Komparativní studie funkčních vlastností video management platforem

Bc. Martin Pektor

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin Pektor**
Osobní číslo:	**A14340**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Komparativní studie funkčních vlastností video management platforem**
Téma anglicky:	**A Comparative Study of the Functional Properties of Video Management Software**

Zásady pro vypracování:

1. **Pojednejte o významu systému pro správu videa ve vztahu k oblasti dohledových videosystémů.**
2. **Definujte základní procesy realizované systémy pro správu videa.**
3. **Navrhněte kritéria hodnocení systému pro správu videa.**
4. **Aplikujte navržený hodnotící aparát na vybraných systémech pro správu videa.**
5. **Zpracujte nejméně dvě laboratorní úlohy pro podporu výuky předmětu kamerové systémy.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **CAPUTO, Tony C. Digital video surveillance and security. Boston: Butterworth-Heinemann/Elsevier, 2010, xvii, 333 p. ISBN 18-561-7747-5.**
2. **ČSN EN 62676-1-1. Dohledové videosystémy pro použití v bezpečnostních aplikacích. Část 1-1: Systémové požadavky-Obecně. Praha: ÚNMZ, 2014.**
3. **ČSN EN 62676-2-1. Dohledové videosystémy pro použití v bezpečnostních aplikacích. Část 2-1: Video přenosové protokoly-Obecné požadavky. Praha: ÚNMZ, 2014.**
4. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.**
5. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012, 386 s. ISBN 978-80-87500-19-4.**

Vedoucí diplomové práce: **Ing. Jiří Ševčík**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **16. května 2016**

Ve Zlíně dne 5. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Diplomová práce se zabývá komparací funkčních vlastností vybraných systémů pro správu videa. Teoretická část je věnována charakteristice těchto softwarových aplikací, objasnění jejich základních procesů a provázání s oblastí dohledových videosystémů. Praktická část se zaobírá návrhem evaluačního systému, pomocí kterého jsou následně konkrétní systémy pro správu videa ohodnoceny a komparovány. Závěrečné kapitoly práce jsou vyhrazeny tvorbě laboratorních úloh pro podporu výuky předmětu Kamerové systémy.

Klíčová slova: dohledový videosystém, systém pro správu videa, komparace, evaluace, Axis Camera Station, Axxon Next, Milestone XProtect, ATEAS Security

ABSTRACT

The thesis deals with the comparison of the functional properties of selected video management systems. The theoretical part is devoted to the characteristics of these software applications, explanation of their basic processes and linking with the section of video surveillance systems. The practical part deals with the design of the evaluation system, by which are the specific video management systems evaluated and compared. The last chapters are dedicated to the creation of laboratory tasks for support subject Kamerové systémy.

Keywords: video surveillance system, video management system, comparison, evaluation, Axis Camera Station, Axxon Next, Milestone XProtect, ATEAS Security

Poděkování

Mé poděkování patří vedoucímu diplomové práce Ing. Jiřímu Ševčíkovi za poskytnutí cenných rad, připomínek, důležitých kontaktů a velice intenzivních konzultací v průběhu zpracování této práce. Dále děkuji svým dvěma kolegům Danielu Bráníkovi a Ladislavu Gbelcovi za spolupráci při vytváření podkladů pro praktickou část. V neposlední řadě děkuji společnosti Axis Communications za příležitost zúčastnění se školení a partnerských dnů. Na závěr bych rád poděkoval své rodině a přátelům za podporu během celého studia na VŠ.

OBSAH

ÚVOD

Se skutečností, že dohledové videosystémy prochází v posledních letech značným rozmachem, se dnes setkáváme téměř na každém kroku. Kamerová technika se již od počátku 21. století stala nedílnou součástí každodenního života a postupně nachází stále nové možnosti uplatnění. Tato situace také zapříčinila významný rozvoj pokročilých softwarových aplikací, které jsou ve světě známy pod slovním spojením video management systémy, respektive systémy pro správu videa. Díky jejich nasazení jsme schopni efektivně spravovat, ovládat a konfigurovat veškeré kamerové vybavení, jakožto i některé další související prvky pro přenos a záznam videa.

V současné době je však velice obtížné nalézt vědecké publikace nebo jakékoliv edukační materiály, které by potencionálního uživatele video management systémů obeznámily s širším pojetím této problematiky. V zásadě tak máme k dispozici pouze propagační materiály a manuály ke konkrétním softwarům, jenž však i přes svou značnou obsáhlost nezachází do hloubky a nevysvětlují dílčí procesy a princip funkčnosti zmíněných aplikací. Neocenitelným zdrojem informací jsou proto různé školící kurzy a semináře pořádané společnostmi specializovanými na jejich vývoj a distribuci.

Účelem diplomové práce je tedy objasnit problematiku video management systémů a seznámit čtenáře s jejich současným portfoliem funkčních vlastností. V návaznosti na to budou vybrané softwary představeny a následně komparovány pomocí multikriteriálního evaluačního systému. Výsledek tohoto procesu by měl poskytnout širší rozhled nad touto oblastí a usnadnit případné rozhodování při výběru vhodného produktu.

Tato práce je také úzce svázána s plánovanou výukou na téma kamerových systémů, jejíž zahájení se uskuteční již v následujícím akademickém roce. Součástí výuky bude mimo jiné i práce s konkrétními video management systémy, jež má potenciál studenty seznámit s co možná nejširším spektrem funkcí a praktickým využitím těchto aplikací. Závěr práce je proto věnován návrhu laboratorních úloh vztažených k řešené problematice. Navíc se do budoucna počítá i s možností aplikace jejich konceptu na vytvoření dalších laboratorních cvičení, pomocí kterých by se video management systémy provázaly s výukou související tematiky, jako je například video analýza nebo obrazové vlastnosti kamer.

I. TEORETICKÁ ČÁST

1 SYSTÉMY PRO SPRÁVU VIDEA JAKO SOUČÁST DOHLEDOVÝCH VIDEOSYSTÉMŮ

Úvodní kapitola pojednává o začlenění systému pro správu videa do širší oblasti dohledových videosystémů (dále jen VSS). Nejprve si definujeme zmíněnou oblast z pohledu aktuálních norem a přiblížíme si, jakou úlohu hrají VSS v různých odvětvích nejen bezpečnostního průmyslu. Součástí této kapitoly bude také popis funkčního bloku VSS a požadavků na provoz, které se přímo týkají systémů pro správu videa.

V navazující kapitole si obecně charakterizujeme systémy pro správu videa (dále jen VMS). Následně si na schématu znázorníme jejich jednotlivé funkční celky, které si posléze krátce představíme. V neposlední řadě si vysvětlíme, na jaké architektuře jsou VMS postaveny a objasníme jejich konkrétní platformy.

1.1 Dohledové videosystémy

Dohledové videosystémy, často obecně nazývané jako kamerové systémy, dohledové systémy, či zkráceně CCTV (Closed Circuit Television – uzavřený televizní okruh), jsou efektivním nástrojem nejen v bezpečnostním průmyslu. Podobných označení se dále nabízí celá řada, v této práci však budeme vycházet z definice České technické normy ČSN EN 62676-1-1 (Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně). Norma definuje *Dohledový videosystém (*zkráceně VSS, z anglického Video Surveillance System) jako „*Systém skládající se z kamerového vybavení, úložiště, monitorovacího zařízení a souvisejících zařízení pro účely přenosu obrazu a ovládání.“*. Norma rovněž upřesňuje, že systémy CCTV jsou chápány jako součást obecnějšího pojmu VSS. [1]

S neustálým rozvojem nových technologií nachází dohledové videosystémy své uplatnění ve stále více průmyslových odvětvích. Hlavní předností zůstává nepostradatelnost při budování komplexních zabezpečovacích systémů, které slouží pro ochranu objektů, majetku a osob. Trendem současné doby je integrace kamer s ostatními prvky, jako jsou např. poplachové zabezpečovací a tísňové systémy (dále jen PZTS), elektrická požární signalizace (dále jen EPS) nebo systémy kontroly vstupu (dále jen ACCESS), jejichž vzájemná kooperace znatelně zvyšuje efektivitu celého systému. [2]

Díky nástupu inteligentních funkcí se pole působnosti dohledových videosystémů razantně zvětšilo. Tyto funkce slouží především k automatizaci různých procesů spojených se snímáním sledované scény, díky čemuž může kamera sama zastat úkony, které by jinak musel vykonávat operátor. Správně navržený a odborně nainstalovaný VSS tak lze využít např. pro sledování a vyhodnocování technologických postupů ve výrobě, kontrole dodržování bezpečnostních předpisů, monitorování délky zástupu lidí čekajících u pokladen či turniketů, detekci zanechaného předmětu ve sledované zóně, kontrole pohybu vozidel s možností detekce SPZ a následné porovnání s databází. Základní inteligentní funkce mohou být zabudovány přímo v kameře, pro využití těch pokročilejší je však nezbytné nasazení několika speciálních softwarů, mezi které patří i software normou označovaný jako systém pro správu videa (zkráceně VMS, z anglického Video Management Systém). Obecně řečeno, VMS jsou primárně určeny pro správu VSS, nicméně profesionální (a značně dražší) verze nabízí i celou řadu dalších nadstandardních funkcí, jimiž se bude zabývat praktická část této práce.

