s centrálním serverem byl vytvořen obrázek 6.2, na kterém je zobrazeno jasné rozvržení soustav v monitorovacím a zabezpečovacím systému. Při návrhu tohoto schématu bylo vycházeno z analýz provedených v podkapitolách 2.1.5, 2.3.7 a 3.2. Na obrázku je šest na sobě nezávislých monitorovacích systémů. Z jejich vzájemné nezávislosti plyne, že kterákoliv ze soustav může a nemusí být zapojena do celkového systému. Bude záležet na konkrétním umístění, požadovaných vlastnostech apod. Při návrhu systému budeme uvažovat zapojení všech soustav. Dosáhneme tak co možná největší obecnosti. Při samotné implementaci však pomineme kouřová čidla a detektory zaplavení. Tyto soustavy nejsou připojené přímo k centrálnímu serveru. Připojují se k němu nepřímo, díky jejich akustickým sirénám (jak již bylo zmíněno v analýze). Podobný způsob není zrovna ideální, a proto nebudou implementovány.

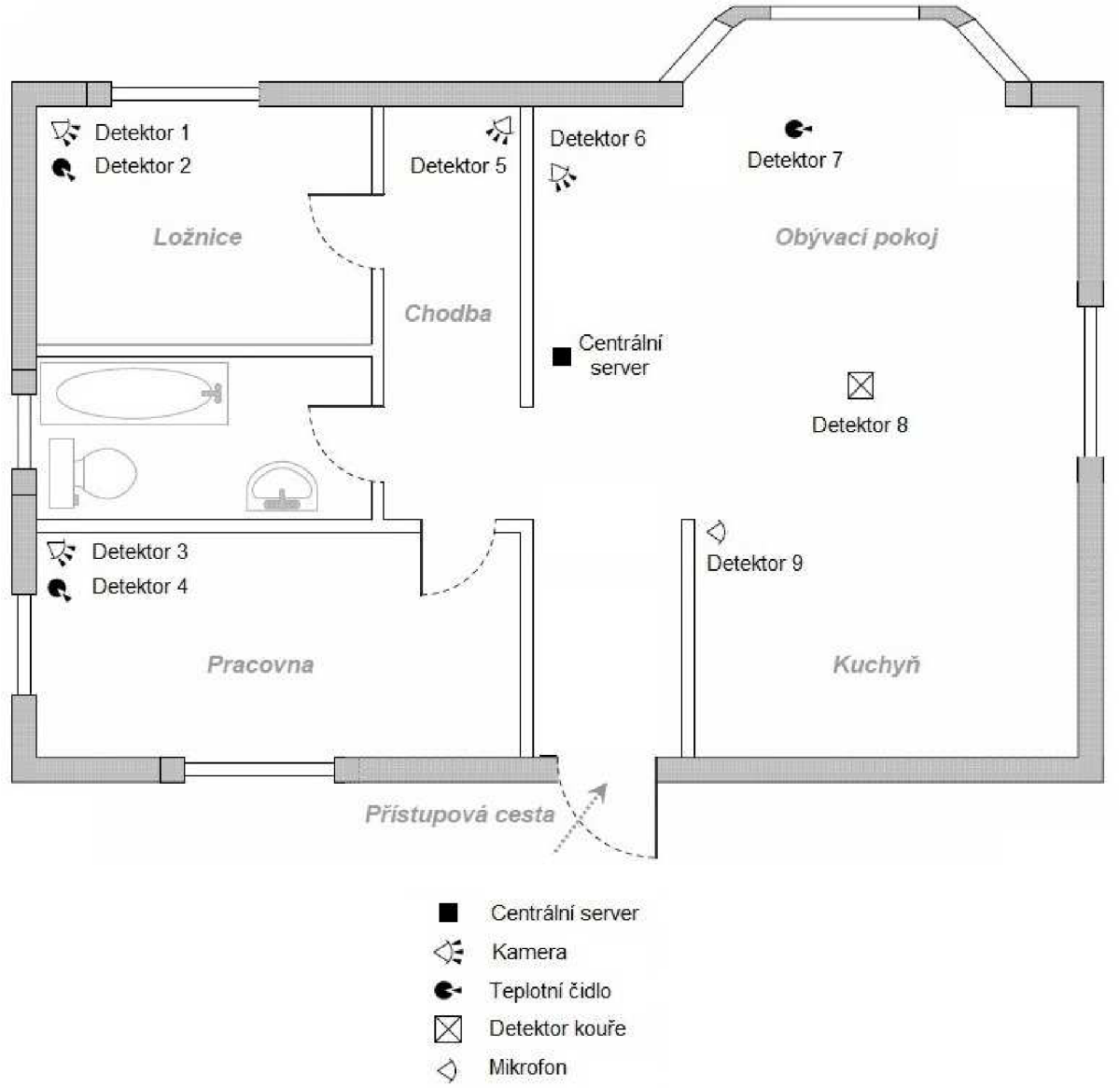
Dalším velmi důležitým bodem, který vidíme na obrázku, je databáze, která bude součástí centrálního serveru. Bude sloužit pro uchování zpracovaných dat a vytvářet spojovací bod mezi zařízeními a uživatelem.



Obr. 6.2: Rozložení soustav monitorovacího a zabezpečovacího systému

6.3 Skupiny zařízení

Při návrhu zabezpečovacího systému je třeba vyřešit polohu a umístění jednotlivých zařízení, tedy vytvoření určitých skupin. Tyto skupiny budou v praxi reprezentovat místnost, ve které budou umístěny. Pokud nějaké koncové zařízení detekuje narušení bezpečnosti, informuje o tom nepřímo ostatní zařízení ve skupině a následně pak všechna zařízení začnou zaznamenávat data. V případě, že některé zařízení ze skupiny bude ve stavu off-line, není možné začít se záznamem dat, proto se automaticky na omezenou dobu přepnou do provizorního on-line stavu, kdy je možno spustit záznam dat. Jako ideální rozpoložení se zdá umístění každého typu koncového zařízení do skupiny, konkrétně tedy teplotní čidlo, detektor kouře a IP kameru. V praxi by však takový systém byl příliš robustní, na obrázku 6.3 vidíme možné rozložení jednotlivých detektorů v rodinném domě, chatě ap.



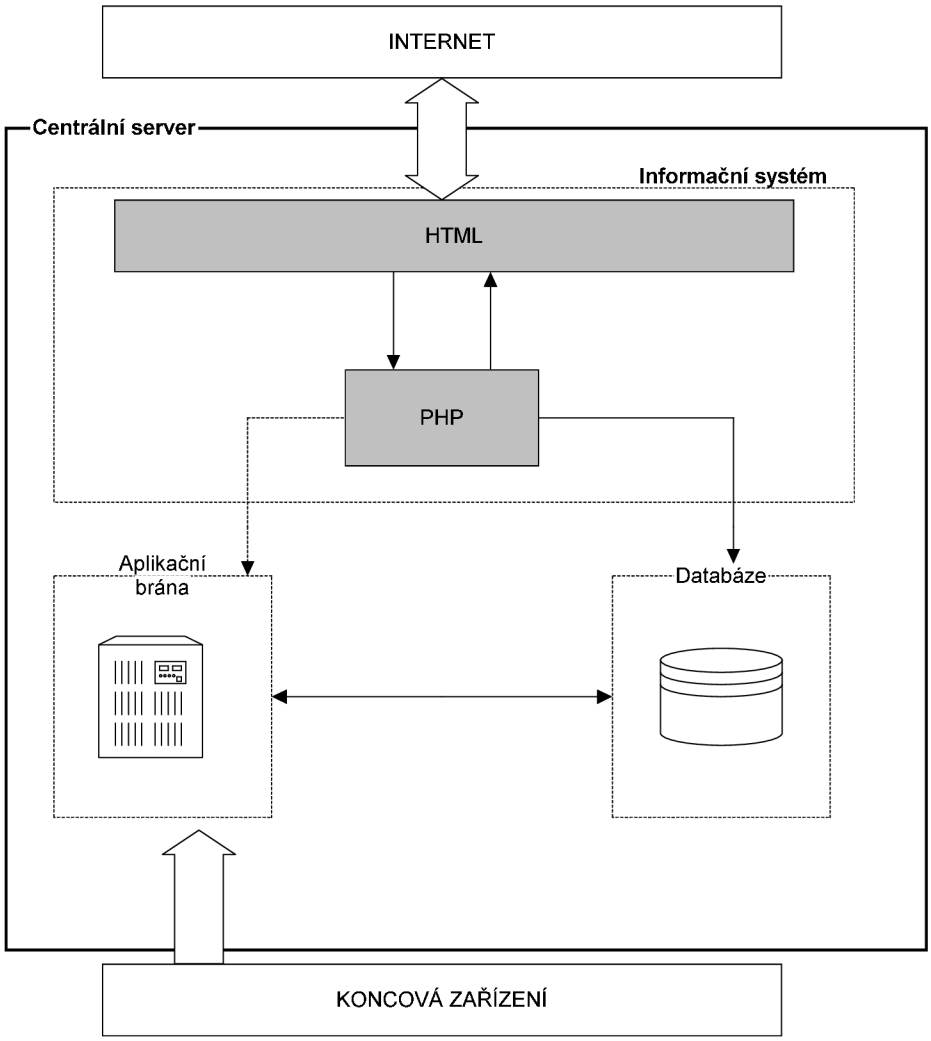
Obr. 6.3: Možné rozložení detektorů v rodinném domě [15]