V dnešní době má koncový zákazník na výběr z mnoha řešení instalace VSS. Stejně jako v mnoha jiných technických odvětvích, i u kamer je důraz kladen na digitalizaci. Zastaralé analogové systémy jsou již několik let na ústupu a do popředí se dostaly IP VSS. Použití analogových kamer však není zcela vyloučeno, uživatel má stále možnost je zahrnout do svého komplexu VSS pomocí různých zařízení, které převádí analogový signál na digitální. Na pomezí mezi klasickým analogem a IP technologií se ještě nachází několik hybridních systémů, které se snaží zkombinovat výhody obou zmíněných technologií do jednoho celku. [2] [3] [4]

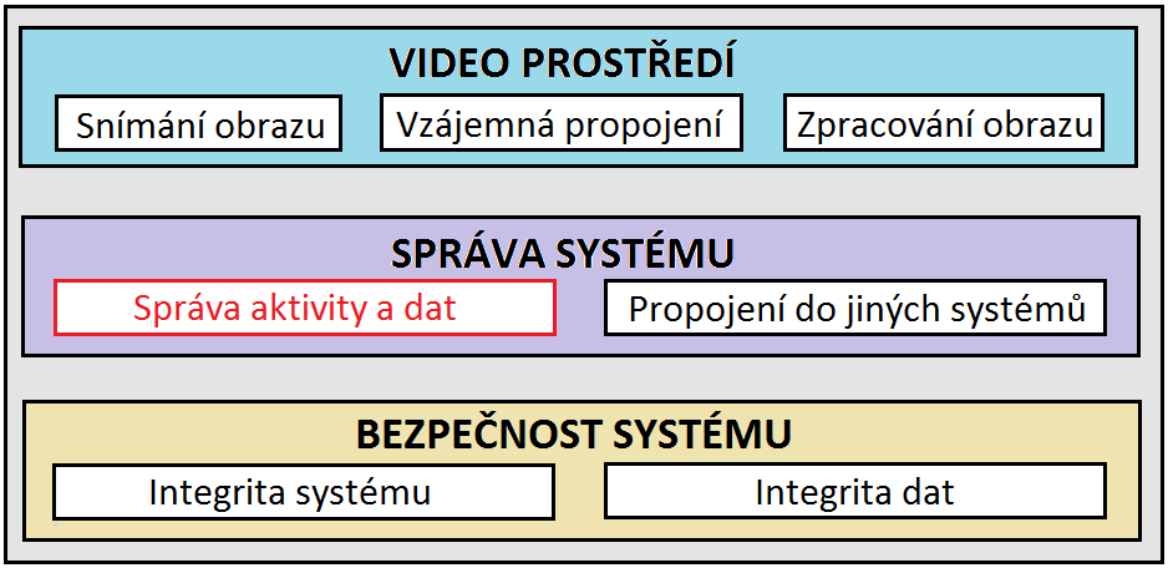
Základní používané technologie dohledových videosystémů jsou:

- analogové systémy,
- AHD systémy,
- IP systémy,
- HD-SDI systémy.

Mimo těchto technologií se dále na trhu objevují určité modifikace, známe pod názvy HD-TVI nebo HD-CVI systémy. Jednotlivé kategorie nebudou nadále více rozebírány, neboť se nejeví pro význam této práce až natolik důležité. Bez ohledu na použitou technologii, samotné kamery i ostatní prvky VSS jsou v konečném důsledku jen zařízení, ze kterých VMS softwary přijímají určitá data. [4] [5]

1.1.1 Funkční popis VSS

VSS můžeme dle normy ČSN EN 62676-1-1 znázornit funkčními bloky, které představují různé části a funkce systému. Pro účely této práce si blíže specifikujeme prostřední blok, jenž reprezentuje správu systému. Ten je dále logicky rozčleněn do dvou samostatných oborů, z nichž je pro nás důležitá především správa aktivity a dat. Tato oblast v sobě zahrnuje široké spektrum činnosti, jež můžeme v praxi spravovat právě prostřednictvím VMS.



Obr. 1. Funkční bloky VSS [1]

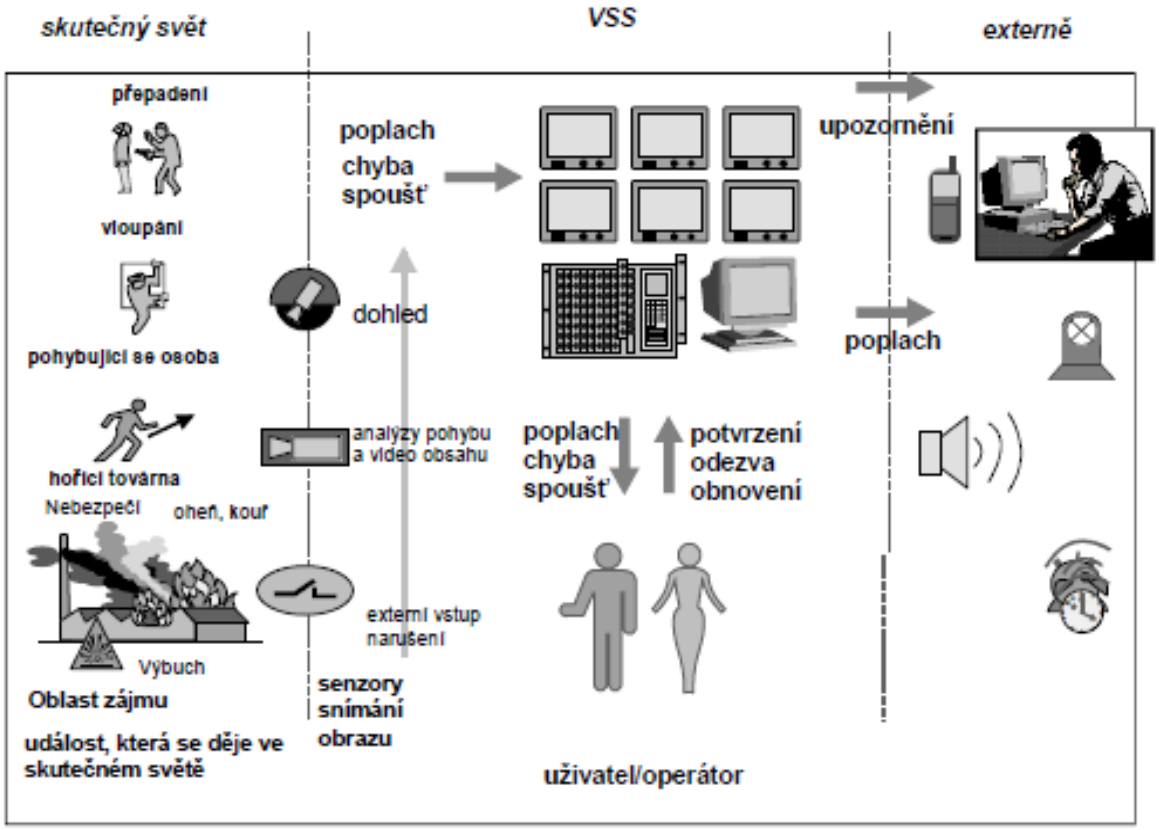
Správa dat obecně zahrnuje jejich získávání, přenos mezi prvky systému, ukládání a následné zobrazování. Tyto funkce může mít na starost konkrétní zařízení z VSS či software instalovaný v těchto zařízeních. Zmíněná data jsou různého typu, převážně se jedná video data, audio data, případně metadata generovaná přímo systémem, nebo získaná z jiného systému. Data mohou být následně zpracována částečně systémem samotným a částečně operátorem. [1]

Systém může ovládat a generovat metadata, která mohou být různého druhu:

- data, která jsou spojena s aktuálními video daty (např. data z pokladen, databáze SPZ, GPS data upřesňující pozici, data analýzy obrazu, …). Tato data mohou být získána z jiného systému nebo generována systémem samotným (např. časové razítko, identifikace zdroje obrazu),
- logovací soubory vygenerované a uložené systémem popisující aktivity systému nebo operátora,
- systémová data ve formě systémových stavů, využití paměťových uložišť atd. [1]

Správa aktivit má na starost veškeré činnosti, které jsou řízené určitými událostmi nebo uživatelskými akcemi. Za událost považujeme předem definovanou situaci, jež by mohla mít negativní dopad na lidské životy, zdraví či majetek. Jedná se např. o požár, vloupání, případně neoprávněnou manipulaci se systémovými prvky. Daná událost pak spouští poplachový postup VSS v reakci na spouštěcí mechanismus, kterým může být výstup ze zpracování obrazu nebo signál z konkrétního detektoru. [1]

Za předpokladu, že dojde ke spuštění poplachového postupu, VSS provede úkoly definované v provozních požadavcích, což ve většině případů znamená odezvu na zaznamenané nebezpečí. Tato odezva může zahrnovat jak určité vnitřní aktivity (např. přesměrování záběru kamery za účelem změny pohledu, záznam nebo zobrazení obrazu), tak upozornění do externího systému (např. řízení přístupu nebo poplachové přijímací centrum). Neméně důležitým úkolem poplachové postupu je pak upozornění operátora, který zajistí další činnosti v souladu s provozními požadavky. Příkladem těchto činností může být nastavení pozic PTZ kamer, zálohování dat, export, tisk atd. [1]



Obr. 2. Správa aktivit VSS [1]

1.1.2 Funkční požadavky na provoz VSS

Norma ČSN EN 62676-1-1 v navazující části specifikuje funkční požadavky na jednotlivé bloky VSS, které se přímo týkají i provozu a obsluhy VMS softwaru. Následující požadavky jsou proto zaměřeny na oblast správy aktivit a dat.