6.4 Aplikační brána

Aplikační brána, jindy také nazývána jako *aplikační proxy*, je aplikace nacházející se mezi koncovým uživatelem a internetem. Brána zachycuje příchozí a odchozí pakety a funguje jako proxy server bránící jakémukoliv přímému spojení mezi důvěryhodným serverem nebo klientem a nedůvěryhodným hostem. Veškerá komunikace přes aplikační bránu probíhá formou dvou spojení, klient se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Aplikační brána přijímá pouze pakety generované službami, které jsou navrženy pro kopírování, přeposílání a filtrování. Pokud je síť založena na aplikačních branách, příchozí a odchozí pakety nejsou dostupné službám, pro které neexistuje brána. [22]

Brána prochází a filtruje jednotlivé pakety, namísto jednoduchého kopírování a přeposílání skrz bránu. Aplikačně specifické proxy kontrolují každý paket procházející bránou. Ověřují obsah paketu na sedmé (aplikační) vrstvě síťového OSI modelu. Proxy může filtrovat specifickou informaci nebo konkrétní příkaz aplikačního protokolu. Aplikační brána filtruje informace na vyšší vrstvě OSI modelu než obyčejný statický či dynamický paketový filtr. Automaticky vytvářejí potřebná filtrovací pravidla, což usnadňuje jejich konfiguraci oproti paketovým filtrům. Nevýhodou aplikačních bran je zejména vysoká náročnost na použitý hardware. Aplikační brány jsou schopny zpracovat mnohem nižší množství spojení a rychlosti než paketové filtry a mají mnohem vyšší latenci. [22]

Pokud tedy aplikujeme výše zmíněnou definici aplikační brány na náš navrhovaný monitorovací systém, dostaneme dvě oddělené sítě. První sítí budou soustavy jednotlivých typů koncových zařízení, jak je vidět na obr. 6.1, a druhou síť bude tvořit TCP/IP spojení s centrálním serverem viz obr. 6.4. Nevýhody zmíněné v předchozím odstavci by se v našem navrhovaném systému nemusely dostavit. Očekáváme totiž připojení velmi malého počtu uživatelů a data přenášená mezi kamerami a serverem budou jistým způsobem limitována, viz podkapitola 5.1.2. Výhodou pro nás naopak bude, že jednotlivé sítě budou od sebe odděleny a tudíž se značně zvýší bezpečnost celkového systému. Samotná aplikační brána pak v systému na obr. 6.3 bude služba běžící na centrálním serveru, ke které se budou připojovat jednotlivá koncová zařízení. Brána bude přijímat zprávy a data z jednotlivých zařízení, zpracuje je a uloží do databáze či na pevný disk. Uživatel se pak připojí do informačního systému, který mu poskytne snadný přístup k uloženým datům.

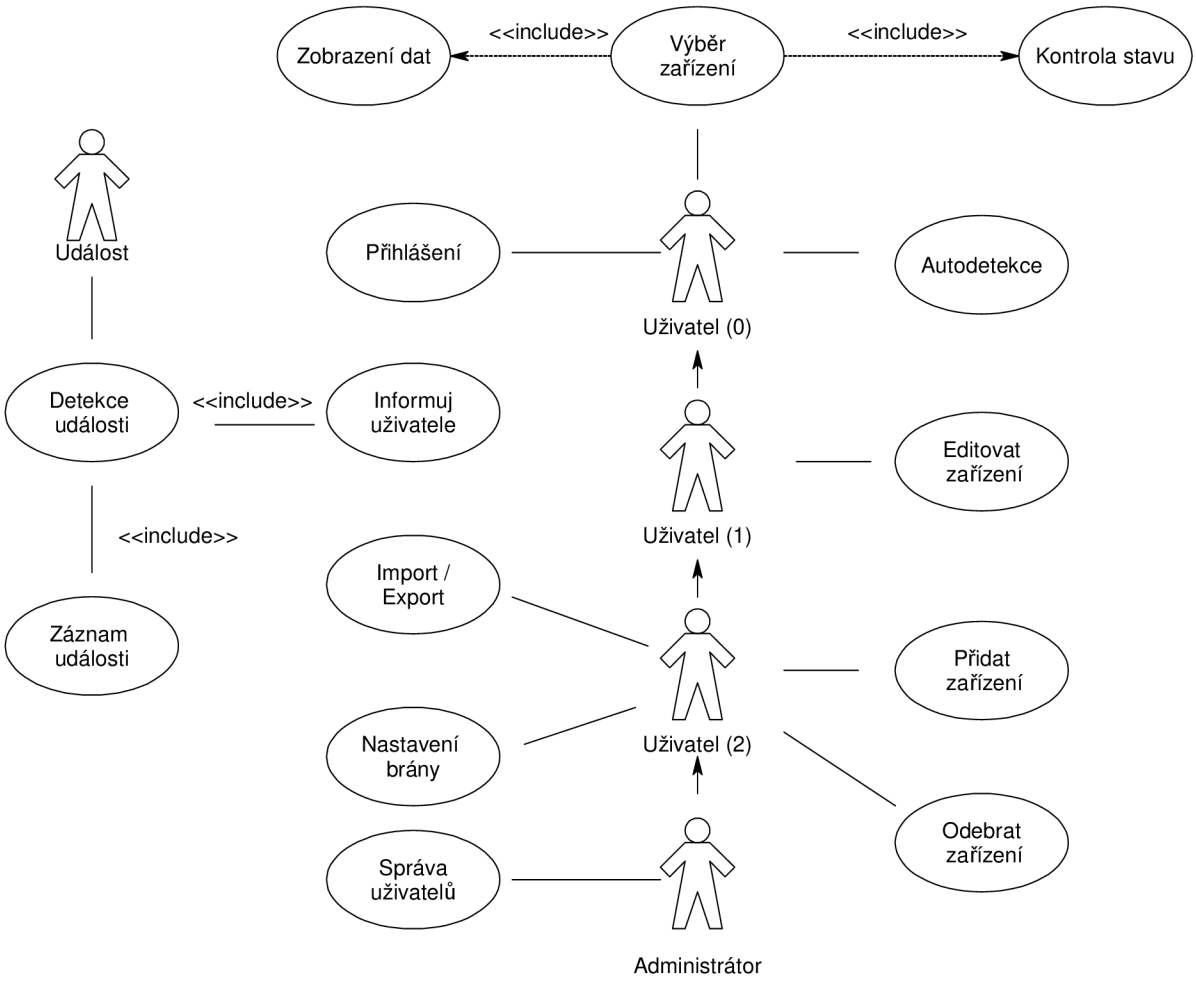


Obr. 6.4: Připojení koncových uživatelů k centrálnímu serveru

Webové stránky budou tvořeny menším informačním systémem. Systém bude evidovat informace o jednotlivých zařízeních, konkrétně tedy identifikátor, adresu v síti, rozhraní zařízení, obnovovací frekvenci a typ akce, která bude provedena při detekci pohybu. Budou se zaznamenávat informace o jednotlivých událostech jako je čas, identifikátor a aktuální hodnota zařízení. Administrátor bude moci přidávat a odebírat uživatele atd. Tyto požadavky budou v podobě různých modelů zpracovány v následujících kapitolách.

6.5 Diagram případů užití

Na obrázku 6.5 je zobrazen návrh případů užití našeho systému. Nachází se zde tři hlavní entity (událost, uživatel a administrátor). Uživatel je pak rozdělen na další tři entity, kdy každá určuje určitý stupeň práv. Administrátor dědí vlastnosti od ostatních uživatelů a navíc má možnost správy těchto uživatelů. Diagram názorně ukazuje, jaké bude mít uživatel možnosti při vstupu do systému. Mezi nejdůležitější bod patří výběr zařízení a s ním spjatá kontrola stavu zařízení s následným zobrazením aktuálních dat ze zařízení. Jak vidíme na diagramu, uživatel se bude muset přihlásit do systému, bude moci nastavit aplikační bránu, importovat a exportovat nastavení a v neposlední řadě spravovat připojená zařízení. Konkrétní případy užití jsou popsány v následující podkapitole.



Obr. 6.5: Diagram případů užití monitorovacího a zabezpečovacího systému

6.5.1 Specifikace případů užití

Primární vlastností specifikace případů užití je ukázka konkrétní funkčnosti systému. Je zde popsáno několik typických kroků, které může uživatel či administrátor zvolit při vstupu do systému.

Případ použití: Přidání uživatele
ID: 1
Stručný popis: Administrátor vyplní formulář a systém vytvoří nového uživatele.
Primární aktéři: Administrátor
Sekundární aktéři: Uživatel
Předpoklady: Daný uživatel ještě v systému není registrován.
Hlavní tok: 1. Případ užití se provede, když Administrátor vybere „správu uživatele“ a systém zobrazí dialog pro editaci uživatelů. 2. Dokud Administrátor nezadá všechny povinné informace, není možné uživatele přidat. 3. Systém zkontroluje vložené údaje, a pokud jsou neplatné, Administrátor musí formulář vyplnit znovu. 4. Systém vytvoří účet.
Následné podmínky: 1. Byl vytvořen účet daného uživatele.
Alternativní tok: 1. Tento zákazník již je vytvořen.

Tab. 6.6: Specifikace případu užití přidání uživatele do systému

Případ použití: Přihlášení
ID: 2
Stručný popis: Uživatel se obdrženým přihlašovacím jménem a heslem přihlásí do systému
Primární aktéři: Uživatel
Sekundární aktéři: Žádný
Předpoklady: Uživatel je registrován
Hlavní tok: 1. Případ užití začíná, když uživatel vyvolá dialog pro přihlášení do systému. 2. Zde zadá přihlašovací jméno a heslo. 3. Systém přihlásí uživatele.
Následné podmínky: 1. Přihlášení Uživatele do systému. 2. Zpřístupnění funkcí systému pro uživatele s odpovídajícím oprávněním.
Alternativní tok: 1. Zadány chybné přihlašovací údaje. 2. Storno

Tab. 6.7: Specifikace případu užití přihlášení uživatele do systému

Případ použití: Prohlížení zařízení
ID: 3
Stručný popis: Uživatel si vybere požadované zařízení v systému a nechá si zobrazit aktuální data.
Primární aktéři: Uživatel
Sekundární aktéři: Žádný
Předpoklady: 1. Uživatel je přihlášen 2. Zařízení je v systému a je aktivní.
Hlavní tok: 1. Případ užití se provede, pokud Uživatel vyvolá zobrazení detailu zařízení. 2. Systém zkontroluje, zda je zařízení aktivní a uživatel přihlášen. 3. Systém zobrazí stránku s informacemi o zařízení a data s ním spojená.
Následné podmínky: Zobrazení informace a data zařízení z databáze.
Alternativní tok: Požadované zařízení není aktivní.

Tab. 6.8: Specifikace případu užití prohlížení zařízení v systému

Případ použití: Přidat zařízení
ID: 4
Stručný popis: Uživatel přidá nové zařízení do systému.
Primární aktéři: Uživatel
Sekundární aktéři: Žádný
Předpoklady: 1. Uživatel je přihlášen 2. Zařízení je v systému a je aktivní.
Hlavní tok: 1. Případ užití se provede, když Administrátor vybere „přehled zařízení“ a systém zobrazí formulář pro správu zařízení. 2. Dokud Administrátor nezadá všechny povinné informace, není možné pokračovat. 3. Systém podle zadaných hodnot zkontroluje, zda je zařízení aktivní. 4. Systém přidá zařízení do databáze.
Následné podmínky: Byla vytvořena nová položka koncového zařízení v databázi.
Alternativní tok: Požadované zařízení není aktivní.

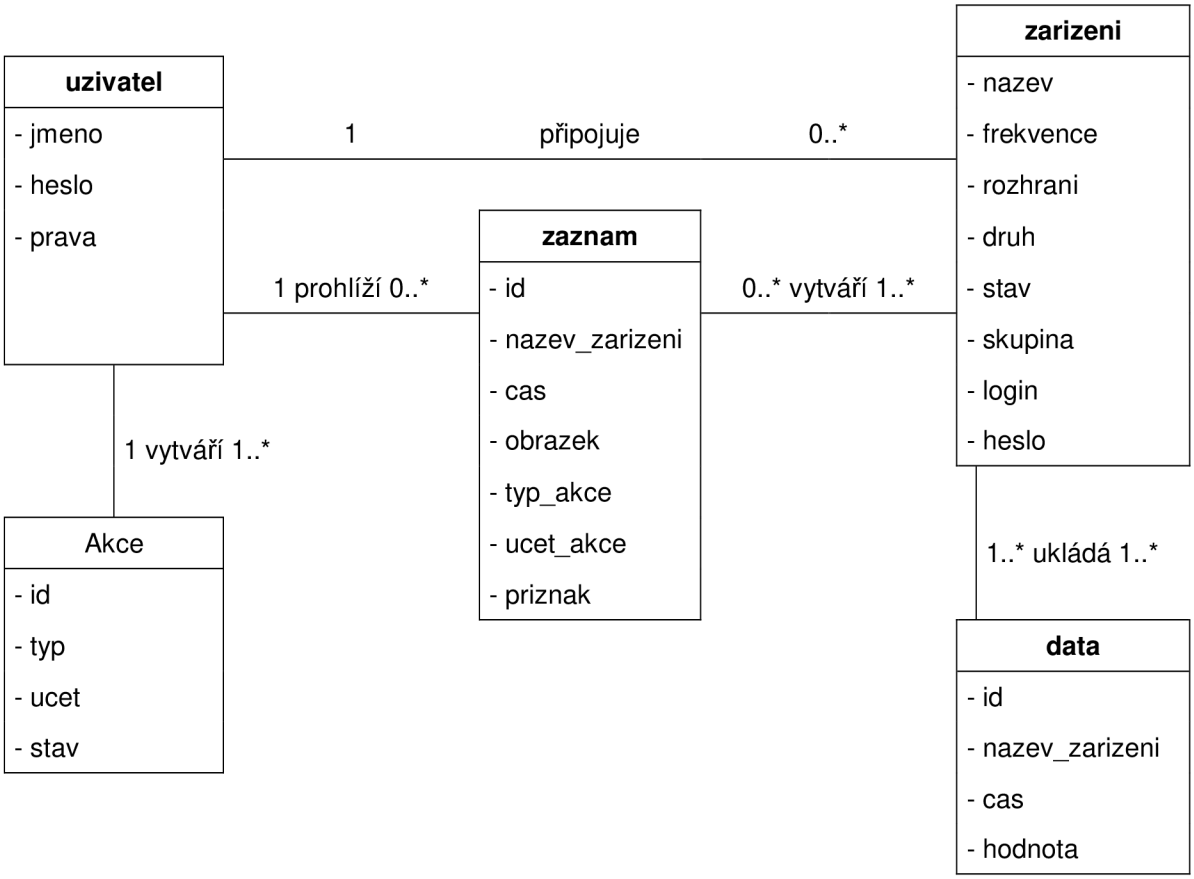
Tab. 6.9: Specifikace případu užití přidání zařízení do systému

6.6 Třídy

Třída je základní konstrukční prvek objektově orientovaného programování. Vytváří most mezi abstrakcí a uživatelsky definovanými typy. Kombinuje reprezentaci dat a metody pro manipulaci s daty do jednoho společného balíčku. Slouží pro vytváření objektů. Vlastnosti tříd mohou odlišovat jednotlivé objekty. V objektově orientovaném návrhu je třída nejvíce specifickým typem objektu ve vztahu ke konkrétní vrstvě. [20]

Abstraktní třída je podobná té klasické s tím rozdílem, že z ní nemůžeme vytvářet objekty. Abstraktní třída má implementované pouze některé ze svých deklarovaných metod. Tyto metody se na všech objektech vykonají stejně. Neimplementované metody se pak liší ve zděděných podtřídách této abstraktní třídy. Zjednodušeně můžeme říct, že se jedná o vzor pro vytváření konkrétních skupin tříd. [20]