Obsluha

Obsluha uživatelského rozhraní, které v tomto případě reprezentuje právě VMS, musí být pro operátora intuitivní, jednoduchá a rychlá. Status systému musí být rozpoznán, zpracován a zobrazen automaticky. Poplachové situace musí být identifikované a přístupné okamžitě v souladu s dokumentací události. [1]

Správa aktivity a dat

Systém musí umět rozlišit data vyžádané uživatelem a data řízené událostmi. Poplachová data mají vždy prioritu před kontinuálně zobrazovanými daty. Snímky, které jsou zobrazovány operátorovi, musí být zřetelně označeny jako „živé“ nebo „záznam“. Stejně tak video řízené nějakou událostí musí být označeno pro odlišení od videa vyvolaného uživatelem. [1]

Události a událostmi spouštěné činnosti

Pokud je VSS navržen tak, aby ovládal činnosti řízené událostmi, musí splňovat několik požadavků. Spouštěcí mechanismy nebo zprávy musí být načteny z fronty v pořadí, v jakém došly. Výjimku tvoří pouze situace, kdy je příslušný vstup upřednostněn. V těchto situacích proto musí být uvedena úroveň priority. V případě, že je ve frontě několik zpráv se stejnou prioritou, jsou rovněž vyvolány v pořadí, v jakém byly doručeny. [1]

Obecné požadavky pro indikaci priorit jsou následující:

- systém musí indikovat existenci více poplachů, než je možné aktuálně zobrazit,
- k zobrazované informaci mohou být na vyžádání k dispozici doplňkové informace, přičemž zobrazované informace s prioritou musí být zachovány,
- žádný normální provoz VSS nesmí zamezit indikaci poplachu.[1]

Dále platí, že VSS musí umožňovat rozlišení různých stavů systému. Jedná se např. o stavy, které spustily aktivitu, stavy poplachové, závady či narušení. VSS musí nabídnout prostředky k viditelné i zvukové indikaci poplachu za účelem varování operátora. Stejně tak musí poskytovat i možnosti pro potvrzení poplachu. [1]

1.2 Systémy pro správu videa

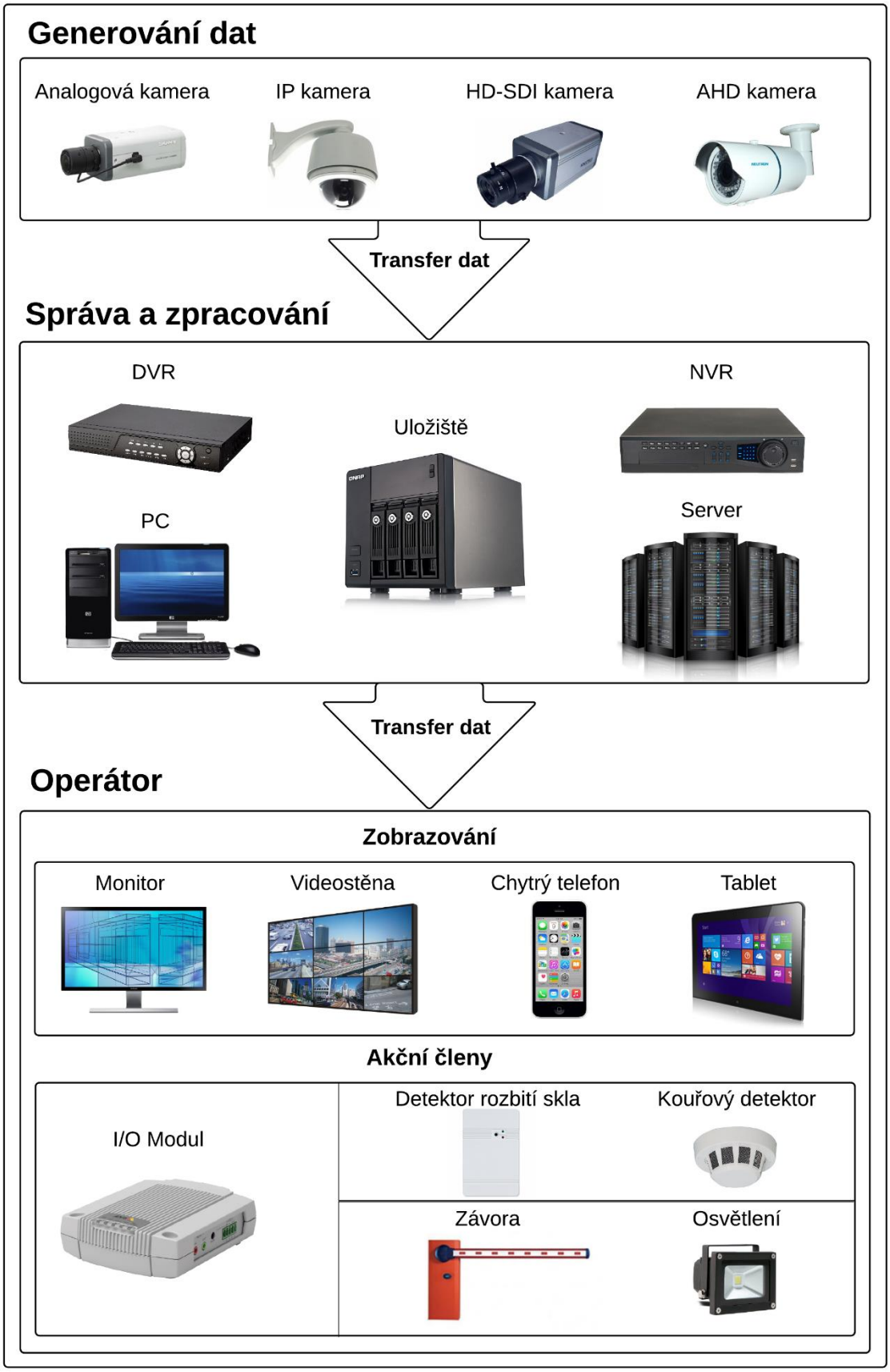
Jak již bylo nastíněno v předchozích kapitolách, systémy pro správu videa můžeme obecně charakterizovat jako softwarový nástroj, který primárně slouží pro komplexní management kamer, potažmo VSS. Vzhledem k současné nadvládě IP VSS je pochopitelné se domnívat, že VMS jsou primárně vyvíjena jen pro podporu IP kamer. Nicméně v dnešní době již není problém do VSS zahrnout i analogové, případně AHD kamery a vytvořit tak funkční hybridní systém, využívající výhod obou technologií. Použití VMS softwaru však nemusí být jediný způsob, jakým provádět správu VSS, i když ostatní varianty se nejeví až natolik efektivní. Aplikování vhodného VMS má nepopiratelně značný vliv na celkovou účinnost a efektivitu dohledového videosystému. [2]

Teoreticky se nám tedy nabízí 3 možnosti. První z nich je prostý monitoring prostřednictvím webového rozhraní. Každá IP kamera má vestavěný webový server s vlastní IP adresou. Pro sledování záběrů z kamery stačí, když ve webovém prohlížeči dáme vyhledat její IP adresu. Webové rozhraní ovšem nabízí pouze omezené možnosti správy, které se liší podle výrobce a modelu kamery. Většinou se jedná o sledování živého přenosu (často nazývaného jako live stream), základní ovládání PTZ funkcí kamery, manuální nahrávání video streamu, případně nahrávání založené na základě naplánovaných nebo spuštěných událostí, kdy se záznam ukládá formou jednotlivých JPEG obrázků. V těchto případech je záznam ukládán na SD/SDHC kartu umístěnou v IP kameře. [2] [6]

Druhou možností je nasazení softwaru od nezávislého výrobce, který je určen pro základní správu IP kamer. Software je v těchto případech vyvíjen pro nekomerční účely, a je tedy k dostání zdarma. Toto řešení však s sebou nese i značnou řadu nevýhod, jako je např. omezená podpora výrobců kamer, složitější instalace, nepřehlednost celého systému, či jen velmi omezené možnosti správy bez pokročilých funkcí. Zmíněný software nebudeme vzhledem k jeho omezeným možnostem považovat za VMS. [2] [6]

Třetí možností je využít veškerých výhod a vymožeností, jež skýtají pokročilé VMS softwary. Takové řešení je koncipováno formou proprietárního softwaru, tzn. softwaru s uzavřeným kódem, vyvíjeného pro komerční účely. V následujících kapitolách se pokusíme objasnit, s kterými částmi VSS jsou VMS softwary provázány, kde se může VMS v systému fyzicky nacházet a jakým způsobem probíhá dohled nad kamerami. Pro lepší pochopení této problematiky si alespoň krátce charakterizujeme jednotlivé prvky VSS a vysvětlíme vzájemnou spojitost mezi nimi a VMS. [2] [6]

1.2.1 Funkční celky VMS



Obr. 3. Funkční celky VMS

Uvedené schéma reprezentuje základní hardwarové komponenty VSS a jejich uspořádání dle toku dat, od jejich generování, přes přijímání, zpracování a ukládání prostřednictvím VMS, až po jejich zobrazení a vyhodnocení operátorem.

Generování dat

Veškeré kamery jsou VMS softwary chápany jako generátory dat. Dle použité technologie z nich pak mohou proudit data různého typu. Datům musí rozumět jak samotné VMS, tak i jednotlivé prvky VSS, které je přijímají, zpracovávají a odesílají dál do systému.

Z analogových a AHD kamer se data přenáší formou analogového signálu. Přenášená data jsou tzv. „raw“, čili nekomprimovaná. Díky tomu nedochází k žádným prodlevám, obraz se nezasekává, nekostičkuje apod. Oproti tomu je z IP kamer přenášen signál digitální, který je zároveň komprimovaný pomocí různých kompresních formátů. Komprese v tomto případě probíhá přímo v kameře. Díky využité digitální technologii nedochází u IP kamer k degradaci přenášeného signálu vzdáleností. V některých případech však může nastat zpoždění obrazu vlivem náročnosti jeho zpracování, který probíhá v kameře. HD-SDI kamery, jakožto zástupce hybridní technologie, poskytují nekomprimovaný digitální signál. Výhoda přenosu vysokého rozlišení je tak kompenzována vysokými nároky na přenosové trasy. [4] [7]

VMS dále dokáže rozlišit přijímaná data na kontinuální nebo událostní. Určitá kamera v VSS může být nastavená na nepřetržité nahrávání. Kvůli úspoře místa na disku je kvalita kontinuálního nahrávání nastavena na nižší. Pomocí VMS můžeme nastavit, aby v případě nějaké definované události kamera začala nahrávat ve vysoké kvalitě. [7]

Transfer dat

Transfer dat na hardwarové úrovni probíhá dvěma základními způsoby, drátově nebo bezdrátově. První způsob má stále své majoritní zastoupení, neboť bezdrátové řešení se užívá jen ve specifických podmínkách a zpravidla při přenosu dat na menší vzdálenosti. [2]

Drátový transfer dat

V případě analogových, HD-SDI a AHD kamer se standardně využívá koaxiálního kabelu ukončeného BNC konektory. Maximální délka vedení je závislá na kvalitě koaxiálního kabelu. Pro přenos je možné využít i UTP kabelu, který může být napojen na stávající koaxiální kabel pomocí tzv. video balunů. Baluny upravují video signál pro impedanci UTP kabelu a zároveň obsahují filtrační a ochranné prvky, jako je přepěťová ochrana nebo filtrace šumu. Nevýhodou tohoto řešení je nutnost další kabeláže, která slouží pro přenos audia či napájení.

IP kamery pro přenos nejčastěji využívají Ethernetovou síť (zpravidla standard 100BASE-T a 1000BASE-T), a klasické UTP kabely, zakončené RJ-45 konektory, po kterých lze současně přenášet i napájení. Tato technologie se zkráceně nazývá PoE (Power over Ethernet) a v oblasti IP kamer je v dnešní době takřka nutností. Kamery se do systému většinou připojují skrze speciální síťové přepínače (tzv. PoE switch), případně má uživatel možnost zakoupit PoE injektory, které slouží k tvorbě napájeného Ethernetového spojení. Směrem od přepínače k ostatním prvkům sítě jsou již znatelně vyšší nároky na přenosovou rychlost, a proto je mnohdy nutnost využít finančně náročnějších variant Ethernetových sítí, které využívají jako přenosové médium také optických vláken. [2] [7]

Bezdrátový transfer dat

Druhým způsobem, avšak ne tak zcela efektivním a rozšířeným, je bezdrátový transfer dat podle standardu IEEE 802.11. Některé typy kamer jsou proto vybaveny Wi-Fi rozhraním, které nejčastěji využívá generálně povolené pásmo 2,4 GHz. Je však třeba zmínit, že bezdrátový spoj řeší pouze náhradu signálového kabelu mezi kamerou a záznamovým zařízením, nezajistí tedy zcela bezdrátovou instalaci kamery. [2] [7]

Správa a zpracování dat

Prostřední blok je zastoupen základními hardwarovými prvky VSS, které přijímají data z kamer, zpracovávají je a případně ukládají. Jednotlivé prvky je pak možné v systému různě kombinovat, záleží čistě na preferencích uživatele a jeho finančních možnostech.

DVR

Za éry klasických analogových VSS se převážně využívalo digitálních video rekordérů (zkráceně DVR). Tato zařízení jsou, stejně jako analogové kamery, dnes již prakticky na ústupu. DVR primárně slouží pro ukládání záznamu z analogových kamer, kdy se záznam ukládá na vestavěný disk. Kamery se připojují koaxiálním kabelem do DVR, který může obsahovat i několik desítek konektorů, respektive kanálů pro připojení. Rekordéry většinou disponují i síťovým rozhraním a nabízí se tedy i možnost vzdáleného dohledu pomocí PC. K DVR lze připojit i samostatně monitor pomocí konektorů HDMI nebo VGA. Současné DVR jsou uzpůsobeny modernějším AHD a HD-SDI technologiím, případně existují ještě tzv. hybridní DVR, které slouží pro připojení analogových i IP kamer současně. Specifickou odnoží DVR jsou tzv. video enkodéry, což jsou samostatná zařízení pro převod signálu z analogových kamer na digitální. Funkce video enkodéru tedy může být zahrnuta i přímo v DVR nebo v níže zmíněném NVR. [4] [7]

NVR

V dnešní době nadvlády IP VSS se pro ukládání záznamu používá síťových videorekordérů (zkráceně NVR, z anglického Network Video Recorder). NVR také slouží k základnímu nastavení připojených kamer, neboť stejně jako IP kamery disponují vestavěným webovým rozhraním. NVR se rovněž využívá jako platforma pro instalaci VMS. [4] [7]

Nespornou výhodou NVR je jednoduchá instalace do VSS, kdy je možné využít stávající síťové infrastruktury. Nevýhodou oproti DVR je vzájemná nekompatibilita síťových prvků, kdy použitá zařízení musí být od stejného výrobce, případně alespoň podporovat globální standard ONVIF, jak bude vysvětleno v kapitole 2.1 této práce. [4] [7]

PC

Klasický PC asi netřeba blíže představovat. V komplexu VSS slouží jako univerzální zařízení např. pro instalaci a ovládání VMS, ukládání záznamu z kamer na vestavěný HDD nebo pro zobrazování snímané scény z kamer pomocí připojeného monitoru. Pro pohodlné ovládání VMS je možné k PC připojit např. řídící panel s programovatelnými klávesami. Podle architektury VSS se pak liší nároky na konfiguraci PC, jehož hardware musí být dostatečně výkonný pro bezproblémový chod systému. V dřívějších dobách se také nabízela možnost z PC vytvořit samostatné DVR pomocí speciální analogové karty, která obsahovala konektory pro připojení analogových kamer. Takové řešení je v už v dnešní době značně nepraktické. [4] [7]

Server

Podobné funkce jako osobní počítač nabízí i speciální počítač, obecně nazývaný jako server. Server na rozdíl od PC disponuje výkonnějším hardwarem a je proto vhodnější pro použití v rozsáhlých VSS. Servery jsou nabízeny renomovanými výrobci (např. Dell, HP, IBM, …), kteří ke koupi zároveň poskytují i nadstandardní služby, jako je prodloužená záruka, certifikáty, nebo kompatibilita s konkrétními HW prvky. Servery rovněž oproti PC pracují na odlišném operačním systému. [7]

Uložiště

Uložiště je obecný pojem pro zařízení, které slouží k ukládání a uchovávání záznamu. Všechny výše zmíněná zařízení tedy mohou sloužit k této funkci, případně existují i jiná speciální síťové datové uložiště, jako jsou např. NAS (Network Attached Storage). NAS většinou obsahují více pevných disků, uložených do pole RAID. Mezi výhody NAS patří

automatické zálohování, přístup z více PC či chytrých telefonů, případně synchronizace a sdílení dat napříč různými platformami. Uložištěm je v případě IP VSS i samotná IP kamera, která může záznam ukládat na vestavěnou paměťovou kartu. Dodatečným uložištěm mohou být i různé externí HDD, vzhledem k jejich vlastnostem ale nejsou vhodné pro větší aplikace. [4] [7]

Operátor

Poslední blok schématu reprezentuje oblasti, do kterých vstupuje přímo vstupuje pověřená osoba, respektive operátor, mající na starost dohled a kontrolu nad celým systémem. Pokud je VSS integrován i s jinými systémy, operátor má možnost je ovládat skrze rozhrani VMS. První částí je zobrazování, tedy hardwarové prvky, které poskytují vizuální kontrolu nad VMS.