6.6.1 Konceptuální diagram tříd

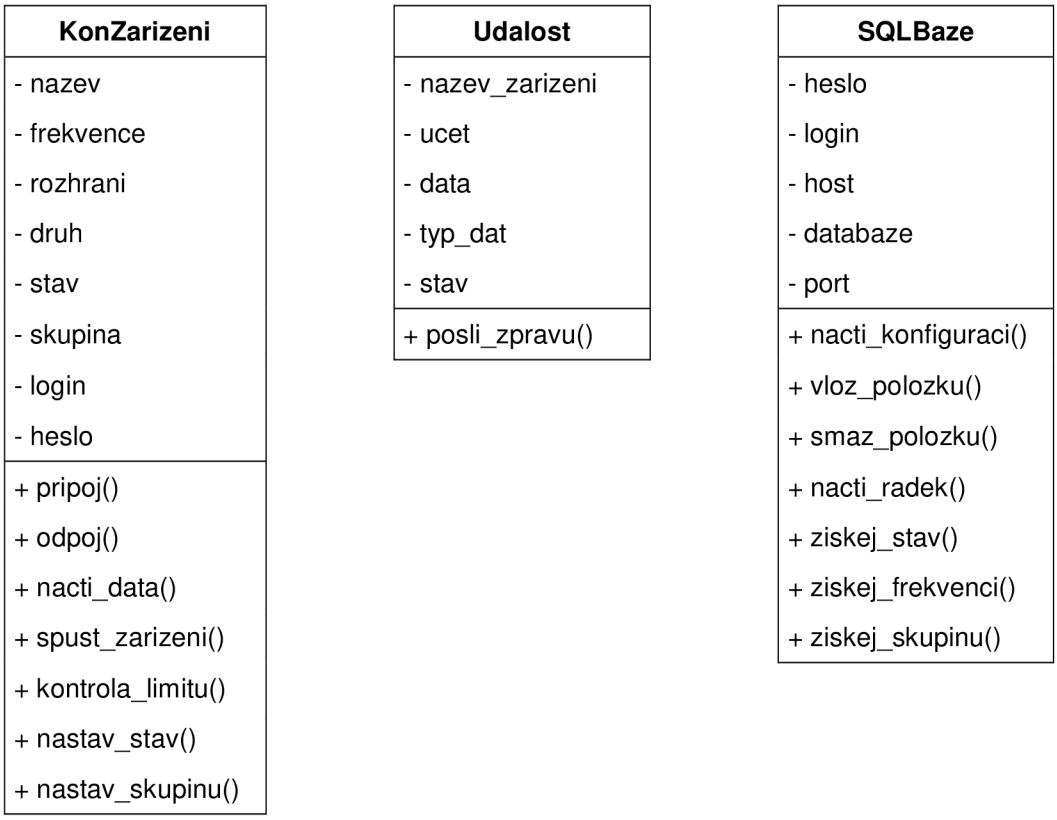


Obr. 6.10: Konceptuální diagram tříd navrhovaného sytému

Konceptuální model uvedený na obrázku 6.10 naznačuje popis dat v databázi nezávisle na jejich samotném uložení. Model představuje formální popis modelované reality. Vidíme zde jednotlivé entity, vtahy a atributy. Tento model bude sloužit k vytvoření schémat a jejich následné transformaci na databázové schéma.

6.6.2 Návrh prototypů tříd

Pokud vezmeme v potaz náš monitorovací systém, vyskytuje se v něm několik objektů, které již byly popsány v předchozích kapitolách. Jsou to tedy analogové kamery, IP kamery, webkamery a teplotní čidla. Vzhledem k tomu, že do budoucna předpokládáme rozšiřování projektu, bude pravděpodobně výhodnější vytvořit jednu abstraktní třídu společnou pro všechna koncová zařízení místo několika různých tříd pro každý druh zařízení. Na obr. 6.11 jsou zobrazeny prototypy tříd, které budou použity při implementaci samotné aplikační brány. Jedná se tedy o třídy zaštiťující práci s koncovými zařízeními, SQL databází a odesílání událostí.



Obr. 6.11: Prototypy tříd navrhovaného systému

7 Implementace

Při implementaci monitorovacího a zabezpečovacího systému bylo vycházeno z provedené analýzy a návrhu. Byly zvoleny konkrétní typy zařízení, na kterých bude aplikace implementována a testována. V praxi jsem pak použil pouze některé z nich, protože podobné vybavení je poměrně drahé a tak jsem ke všem neměl přístup. Existuje však celá řada emulátorů a různých metod, které mi nedostupná zařízení nahradily.

Před samotným začátkem bylo třeba zvolit vhodný programovací jazyk, ve kterém bude aplikační brána napsána. Nejvýhodnějším jazykem pro aplikaci podobného rázu se ukázal být programovací jazyk C++, který je objektově orientovaný a splňuje požadavky pro tvorbu podobně rozsáhlého a sofistikovaného systému. Při psaní kódu jsem dbal na řádné komentování kódu a to ve formátu, který podporuje `doxygen` (generátor dokumentací). Nástroj `doxygen` při kompilaci vytvoří programovou dokumentaci, která je umístěna na webový server a je dostupná uživateli přímo z rozhraní stránek. Dokumentace je generována pro snadné orientování v kódu a jasný popis jednotlivých implementovaných metod tříd.

Prostředníkem mezi aplikační bránou a webovým portálem, reprezentujícím grafické uživatelské rozhraní celého projektu, je databáze obsahující všechna potřebná data. Bylo třeba zvolit typ databáze, se kterou budeme pracovat. Mezi nejrozšířenější patří MYSQL a POSTGRESQL databáze. Obě mají své výhody i nevýhody. Implementace funkcí pro přístup do databáze MYSQL nebo POSTGRESQL je velmi jednoduchá, proto jsem se rozhodl, že náš systém bude poskytovat podporu pro oba typy databází. Před samotným spuštěním brány je zapotřebí nejdříve vytvořit tabulky v těchto databázích. Součástí systému je skript, který toto zajišťuje. Skript bude blíže popsán v podkapitole 7.3.

7.1 Aplikační brána

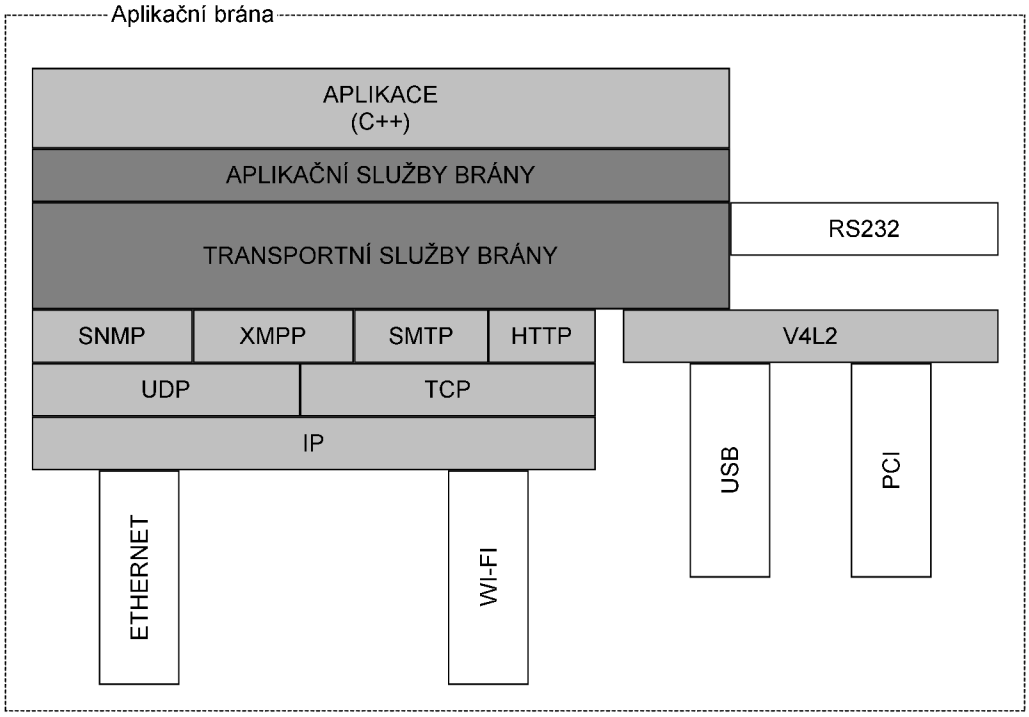
Aplikační bránu můžeme rozdělit na několik částí, každá část vykonává specifickou funkci a zajišťuje tak celkový chod programu. V každé podkapitole bude popsáno, jakým způsobem byla prováděna její implementace a problémy, které se během implementace objevily.

Po spuštění brány se prohledá databáze. Pokud se v ní nachází relevantní informace, dojde k jejich extrakci. Podle typu této informace se upraví nastavení samotné brány. Následně se vytvoří nové vlákno pro každé zařízení nalezené v databázi. Od této chvíle se každé vlákno stará o své zařízení. Pokud během činnosti zařízení nastane jakákoliv chyba, samo se ukončí, upraví hodnoty v databázi a uvolní pro něj alokovanou paměť.

Aplikační brána je schopna přijímat zprávy od PHP serveru. Tyto zprávy jsou důležité, jelikož jsou asynchronně posílány při změně dat v databázi. Brána tedy naslouchá na zadaném, předem domluveném portu. Pokud na tento port přijde zpráva z PHP serveru, přijme se a provede se akce daná obsahem zprávy. Může to být například informace o změně položky v databázi anebo pokus o vyhledání dostupných zařízení připojených k počítači. Popis komunikace se nachází v kap. 7.1.2.

7.1.1 Komunikace s koncovými zařízeními

Komunikace s koncovými zařízeními má zásadní postavení v celém projektu. Bylo třeba vytvořit systém, který by byl pokud možno univerzální a podporoval velké množství druhů zařízení. Jak už bylo zmíněno v návrhu, vytvořit nějaký jednotný obecný protokol je v podstatě nemožné, vzhledem k nedostupnosti jakéhokoliv standardu. Snažil jsem se tedy při implementaci použít takové komunikační protokoly, které jsou alespoň z části rozšířené napříč výrobci a dodavateli. Použil jsem proto protokoly SNMP, HTTP, V4L2 a jednoduchý protokol pro komunikaci po sériové lince. Přesný popis jednotlivých protokolů byl uveden v kapitole 4. Systém pro komunikaci je tedy tvořen z jednotlivých základních protokolů, které ve výsledku poskytují jednotný přístup k aktuálním hodnotám ze zařízení. Celkový pohled na aplikační bránu z hlediska použitých protokolů je zobrazen na obrázku 7.1. Vidíme zde jednotlivé vrstvy a rozhraní, přes která se zařízení připojují.



Obr. 7.1: Popis aplikační brány z hlediska použitých protokolů

Hlavní smyčka, která je pro všechna zařízení stejná obstarává zhruba následující funkci. Nejprve proběhne načtení dat a jejich uložení. Následně dojde k porovnání načtené hodnoty s nastavenými limitními hodnotami. Při překročení dojde k záznamu dat a informování uživatele o nastalé události. Specifikem komunikace s IP kamerami je jejich schopnost detekovat pomocí vnitřních mechanizmů pohyb. Pokud je součástí kamery i mikrofon, tak i zvýšenou hladinu zvuku. IP kamera při detekci odesílá na předem specifikovanou adresu a port zprávu o nastalé události. Aplikační brána tuto zprávu zachytává a podle jejího obsahu jednak informuje ostatní zařízení ve skupině a jednak začíná se záznamem dat na disk.

7.1.2 Komunikace s PHP serverem

Tato podkapitola se poněkud liší od předchozí, neboť nepopisuje komunikaci s koncovými zařízeními, ale komunikaci mezi aplikační bránou a PHP serverem. Při návrhu a implementaci systému bylo totiž zjištěno, že by bylo vhodné asynchronně detekovat změny v databázi. Prvotní myšlenkou řešení bylo zasílání notifikací přímo z SQL serveru. Toto řešení se však ukázalo jako nevhodné, protože podobné notifikace nepodporují všechny druhy SQL serverů. Proto byl navržen velmi jednoduchý protokol pro komunikaci mezi PHP serverem a aplikační bránou. Komunikace pracuje na aplikační vrstvě. Syntaxe protokolu je popsána níže.

INF <parametr> \r\n Host: Apache\r\n\r\n

Parametr	Popis
nove-zarizeni	Uživatel přidal nové zařízení
zmenazarizeni	Uživatel změnil nastavení zařízení
zmenaparametr	Uživatel změnil nastavení brany

Tab. 7.2: Tabulka parametrů pro komunikaci s PHP serverem

7.1.3 Zpracování a záznam dat

Po příjmu obrazových dat ze zařízení je třeba vyřešit, jakým způsobem budou data zpracována a zdali budou archivována či nikoliv. Pro jednotný způsob práce se snímky je potřeba mít společný formát dat, který nám poskytuje pouze část zařízení. Nejrozšířenějším formátem obrázků je JPEG. Proto budeme všechny přijaté snímky konvertovat na tento formát, postup konverze je popsán dále. Po konverzi na jednotný formát je potřeba snímek nějakým způsobem zpracovat. V našem v případě znamená detekovat v něm pohyb. Problematika detekce pohybu je podrobněji popsána v podkapitole 7.1.4. Po všech provedených operacích je potřeba data někam uložit. Máme k dispozici databázi a místo na HTTP serveru reprezentovaným naším webovým portálem. Implementace archivace dat je popsána na konci této podkapitoly.

7.1.3.1 Konverze dat

Vzhledem k tomu, že přijímaná obrazová data z kamer nemusí být vždy v žádoucím JPEG formátu, bylo třeba si vytvořit funkce zajišťující konverzi z různých formátů do JPEG. Tato problematika se týká především USB a PCI kamer, které typicky podporují jen standardní formáty dat. IP kamery jsou v tomto směru opět několik kroků vpředu. IP kamery, které tento formát nepodporují, jsou již spíše výjimkou. Vytvořil jsem tedy postup konverzí, kdy se nejdříve surová obrazová data převedou do formátu PPM. Následně jsou za využití knihovny *libjpeg* převedena do požadovaného JPEG formátu.

7.1.3.2 Záznam dat

Můžeme zaznamenávat tři základní druhy dat, teplotu z čidla, snímek z kamery a zvukový záznam z mikrofonu. Teplotu z čidel budeme ukládat do databáze, kde bude ponechána minimálně jeden týden. Budeme mít tedy přehled o vývoji teploty na každém čidle za několik posledních dní. Zachycené snímky z kamery budeme ukládat na HTTP server dvojím způsobem. Jednak budeme ukládat samotné snímky, které budou sloužit uživateli pro zobrazení aktuálního obrazu na kameře. Jednak budeme ukládat několikaminutové video, které bude nahráváno při narušení bezpečnosti. Toto video bude ve formátu MJPEG, který má své výhody, ale i nevýhody. Mezi výhody jistě patří jednoduchost formátu dat. Naopak mezi nevýhody patří velikost takto zpracovaných dat. Zvuk pak bude zaznamenáván pouze při narušení bezpečnosti a to ve formátu WAV.

7.1.4 Detekce narušení bezpečnosti

Data získaná ze zařízení jsou kontrolována na překročení hraničních limitů, které jsou jim nastaveny při inicializaci brány. V praxi musíme oddělit různé typy dat. Pokud zařízení poskytuje číselnou hodnotu, není nic snazšího, než ji porovnat s nastavenými limitními hodnotami. Výchozí limitní hodnoty pro teplotní čidla jsou - 5°C a +35°C. Detekce narušení ve snímcích z kamery je mnohem komplikovanější a vyžaduje sofistikovanější přístup. Dalším typem dat přijímané naším systémem jsou zvukové stopy. Při implementaci jsem využil interní podpory IP kamer pro zasílání událostí o překročení určité hladiny zvukového pásma.

Některé kamery, které jsou součástí systému, nedokáží samy interně detekovat pohyb. Bylo proto nutné využít nějakého algoritmu, který bude přímo součástí brány a pohyb dokáže detekovat. Dá se předpokládat, že se tento problém bude týkat pouze webkamer. Můžeme tedy využít toho, že takové kamery jsou stacionární a obraz před kamerou bude tudíž neměnný. Zvolil jsem proto velmi jednoduchý algoritmus, který porovnává dva po sobě jdoucí snímky z kamery a porovnává jednotlivé obrazové body. Bylo třeba zvolit nějakou vhodnou hladinu šumu, aby nevznikaly problémy s falešnou detekcí. Společně s tím bylo třeba zvolit určitou procentuální hranici změny obrázku, aby se zabránilo stejnému problému. Tyto hladiny se po testování podařilo úspěšně nastavit, a přestože se jedná o velmi jednoduchý algoritmus, poskytuje velmi dobré výsledky.

Je vhodné, aby existoval nějaký záznam o detekovaných událostech. K tomu nám poslouží tabulka záznamů v databázi. Pokud systém detekuje narušení bezpečnosti, uloží do databáze informace o zařízení, které detekci vyvolalo. Dále se uloží aktuální hodnota spjatá se zařízením, aktuální čas a příznak, zda se jedná o počátek detekce či jeho konec.

7.1.5 Informování uživatele

Uživatel(é) je při narušení bezpečnosti informován SMS zprávou, e-mailem, JABBER zprávou anebo webovým požadavkem. Záleží na uživateli, které typ oznamování si vybere, na které účty si oznámení nechá posílat apod. Pro posílání zpráv e-mailem jsem vytvořil účet *mass349752@seznam.cz* skrz který jsou e-maily posílány na cílový účet. Zpráva obsahuje název zařízení, které vyvolalo detekci a v příloze je přiložen snímek zobrazující aktuální data ze zařízení. Odesílání JABBER zpráv probíhá z účtu *mass349752@jabbim.cz*. Zpráva obsahuje odkaz na zachycený snímek, který je uložen na webovém serveru. Heslo pro oba účty je *massVUTproject*.

Při odesílání zpráv na JABBER však nastává nepříjemnost se zachytáváním automaticky rozesílaných zpráv jako nevyžádaných. Jsou dvě možnosti řešení tohoto problému. Vypnout na cílovém účtu kontrolu nežádoucích zpráv anebo přidat JABBER účet do seznamu kontaktů cílového účtu, a tím se kontrole na nevyžádané zprávy vyhnout.