Monitor

Nejčastějším způsobem je sledování obrazu na monitoru připojeném k PC nebo serveru. Pokud využíváme více softwarových řešení, např. VMS + nádstavbový SW modul pro video analýzu, je vhodné využít více monitorů pro lepší přehled. [7]

Videostěna

Videostěna je označení pro speciální multi-obrazové zařízení, které kombinuje několik monitorů, video projektorů nebo televizí do jednoho celku. Typickou vlastností obrazovek je užití co možná nejtenšího rámečku, aby byl zachován dojem jedné velké obrazovky. Videostěny se aplikují u rozsáhlých kamerových instalací pro zvýšení přehlednosti a komfortu dohledu. Typickou aplikaci videostěn jsou kontrolní místnosti v letištních halách, stadionech nebo ve velkých podnicích. [8]

Chytrý telefon/tablet

Dnešní trendy mobilních technologií nahrávají i expanzi VMS na mobilní platformy. Všudypřítomné chytré telefony (nazývané také smartphony) nebo tablety tak mohou sloužit i jako dodatečné dohledové zařízení. Na trhu se nachází řada VMS, které podporují i instalaci softwarového klienta na uživatelův smartphone, a tím umožňují ovládání alespoň základních funkcí. Pochopitelně takové řešení není vhodné aplikovat na místa, kde je zapotřebí neustálý dohled operátora. Navíc díky poměrně malým rozměrům displeje těchto zařízení je dohled značně nepřehledný a je spíše považován za krajní řešení. [7]

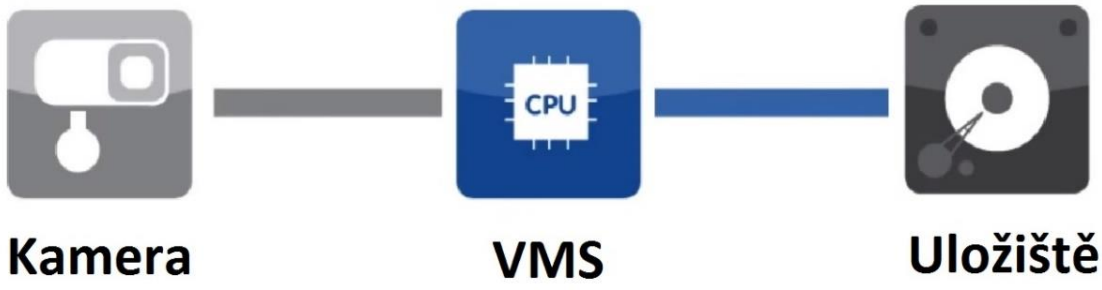
Akční členy

Druhou částí bloku operátorova dohledu jsou akční členy. Většina moderních IP kamer disponuje logickými vstupy a výstupy pro připojení externích zařízení. Při vetším počtu kamer je praktičtější do systému zahrnout expanzní I/O modul, který obsahuje hned několik logických vstupů a výstupů. Vstupy modulu slouží především k přenesení logické informace z prvků PZTS, EPS nebo ACCESS. Tato informace je zpracována VMS, který následně dle uživatelské konfigurace vydá příkazy ostatním prvkům VSS a zároveň upozorní operátora. Dále může dojít např. k natočení kamery do předem definované pozice a spuštění nahrávání záznamu ve vysoké kvalitě. Logické výstupy naopak slouží k odesílání informace do externích zařízení. Operátor tak má možnost pomocí VMS rozhraní manuálně ovládát elektronické brány, závory či venkovní osvětlení. Případně je možné prostřednictvím VMS nakonfigurovat tyto činnosti na automatické spínání. [2] [7]

1.2.2 Struktura VMS

VMS software se může fyzicky nacházet v různých částech VSS, záleží na preferencích daného výrobce nebo uživatele. Toto místo označíme jako platformu. Jednotlivé platformy vychází ze dvou různých koncepcí - struktur VMS, v jakých je software dodáván zákazníkům. Zmíněné koncepty jsou nazývány jako centralizované a decentralizované VMS. Dále existuje ještě jedna speciální kategorie, která je založená na bázi tzv. cloud computingu.

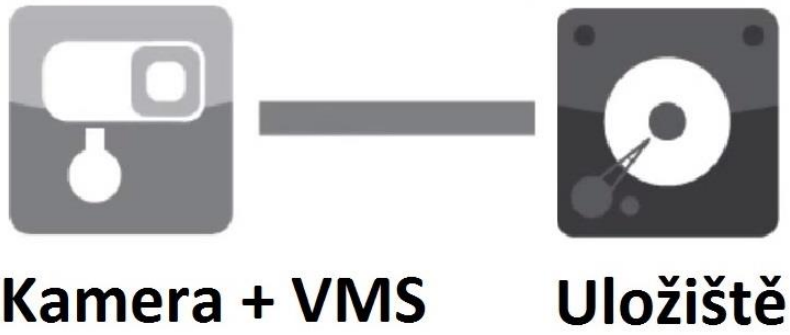
Centralizovaný VMS (platforma PC, server nebo NVR)



Obr. 4. Centralizovaný VMS [9]

V případě centralizovaného způsobu je VMS nainstalován na centrální nahrávací zařízení, což je zpravidla PC, server nebo NVR. Více jak 90% současných VMS je postavených na centralizované bázi. Centralizované VMS mají, dle konkrétního výrobce, nastavenou svou vlastní licenční politiku, tzn. uživatel je nucen si zakoupit jednotlivé licence podle počtu připojených kamer a dalších zařízení. [9] [10]

Decentralizovaný VMS (platforma kamera)



Obr. 5. Decentralizovaný VMS [9]

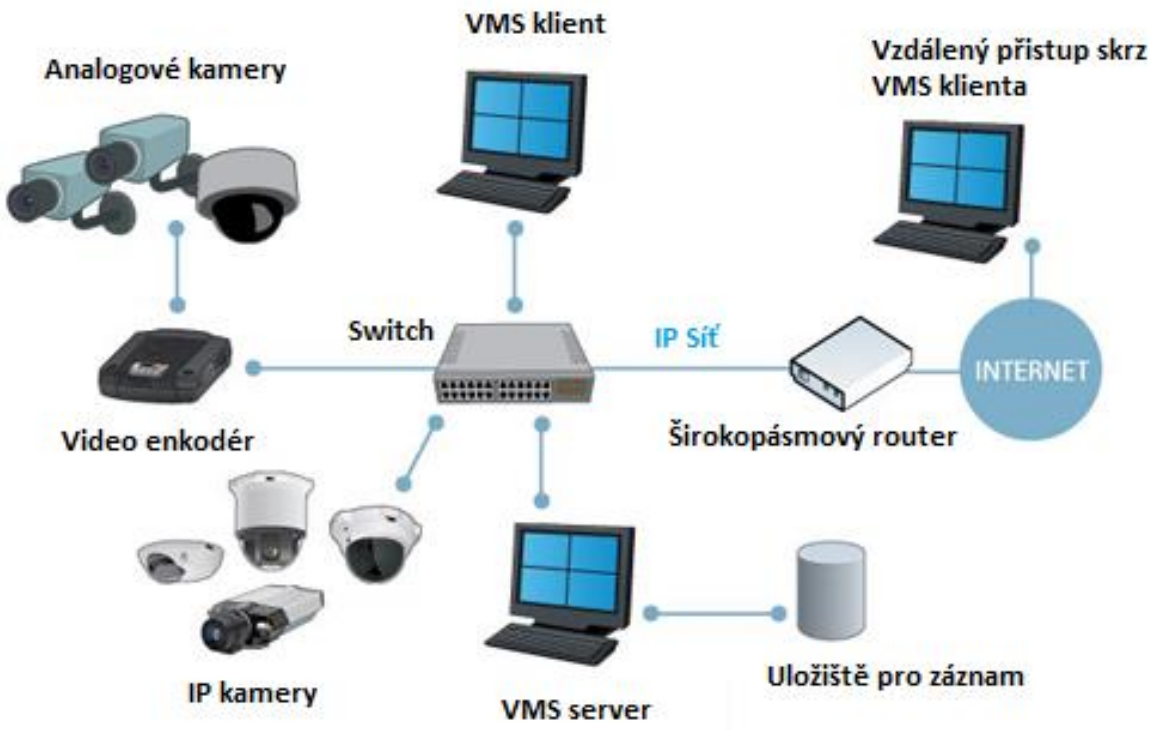
V případě decentralizovaného způsobu je VMS nainstalován přímo v jednotlivých kamerách. Z toho vyplývá, že každá kamera v sobě má zabudovanou funkcionalitu NVR. Kamery tedy mohou nahrávat přímo do jakékoliv databáze a jakéhokoliv uložiště. Uživatelé decentralizovaného VMS navíc nemusí kupovat žádné licence. V současné době se však na trhu vyskytuje velice malé množství VMS, které jsou postaveny na decentralizované struktuře. Příčinou této situace je pravděpodobně nižší zisk z prodeje softwaru, než v případě centralizovaného VMS. [9] [10]