Dále bylo potřeba nastavit určitý časový limit, určující mezeru mezi odesláním dvou po sobě jdoucích varování, protože by mohlo dojít k zaplavení uživatele velkým množstvím zpráv. Tento limit je ve výchozím nastavení inicializován na hodnotu přibližně 180-ti minut.

7.1.6 Konfigurace brány

Samotnou aplikační bránu je možné konfigurovat v souboru `config.h`. Nachází se zde konstanty, které přizpůsobují chování systému potřebám uživatele. Většina nastavení, která nejsou přímo spjatá s chodem programu, jsou nastavitelná pomocí webového portálu viz další kapitola. Systém byl navržen tak, aby jej bylo do budoucna možno snadno rozšířit. V konfiguračním souboru tedy lze jednoduše přidat nové typy zařízení nebo nové možnosti odesílání událostí.

7.2 Webový portál

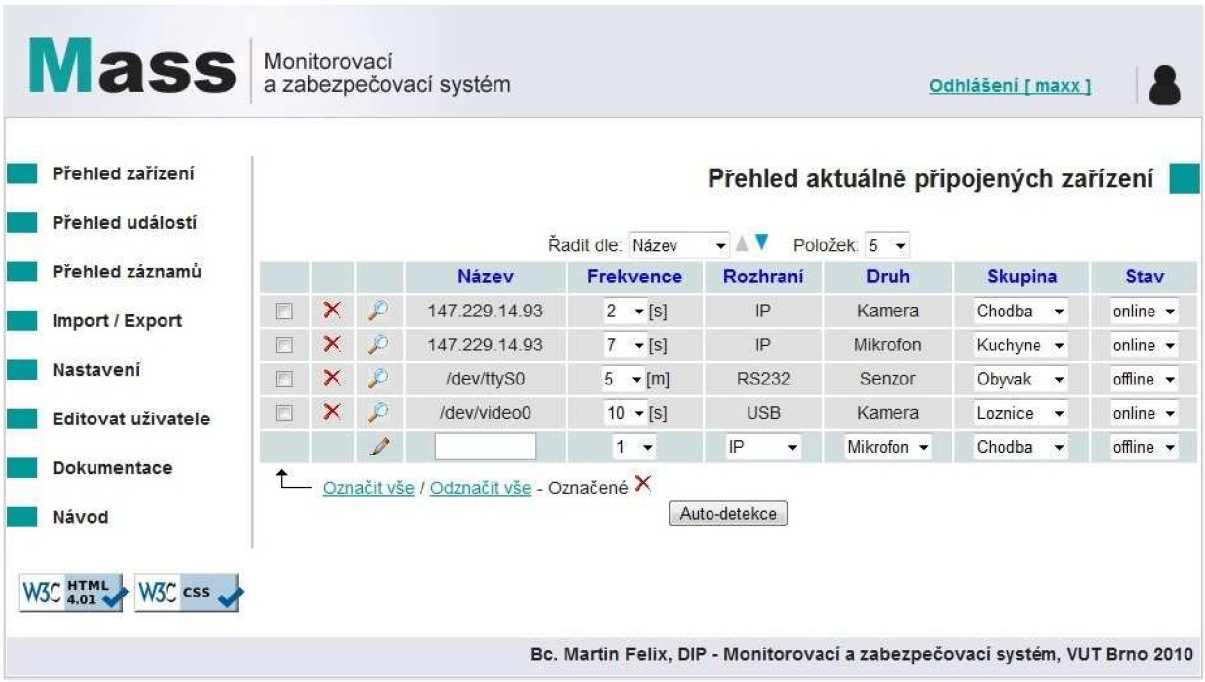
Počítačové systémy jsou značně složitou technologickou oblastí. Kromě toho, že musí přinášet užitek, musí být i pro koncového uživatele příjemné na ovládání. Skupina těchto vlastností se nachází pod zkratkou GUI neboli grafické uživatelské rozhraní. Možností grafické reprezentace uživatelského rozhraní je obrovské množství. Při jeho návrhu je nutné využít vhodnou míru abstrakce a učinit tak ovládání co nejvíce intuitivní. Uživatelské prostředí jsem tedy realizoval jako webovou stránku HTML, vytvořenou pomocí technologie PHP.

Velmi důležitá součást sloužící ke vzdálenému uživatelskému přístupu do celého systému. Uživatel má možnost prohlížet data ze zařízení, nastavovat parametry zařízení systému atd. Webový portál poskytuje přístup uživatelům pod různými typy práv. Nejvyšším uživatelem je *superuživatel*, který jako jediný může přidávat či odebírat ostatní uživatele. Práva uživatelů určují rozsah přístupu do systému. Uživatel s nejnižšími právy například může pouze prohlížet připojená zařízení atd.

Portál byl napsán v jazyce PHP a je HTML 4.01 validní. Některé komponenty portálu vyžadují *javascript*, tyto komponenty však nejsou nezbytně důležité pro chod portálu. V případě, že javascript nebude povolen, systém bude bez problému fungovat dále, ale s částečně omezenou funkčností.

7.2.1 Přehled zařízení

V následující podkapitole si ukážeme, jakým konkrétním způsobem je možné využívat web z pohledu *superuživatele*. Na obrázku 7.3 vidíme přehled zařízení připojených k počítači. Zařízení je možno odstranit, přidat anebo změnit nastavení jednotlivých zařízení. Zařízení je možno přidat ručně anebo se je pokusit automaticky vyhledat, není totiž zaručeno, že všechna zařízení budou nalezena. Zvláštností při přidávání IP zařízení je formulář vyžadující jméno a heslo pro přístup k zařízení nebo případně název čtecí a zapisovací komunity. Zvláště důležitá je nabídka *Stav*, která určuje, zda má být zařízení vypnuto či zapnuto. Tímto se dá docílit mnohem nižší spotřeby systému. Dále vidíme, že zařízení jsou součástí skupin (místností) viz kapitola 6.3. Další obrázky webového portálu se nachází v příloze 3.



Obr. 7.3: Rozhraní pro ovládání zařízení v síti. Klientská část komunikace

7.3 Skript

Součástí kompletní implementace je i skript napsaný pro *bash*, který se stará o komplexní kontrolu nastavení apod. Nachází se pod názvem `configure.sh`. Probíhá zde kontrola dostupnosti všech požadovaných knihoven a aplikací. Následně je detekován typ serverové databáze a podle toho jsou nastaveny příslušné příznaky brány a webového portálu. Na závěr jsou přeneseny zdrojové soubory webového portálu do výchozí složky Apache serveru.

7.4 Shrnutí

Značnou překážkou při samotném návrhu, ale především při implementaci byla nedostupnost potřebných koncových zařízení. Tento nedostatek jsem řešil různými emulátory apod. Zejména jsem jich využil při implementaci komunikace mezi bránou a teplotními čidly. Vzhledem k vysoké ceně IP kamer jsem pro počáteční testování využil rovněž emulátorů a pro finální testování a korekci jsem využil přístupu ke školní IP kameře, která obsahuje i mikrofon využitelný v našem systému.

Při implementaci komunikace pomocí knihovny V4L2 dochází po jisté době chodu aplikace k interním chybám knihovny, bohužel se mi ani po dlouhém zkoumání nepodařilo tento problém vyřešit. Problém však nemá zásadní vliv na chod aplikace.

Nastavení způsobu zaostřování a hlavně kontroly jasu se ukázalo, jako poměrně složitý problém. Webkamery obsahují (do jisté míry) spolehlivý interní mechanismus upravující jas a ostrost. Někdy nastávají situace, kdy dojde ke skokovým změnám jasu a vznikne tím nežádoucí falešná detekce pohybu. Snažil jsem se to vyřešit manuálním nastavením jasu apod., ale dosáhl jsem ještě horších výsledků, a proto jsem zůstal u automatického nastavování. Přestože knihovna V4L2 obsahuje funkce pro získání zvukových stop z webkamer, nepodařilo se mi stopu úspěšně načíst. Pravděpodobně to bylo způsobeno neexistující podporou pro konkrétní typy zařízení.

8 Závěr

Práce přímo navázala na znalosti získané při tvorbě semestrálního projektu. Byla provedena analýza využitelnosti jednotlivých druhů koncových zařízení a kamerových systémů jako celku pro monitorovací a zabezpečovací systém. Bylo zjištěno, jaké druhy koncových zařízení jsou pro tyto systémy nejvhodnější, a ty byly dále využity v systému. Z této analýzy pak vyplynula fakta, která byla využita při návrhu a implementaci požadovaného systému.

Monitorovací a zabezpečovací systémy nacházejí široké uplatnění v nejrůznějších oblastech života. Vytvořený systém najde své uplatnění především v domácnostech. Jeho využití v ostatních oblastech (např. průmyslu) je však neomezené. Systém by mohl například sloužit rodinám, které jsou na dovolené a chtějí mít přehled o svém domovu. Systém by také mohl nahradit elektrickou požární signalizaci v případě, že by systém byl složen z několika teplotních čidel.