1.2.3 Platformy VMS

Platforma PC/server

Řešení pro správu videa založené na bázi PC či serveru nabízí značné množství výhod vycházejících z konceptu otevřené platformy. Tou hlavní je velice snadné přidávání nových funkcí a prvků do systému, jako jsou externí uložiště, firewally nebo antivirové ochrany. Platforma PC/serveru je také plně škálovatelná, díky čemuž můžeme do systému přidat libovolný počet síťových video prvků. Hardware systému lze rozšířit nebo modernizovat tak, aby dosáhl požadavků posledních trendů. Otevřená platforma rovněž umožňuje snadnější integraci s jinými systémy (ACCESS, PZTS, EPS, …). [7]

S platformou PC/serveru je úzce spjata architektura klient-server, kterou nabízí pokročilé VMS softwary. Platforma pochopitelně nabízí i samostatnou instalaci pouze na jedno PC, uživatelé však mají možnost tento koncept rozvinout různými směry právě díky vlastnostem zmíněné architektury. [7]



Obr. 6. Platforma PC/server [7]

Uvedené schéma slouží jako příklad, jak by dané řešení mohlo vypadat. Mimo klasických IP kamer lze do systému zahrnout i starší analogové kamery, jejichž signál by byl prostřednictvím video enkodéru převeden na digitální. V systému by se nacházel PC, na kterém by byl nainstalován VMS software sloužící jako server. Možnosti správy na serveru se liší dle konkrétního VMS, někteří výrobci umožnují instalaci serveru i klienta na jedno PC. Za předpokladu, že jedna dohledová stanice není dostačující, je možné do systému zakomponovat další stanice pomocí VMS klientů. PC s nainstalovaným VMS klientem by se mohly nacházet jak přímo v budově, tak být rozmístěny kdekoliv po světě a připojeny prostřednictvím Internetu.

Díky vlastnostem této platformy je tedy možné sledovat live stream nebo záznam z více pracovních stanic. Administrátor VMS serveru má možnost nastavovat a přidělovat práva dalším uživatelům, kteří jsou do systému připojeni pomocí VMS klienta. Architektura je také snadno škálovatelná, díky čemuž je snadné do systému zahrnout další prvky pro dohled a správu, např. instalací VMS klienta na chytrý telefon. Řešení na bázi klient – server je vhodné pro aplikaci především ve středně velkých a velkých firmách, jejichž VSS mohou čítat až několik desítek kamer. [7]

Platforma NVR

Obecně se takový model označuje jako „Edge“, tzn. VMS je nainstalován přímo na konkrétním síťovém prvku, takzvaně na okraji. Příkladem takového zařízení je níže zmíněný NVR nebo samotná kamera. Hlavní přínosy takového řešení jsou celkové nižší náklady, menší využití šířky pásma nebo nižší požadavky na výpočetní výkon PC či serveru. [7]

Řešení založené na NVR platformě, tedy kdy je VMS předinstalované přímo v síťovém rekordéru, je podstatně jednodušší než v případě PC/serveru. NVR je navržen tak, aby nabízel optimální výkon pro předem stanovený počet kamer a je tedy méně škálovatelný. Díky tomu je řešení vhodné spíše pro menší systémy s malým počtem kamer. [7]

Obr. 7. Platforma NVR [7]

Platforma VMS v kameře

Jak již bylo zmíněno výše, v případě decentralizovaného VMS se software nachází přímo v konkrétní kameře. Takové řešení je však velice specifické a zatím ho praktikuje pouze několik výrobců, jmenovitě např. MOBOTIX. Vývojáři společnosti MOBOTIX tvrdí, že veškeré funkce VMS jsou ovládány pomocí samotných kamer. Tento koncept tak nevyžaduje žádné NVR zařízení a výstup z kamer je zaznamenáván přímo do jakéhokoliv digitálního uložiště (paměťová karta, HDD v PC, NAS, ...). Výhodou takového řešení je nižší finanční nákladnost, neboť není nutné zakupovat licence pro jednotlivé prvky VSS. [9]

Hosting/Cloud

Jedná se o specifické řešení fungující na principu poskytování služby. Koncový zákazník má ve svém objektu pouze kamery a ostatní prvky systému zajišťuje poskytovatel hostingu. Video záznam je nahráván skrze Internet na cloud poskytovatele a uživatel do systému vstupuje pomocí webovou aplikace. Mezi hlavní výhody patří jednoduchá instalace, neboť není zapotřebí konfigurace jednotlivých síťových prvků. Uživatel rovněž nemusí řešit údržbu a provozování serveru. Vzdálený přístup navíc skýtá i vyšší bezpečnost z hlediska předejití krádeže nebo poničení uložišť. Dohled ve formě cloudové služby je vhodný pro podniky s mnoha malými pobočkami či provozovnami, jako jsou například řetězce malých obchodů. Co se týká finanční náročnosti, tak v případě hostovaného videa se platí určitá částka za kameru na měsíc. Příkladem společnosti, jež nabízí službu ve formě hostovaného videa, je například Axis nebo česká firma NetRex. [7]

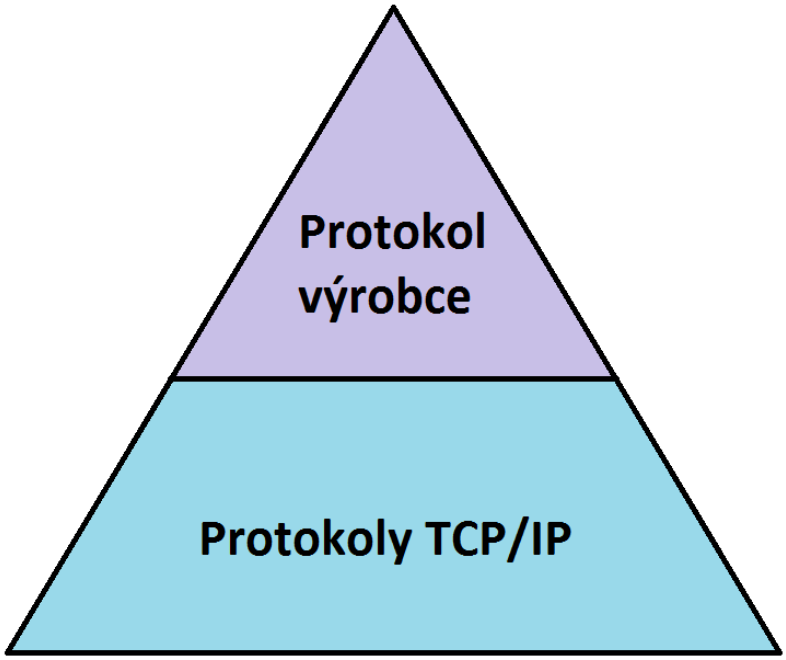
2 ZÁKLADNÍ PROCESY REALIZOVANÉ SYSTÉMY PRO SPRÁVU VIDEA

Druhý segment teoretické části je věnován základním procesům, které jsou realizovány prostřednictvím VMS. Podrobný popis veškerých procesů a s nimi spojených funkcí by vyžadoval několikanásobně větší rozsah práce, a proto budou v této kapitole zmíněny alespoň ty základní, které jsou nutné pro pochopení této problematiky. Procesy nám tedy označují, co všechno v prostředí VMS probíhá a jaké možnosti jsou poté nabídnuty uživatelům. Do oblasti procesů tak lze svým způsobem zahrnout i oblast funkčních vlastností VMS, jejichž komparace bude hlavní náplní praktické části této práce. Procesy a funkce zmíněné v následujících kapitolách budou popsány spíše formou obecné charakteristiky, neboť jednotlivé VMS mají dle výrobce své vlastní způsoby řešení dané problematiky.

První podkapitola se zaobírá možnostmi a způsobům komunikace VMS s ostatními prvky dohledových videosystémů jako celku. Nejprve si tedy charakterizujeme proces komunikace a objasníme konkrétní standardy a protokoly, na jejichž základě komunikace probíhá. Dále se zaměříme na způsob, jakým probíhá management zařízení připojených k VMS.
V navazující části si přiblížíme princip správy událostí v prostředí VMS a uživatelské možnosti v této kategorii. Další kapitoly jsou věnovány administraci uživatelských práv a možnostem správy uložiště. Poslední kapitolou jsou systémové logy, které monitoruji a zaznamenávají veškeré události a změny v systému.

2.1 Komunikace VMS s ostatními prvky systému

Jednou z mála výhod klasických analogových systému oproti IP technologii je vzájemná kompatibilita veškerých prvků VSS, které mohou být dodány od různých výrobců. Nicméně vzhledem k masivnímu rozvoji IP VSS a jeho zastoupení na trhu se bude následující text věnovat převážně oblasti komunikace mezi prvky síťového videa. Navíc současné VSS mohou kombinovat obě zmíněné technologie, případně i v aplikacích pouze analogových kamer je signál dále rozváděn po síti pomocí DVR. Samotné systémy pro správu videa se pak v této sféře potýkají se stejnými problémy, které sužují celé odvětví IP VSS již od počátku vzniku. Nutno však podotknout, že během posledních let došlo ke značnému zlepšení hlavně v kritické podoblasti – standardizace a interoperability. Zásluhu na tom nesou především dva speciálně vytvořené globální standardy ONVIF&PSIA, které vyplňují prázdné místo na poli reciproční komunikace prvků IP VSS. [2] [11]



Obr. 8. Základní úrovně procesu komunikace [11]

Proces komunikace je rozvrstven do několika úrovní, pro znázornění si uvedeme dvě základní úrovně, které reprezentuje obr. 4. Nejnižší úroveň komunikace, kde se používají protokoly TCP/IP, standardizována je. Nadřazená úroveň protokolů výrobců už však standardizována není. Tento problém by mohl v reálné situaci vypadat následovně: NVR bude chtít po IP kameře, aby mu poslala aktuální snímek obrazovky. K tomuto úkonu se často používá standardizovaný protokol HTTP. Samotný způsob, jakým NVR pomocí protokolu HTTP požádá kameru o daný snímek, standardizovaný není. [11]

V zásadě se nabízí dvě řešení výše zmíněného problému. Prvním je používat všechny komponenty VSS od stejného výrobce, z čehož plyne několik nevýhod. Námi favorizovaný výrobce nemusí nabízet kameru určitého typu, VMS nenabízí požadované funkce, či nám jiným způsobem nevyhovuje. Druhým řešením je použití univerzálního komunikačního standardu ONVIF, případně PSIA. ONVIF se týká především evropských a asijských výrobců, zatímco PSIA je zaměřen na americký trh. [11]

ONVIF

ONVIF (Open Network Video Interface Forum), založené v roce 2008 společnostmi Axis Communications, Bosch Security Systems a Sony Corporation, je otevřené průmyslové fórum zabývající se rozvojem globálního komunikačního standardu pro prvky IP videa. V současné době ONVIF čítá bezmála 500 členů, kteří se podílí na jeho dalším vývoji. [12]

Základními stavebními kameny ONVIF jsou:

- standardizace komunikace mezi prvky pracujícími na bázi IP,
- interoperabilita bez ohledu na výrobce,
- otevřenost pro všechny společnosti a organizace. [12]

Z otevřeného standardu ONVIF pramení mnoho výhod, jak pro koncové uživatele, tak pro systémové integrátory či samotné výrobce. Pro zákazníka je to především flexibilita a možnost volby mezi produkty různých značek. Díky této přednosti může i systémový integrátor dodat nákladově efektivní řešení s podstatně jednodušší instalací. Výrobci začlenění do asociace ONVIF mají větší přehled na trhu, přístup k novým příležitostem, projektům, a možnosti budování nových partnerství. [11] [12]

Verze standardu ONVIF se dělí na profily, které uživateli garantují vzájemnou kompatibilitu zařízení. Pokud dva komponenty podporují stejný profil, jsou kompatibilní a je zaručena bezproblémová činnost profilem podporovaných funkcí. [11] [12]

Profil S je určený pro IP video systémy. Je zaměřený na audio-video streaming, PTZ ovládání, video konfiguraci a multicast (zjednodušeně - komunikace jednoho odesilatele více příjemcům). V současnosti se na trhu vyskytuje bezmála 5 300 produktu kompatibilní s profilem S. [12]

Profil C slouží pro systémy kontroly vstupu založených na IP technologii. Orientuje se na správu poplachů, událostí a řízení ovládání dveří a přístupu. [12]

Profil G je určen pro média a uložiště na bázi IP. Slouží pro přehrávání audio-video záznamu, vyhledávání záznamů, ukládání a načítání konfigurací a také pro příjem zvuku a metadat ze streamu. [12]

Profil Q je zaměřený na tzv. „Out Of The Box“ vlastnost produktů. Díky ní je produkt schopný fungovat zpravidla ihned po instalaci a bez jakékoliv další konfigurace. Cílem profilu Q je datová integrita, pokročilá bezpečnost a soukromí. [12]

Samotný standard ONVIF je založený na technologiích WSDL+SOAP, RTP/RTSP a formátech MJPEG, MJPEG, MPEG-4 a H. 264, které budou popsány v následujících podkapitolách. [12]

PSIA

PSIA (The Physical Security Interoperability Alliance) je globální konsorcium více než 65 výrobců bezpečnostních systémů a systémových integrátorů. Jeho cílem je, podobně jako u ONVIF, podpora interoperability produktů a systémů pracujících na IP technologii. Vývoj standardu je rozvětven do několika kategorií, které pokrývají značnou část bezpečnostního průmyslu. Tyto kategorie jsou konsorciem označovány jako specifikace a v současné době jich má celkem 7. Abychom se vyhnuli nepřesnému označení, ponecháme jejich názvy v původním znění. Bližší informace o specifikacích jsou k dispozici na oficiálních stránkách PSIA. Jedná se tedy o:

- Service Model,
- Common Metadata & Event Model,
- Common Security Model,
- IP Media Device Specification,
- Recording and Content Management,
- Video Analytics specification,
- Area Control Specification. [13]

Výhody použití PSIA kompatibilních produktů jsou veskrze podobné, jako je tomu u standardu ONVIF. Samotný standard PSIA je založen na technologiích REST, RTP/RTSP a komprimačních formátech MJPEG,MPEG-4 a H. 264, které budou rovněž popsány v následujících podkapitolách. [13]

2.1.1 Komunikační protokoly síťového videa

Pro lepší pochopení problematiky přenosu síťového videa si nejprve definujeme rodinu protokolů TCP/IP, pomocí které komunikují všechna zařízení připojené do Internetu, tedy i komponenty IP VSS. TCP/IP je založen na čtyřvrstvém referenčním modelu, jenž je znázorněn následující tabulkou č. 1. Z důvodu rozlohy tabulky a lepší přehlednosti je tabulka umístěna na následující straně. [14]

Tab. 1. Model protokolu TCP/IP [14]

Vrstva	Popis	Protokoly
Aplikační	Definuje aplikační protokoly TCP/IP a způsob spolupráce hostitelských programů se službami přenosové vrstvy	HTTP, Telnet, FTP, SNMP, DNS, SMTP
Přenosová	Zajišťuje správu komunikačních relací mezi hostitelskými počítači. Definuje úroveň služeb a stav připojení při přenosu dat.	TCP, UDP
Internetová	Vkládá data do datagramů IP obsahující informace o zdrojové a cílové adrese, která slouží k přenosu datagramů mezi hostiteli a sítěmi. Provádí směrování datagramů IP	IP, ICMP, ARP, RARP
Síťové rozhraní	Určuje podrobnosti týkající se fyzického přenosu dat po síti včetně jejich převodu na elektrické signály používané hardwarovými zařízeními, která pracují přímo se síťovými médii, jako jsou koaxiální kabely, optická vlákna nebo kroucené měděné dvoulinky.	Ethernet, Token Ring, Frame Relay

Adresování v IP sítích

Pokud chceme připojit jakékoliv zařízení k Internetu nebo k LAN (Local Area Network – lokální síť), musí takové zařízení disponovat unikátní IP adresou. Pomocí IP adresy tak snadno identifikujeme kameru v síti a zaregistrujeme ji do VMS softwaru. V současné době existují dvě verze IP adresy: starší a stále více rozšířená IP verze 4 (zkráceně IPv4) a novější IP verze 6 (zkráceně IPv6). Hlavním rozdílem mezi verzemi je šířka adresního prostoru, IPv6 používá 128bitů oproti 32 bitům IPv4. [2] [7]

IPv4 adresování

IPv4 adresu tvoří čtyři části, tzv. oktety, které jsou odděleny tečkou. Oktety se zapisují pomocí čísel, které jsou v rozsahu 0-255. Teoreticky se můžeme setkat s IP adresami v rozsahu 0.0.0.0 až 255.255.255.255. [2]

IPv6 adresování

Ipv6 adresa se zapisuje v šestnáctkové soustavě a jednotlivé dvojice bajtů se oddělují dvojtečkami. Hlavní výhodou IPv6 adresy, kromě obrovského množství dostupných IP adres, je schopnost zařízení automaticky si nakonfigurovat vlastní IP adresu pomocí MAC adresy. Mezi další výhody patří rychlejší směrování, šifrování point-to-point a větší podpora mobilních zařízení. [7]

Síťové porty

Porty jsou používány pro identifikaci konkrétní služby nebo aplikace v rámci jedné IP adresy. Díky číslu portu tak IP kamera ví, jak zpracovávat přijímaná data. Čísla portů přiřazuje organizace ICANN a mohou nabývat hodnot od 0 do 65 535, přičemž rozsah 0-1023 je vyhrazen pro nejběžnější služby. [7]

2.1.2 Protokoly využívané pro přenos videosignálu

Ke komunikaci VMS prostřednictvím datové sítě s ostatními prvky VSS je využíváno několika různých protokolů. Základem pro sítě a připojení video přenosových zařízení je IP video protokol. IP je na základě specifikací průmyslových standardů implementován a podporován širokou škálou zařízení. Pro přenos dat je poté nejčastěji využívaný protokol TCP/IP, který zároveň funguje jako nosič pro mnoho jiných protokolů. IP je na základě specifikací průmyslových standardů implementován a podporován širokou škálou zařízení. Díky jejich specifickým vlastnostem má každý z nich své nezastupitelné místo při použití v oblasti síťového videa, jak následně uvádí tabulka č. 2. [2] [15]