Při tvorbě systému bylo dbáno na co největší univerzálnost. Hlavní snahou bylo, aby systém zvládal připojení různých druhů zařízení, vykazoval nízkou spotřebu a malou náročnost na objem přenášených dat. Implementační část byla psána s ohledem na další rozšiřování systému, zdrojové kódy jsou velmi důkladně komentovány. Celý návrh byl objektově orientován za cílem poskytnout co největší modularitu. Systém lze tedy velmi jednoduše rozšířit a byl úspěšně otestován na operačních systémech Ubuntu a Fedora.

Byl vytvořen systém pro zabezpečení a monitoring objektů. Přístup do systému je možný skrz webový portál, který přímo či nepřímo komunikuje s aplikační bránou. Aplikační brána se stará o komunikaci s jednotlivými zařízeními. Práce byla provázena mnohými komplikacemi a většinu z nich se podařilo vyřešit. Přesto však obsahuje několik nedokonalostí, které poskytují další možnosti rozšíření a studia dané problematiky.

Do budoucna by bylo vhodné rozšířit systém o další bezpečnostní prvky a využít lepší zpracování získávaných dat. Systém by tedy mohl být rozšířen o podporu audio vstupu ze zvukových karet a určité uplatnění by v systému mohly najít i čidla založená na technologii Zigbee. Algoritmy pro detekci pohybu z webkamer by mohly být sofistikovanější, např. detekce obličeje a detekce v části zorného pole. Pro dosažení širší podpory různých typů zařízení, by bylo vhodné rozšířit komunikační protokoly o protokoly jiných výrobců těchto zařízení. Dále by mohla být poskytnuta větší nabídka možností informování uživatele. Jako přídavek vzdálené ovládání jednotlivých zařízení (kamer apod.).

Za vlastní přínos bych především uvedl sestavení komplexního systému skládajícího se z poměrně různorodých komponent. Především zapojení webkamer jako bezpečnostního prvku nebylo jednoduchou záležitostí. Považuji za velmi přínosné, že jsem se obeznámil s různými druhy komunikačních protokolů a získal cenné zkušenosti při tvorbě takto komplexního systému.

Literatura

[1] Aghajan, R, Cavallaro, A.: *Multi-Camera Networks: Principles and Applications.* Elsevier inc, Burlington, ©2009. ISBN 13:978-0-12-374633-7

[2] Axis Communications AB: *User´s Manual: Axis Q1755 Network Camera* [on-line]. ©2010. Dostupné na URL: < http://www.axis.com/products/cam_q1755>

[3] Axis Communications AB: *Vapix: Event Handling version 3* [on-line]. ©2008. Dostupné na URL: < http://www.axis.com/files/manuals/VAPIX_3_EventHandling_1_01.pdf

[4] Axis Communications AB: *Vapix: HTTP API version 3* [on-line]. ©2008. Dostupné na URL: <http://www.axis.com/files/manuals/VAPIX_3_HTTP_API_3_00.pdf>

[5] Damjanovski, V.: *CCTV: Networking and Digital Technology, Second Edition.* Elsevier inc, Burlington, ©2005. ISBN 0-7506-7800-3

[6] Dirks, B., Schimek, H.,M.,Verkuil, H., Rubli, M.: *Video for Linux Two: API Specification, Revision 0.24* [on-line]. GNU Free Documentation License, ©1999-2008. Dostupné na URL: < http://v4l2spec.bytesex.org/v4l2spec/v4l2.pdf>

[7] Douglas, R., Mauro & Kevin, J., Schmidt.: *Essential SNMP.* 2nd edition. O´Rielly Media, Inc., Sebastipol, ©2005. ISBN 0-596-00840-6

[8] ESCAD Trade s.r.o.: *Bezpečnostní kamery* [on-line]. Praha, ©2010, [cit. 2009-12-08] Dostupné na URL:<http://www.escadtrade.cz>

[9] ESCAD Trade s.r.o.: *YK-564K Camera Kit* [on-line]. Praha, ©2010, [cit. 2009-12-08] Dostupné na URL:<http://escadtrade.cz/data/mod_eshop/127/mo/down/prospekt-en.pdf>

[10] Fraden, J.: *Handbook of Modern Sensors: Physics, Designs, and Applications* Springer Science, ©2004. ISBN 0-387-00750-4

[11] Hama spol. s r. o.: *Dynamický mikrofon DM 20* [on-line]. Brno, ©2010, [cit. 2009-12-08] Dostupné na URL:< http://www.hama.cz/ProductDetail.aspx?id=46020>

[12] HP Tronic Zlín spol. s r.o.: *GSM kamera* [on-line]. Zlín, ©2010, [cit. 2009-12-08] Dostupné na URL:<http://www.eproton.cz/Asp/DescrView.asp?IDArticle=163472>

[13] Jablotron Alarms a.s.: *The SD-280 fire detector* [on-line]. Jablonec nad Nisou, ©2008. Dostupné na URL:<http://jablotron.cz/upload/download/en/sd-280_en_mle51000.pdf>

[14] Jablotron Alarms a.s.: *LD-63HS Overflow Alert Detector* [on-line]. Jablonec nad Nisou, ©2008. Dostupné na URL:<http://www.audon.co.uk/mzz51302.pdf>

[15] Komínek, P.: *Systém pro zabezpečení a střežení objektů a prostor.* Bakalářská práce naVysokém učení technické v Brně: ©2008. Vedoucí práce Ing. Josef Strnadel, Ph.D.

[16] Kruegle, H.: *CCTV: Surveillance video practises and technology.* 2nd edition Elsevier inc, Burlington, ©2007. ISBN 13:9780-7506-7768-4

[17] Logitech: *Webcam C200 specification* [on-line]. ©2009. Dostupné na URL: <http://logitech.com/index.cfm/webcam_communications/webcams/devices/5865>

[18] Papouch s.r.o.: *Manuál digitálního, teplotního čidla TM* [on-line]. Praha, ©2005. Dostupné na URL:< http://www.papouch.com/shop/scripts/pdf/tm.pdf>

[19] Papouch s.r.o.: *Manuál digitálního, ethernetového, teplotního čidla TME* [on-line]. Praha, ©2005. Dostupné na URL:< http://www.papouch.com/shop/scripts/pdf/tme.pdf>

[20] Prata, S., Brunno, P.: *C++: Primer Plus, Fourth Edition.* Sams Publishing, ©2002. ISBN 0-67-2322223-4

[21] Schildt, H.: *CCTV: Networking and Digital Technology, Second Edition.* Elsevier inc, Burlington, ©2005. ISBN 0-7506-7800-3

[22] Tipton, H., F., Krause, M.: *Information Security: Management Handbook.* Fifth Edition, 2. vydání. CRC Press LLC, ©2005. ISBN 0-8493-3210-9

[23] Valach, S.: *Inteligentní průmyslové kamery* [on-line]. Automatizace, ©2008, [cit.-2009-12-08]. Dostupné na URL:<http://www.automatizace.cz/article.PHP?a=389>

[24] Viakom s.r.o.: *Specifikace VGUARD RT-4* [on-line]. Praha, ©2009, [cit. 2009-12-08] Dostupné na URL:<http://viakom.cz/stahuj/VGUARD/specifikace_vguard_eng.pdf>

[25] Zabezpecovacky.cz.: *Čidla* [on-line]. Brno, ©2007, [cit. 2009-12-08]. Dostupné na URL: <http://www.zabezpecovacky.cz/cidla-detektory-dratove>

Seznam příloh

Příloha 1 - Adresářová struktura a obsah přiloženého DVD

Zdrojové soubory aplikační brány. Adresář: mass	
Soubor	**Popis**
event.cpp	- třída událostí
image.cpp	- třída pro zpracování obrázků
ip_camera.cpp	- třída IP kamer
ip_micro.cpp	- třída IP mikrofonů
ip_sensor.cpp	- třída IP senzorů
main.cpp	- hlavní zdrojový soubor
mysql.cpp	- třída pro mysql databázi
pgsql.cpp	- třída pro postgresql databázi
serial.cpp	- třída sériových senzorů
usb_cam.cpp	- třída webkamer a pci kamer

Zdrojové soubory webového portálu. Adresář: web	
Soubor	**Popis**
config.php	- konfigurační soubor k databázi
device.php	- přehled zařízení
event.php	- přehled událostí
functions.js	- javascriptové funkce
image.php	- zobrazení obrázku
index.php	- startovní stránky
logout.php	- odhlášení z webu
main.php	- pomocné globální funkce
manual.php	- návod
sql.php	- práce s sql databází
style.css	- kaskádové styly
user.php	- editace uživatelů
view.php	- prohlížet zařízení
xml.php	- import / export xml

Ostatní soubory. Adresář mass	
Soubor	**Popis**
Makefile	- makefile pro linuxové systémy
configure.sh	- konfigurační skript
dip.doc	- zdrojový text zprávy
doxy	- adresář s programovou dokumentací
doxy_config	- konfigurace pro tvorbu dokumentace
INSTALL	- popis instalace
my_script.sql	- skript pro vytvoření mysql tabulek
pg_script.sql	- skript pro vytvoření postgresql tabulek
README	- seznam souborů

Tab. P1.1, P1.2, P1.3: Tabulky obsahující strukturu souborů a adresářů DVD

Příloha 2 - Instalace systému

1) Požadavky na hardware:

a) Osobní počítač vybavený sériovým portem (9 pin), síťovou kartou, USB rozhraním, připojením k internetu a operačním systémem Linux.

b) IP kamera nebo webkamera nebo analogová kamera nebo teplotní čidlo nebo detektor.

2) Předpoklady pro správnou instalaci systému:

a) Nainstalovaný software třetích stran:

- MYSQL server nebo POSTGRESQL server.
- PHP server.
- Knihovna V4L2 pro práci s video zařízeními.
- Knihovna Gloox pro komunikaci nad XMPP protokolem.
- Knihovna Snmp++ pro práci nad SNMP protokolem.

b) Znalost uživatelského jména a hesla pro přístup k SQL serveru.

c) Administrátorská práva pro spuštění konfiguračního skriptu (nemusí být nezbytné).

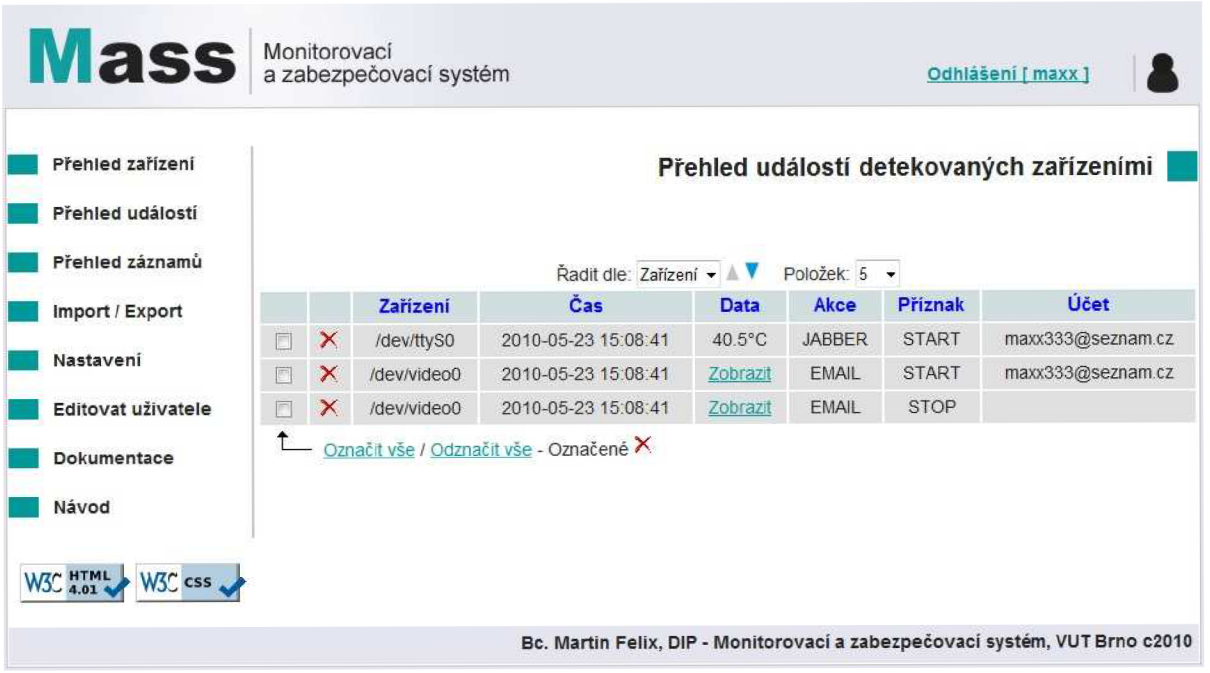
3) Instalace:

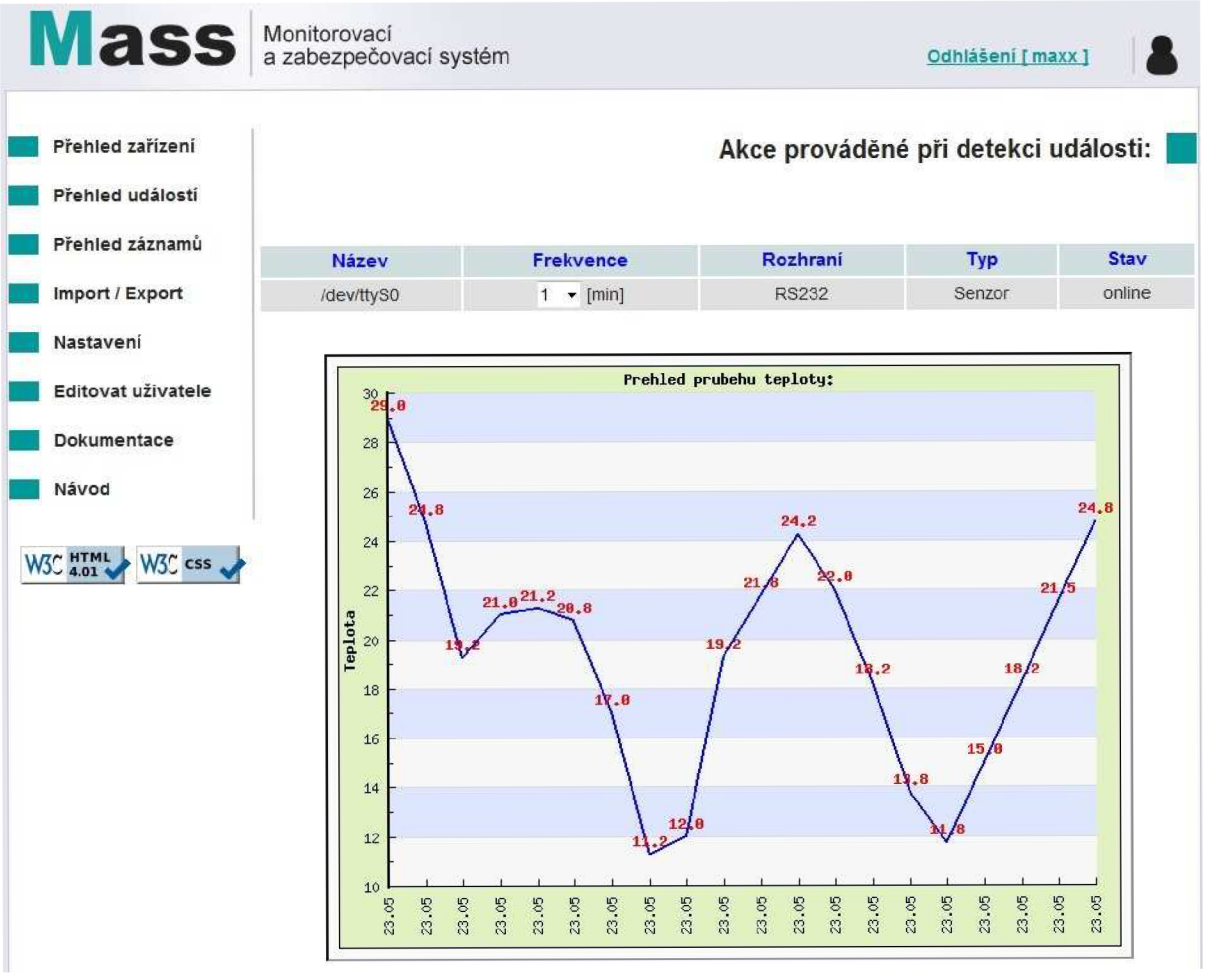
Nejprve je třeba spustit konfigurační skript `configure.sh`, který se postará o kontrolu požadavků na systém uvedených v bodě 2. Po kontrole bude uživatel dotázán na jméno a heslo k SQL serveru. Následně se vytvoří databázové tabulky, programová dokumentace a webové stránky. Je třeba si dávat pozor, aby byla správně nastavena uživatelská práva webového portálu. Nyní je možné zkompilovat samotný sever příkazem `make`.

4) Spuštění:

Aplikační bránu spustíme souborem `mass`. Připojíme koncová zařízení a spustíme internetový prohlížeč. V něm zadáme adresu `http://localhost/mass`. Přístupové jméno a heslo je stejné jako k SQL serveru. Na stránkách zadáme připojená koncová zařízení, zadáme události a systém je tímto plně funkční.

Příloha 3 - Obrázky webového portálu





Obr. P3.1, P3.2: Zachycené obrázky webového portálu monitorovacího systému