Protokol TCP nám zaručuje, že data vyslaná jednou aplikací budou druhé aplikaci doručena ve stejném pořadí, v jakém byla odeslána. Zároveň také garantuje spolehlivé doručení dat (nedochází ke ztrátě). Naproti tomu UDP využívá jednoduchého přenosového modelu a nezaručuje spolehlivost ani pořadí přicházejících dat. Obvykle je proto používán pro časově citlivý přenos dat, což je v případě síťového videa live stream. [7]

Obecně platí, že IP kamery podporují oba protokoly TCP i UDP, ale jen ve výjimečných případech obsahují mechanismus pro přepínání mezi nimi. Naproti tomu VMS určuje, který protokol by měl být použit. V některých případech to dělá automaticky, jindy nabízí možnost manuálního výběru. [2][3]

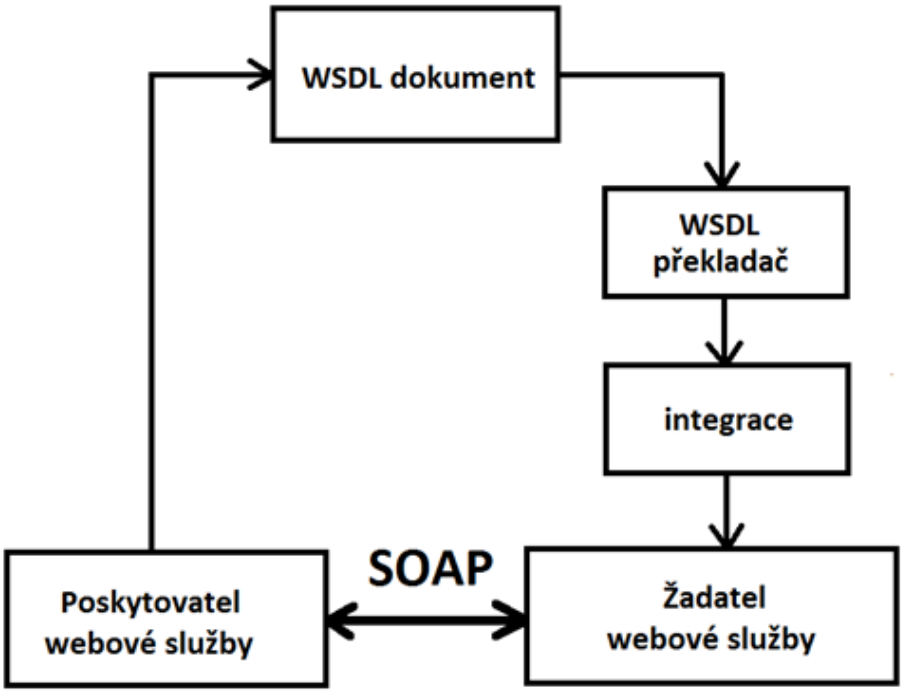
Tab. 2. Protokoly pro přenos videosignálu [7]

Protokol	**Přenosový protokol**	**Port**	**Běžné použití**	**Použití v síťovém videu**
FTP	TCP	21	Přenos souborů přes internet/intranet	Přenos záběrů nebo videa z IP kamer/video serverů na FTP server nebo do aplikace
SMPT	TCP	25	Odesílání e-mailů	Zasílání obrázků nebo upozornění z IP kamery/video serveru pomocí vestavěného e-mailového klienta
HTTP	TCP	80	Prohlížení webových stránek, resp. přijímání stránek s webového serveru	Přenos videa z IP kamery/video serveru, kde tyto zařízení fungují na principu webového serveru, jež zpřístupňuje video uživateli nebo aplikačnímu serveru
HTTPS	TCP	443	Zabezpečený přístup k webovým stránkám pomocí šifrovací technologie	Zabezpečený přenos videa z IP kamery/video serveru
RTP	UDP/TCP	nedefinován	Poskytování zvuku a videa skrze internet	Live stream H.264/MPEG videa, může být Unicast nebo Multicast
RTSP	TCP	554	Slouží k nastavení a ovládání multimediálních relací přes RTP	

2.1.3 Komunikace s webovou službou

Termín webová služba je název standardizované metody, která slouží k interakci mezi aplikacemi na počítačové síti. Tato interakce je založena na osvědčených webových standardech, zejména na značkovacím jazyku XML a jazyku pro popis služeb WSDL. Díky tomu je možné propojit různorodé systémy bez ohledu na použité programovací jazyky, procesory a operační systémy. Komunikace s webovou službou nejčastěji probíhá pomocí technologií nazývaných SOAP nebo REST. [16]

SOAP, respektive jeho současná verze SOAP 1.2, je protokol, který slouží pro výměnu XML zpráv. Tento přenos je obvykle proveden protokolem HTTP, ale může být realizován i jinými, jako jsou SMTP, FTP, JMS a další. [16]



Obr. 9. Schéma protokolu SOAP [17]

Výše uvedené schéma podává přehled o základním principu komunikace s webovou službou. Poskytovatel webové služby (zařízení) implementuje službu nebo služby ONVIF. Tato služba je založená na jazyku XML a popsána pomocí WSDL. Integrace na straně klienta je zjednodušena pomocí nástrojů WSDL překladače, který generuje specifický kód, jenž se používá k integraci webové služby do konkrétní aplikace. Komunikace mezi poskytovatelem a žadatelem webové služby probíhá prostřednictvím výměny SOAP zpráv. Výhodou SOAP zpráv je fakt, že jsou zcela nezávislé na použitém operačním systému a mohou být přepravovány pomocí široké škály internetových protokolů. [17]

REST

REST (Representational State Transfer) je architektura rozhraní, na jejímž základě je postaven standard PSIA. Architektura REST je orientována na zdroje, jimiž mohou být jakékoliv objekty uložené na síti, tedy libovolná data nebo soubor informací. Komunikace s webovou službou probíhá na bázi klient – server. Přenos dat je však možný pouze protokolem HTTP. V porovnání s protokolem SOAP jsou služby REST navrženy především pro publikaci dat, zatímco SOAP spíše pro zpracování dat. REST nabízí jednotné a méně strukturované rozhraní, které je snáze zpracovatelné, než u protokolu SOAP. [18]

2.1.4 Komprese videa a komprimační formáty

Posledním bodem v oblasti komunikace je komprese videa. Kompresi můžeme obecně charakterizovat jako způsob zpracovaní dat, jehož účelem je zmenšit jejich objem při zachování informací v datech obsažených. Komprese videa tedy snižuje datový tok videa za pomocí různých komprimačních algoritmů tak, abychom získali co nejlepší poměr mezi kvalitou výsledného videa a velikostí souboru. [19]

Samotný proces komprese není přímo součástí VMS, neboť je prováděn pomocí kamer, respektive IP kamer. Jak bylo zmíněno v předcházejících kapitolách, z analogových a HD-SDI kamer jsou přenášeny pouze data nekomprimovaná. V případě IP kamer jsou poté komprimovaná data při procesu zobrazování dekomprimována, většinou pomocí PC či serveru. Kvůli vzájemné komunikaci s kamerou tedy musí VMS komprimačním formátům rozumět. Jednotlivé VMS na trhu podporují různé formáty, z nichž se mezi ty nejvyužívanější řadí M-JPEG, MPEG-4 a H. 264. [7] [19]

M-JPEG pracuje na principu komprimace a kódování celých jednotlivých obrázků. Statické části obrazu nejsou filtrovány, a proto vzniká velký objem dat. Výhodou M-JPEG je relativní jednoduchost, díky čemuž jsou kladeny nižší nároky na hardware. Tento typ komprese se používá v případech, kde je zapotřebí co nejrychleji a bez velké HW náročnosti získat původní obraz. [4] [7]

MPEG-4, respektive **MPEG-4 part 2**, zároveň komprimuje přenos videa i audio signálu. Při kompresi se nejprve přenáší tzv. klíčový snímek. V následném snímku se již přenáší pouze rozdíl oproti referenčnímu snímku, čímž se významně redukuje množství dat k přenosu. Formát MPEG-4 je až o 50% účinnější než M-JPEG a klade menší nároky na místo pro záznam. Nevýhodou jsou vyšší nároky na výkonnost hardwaru. [4] [7]

H.264, někdy zvaný též **MPEG-4 AVC** nebo **MPEG-4 part 10**, vychází z předchozího formátu MPEG-4. Jedná se však o modernější standard, který dokáže zredukovat velikost digitálního video souboru až o 80% v porovnání s M-JPEG a o 50% ve srovnání s MPEG-4. Tento typ komprese je využíván téměř všemi současnými VMS pro záznam videosignálu. [4] [7]

2.2 Správa a konfigurace připojených zařízení

Podmínkou správného chodu VMS je fungující komunikace mezi softwarem a hardwarovými prvky. Proces komunikace probíhá na základě různých standardů a protokolů, jak bylo vysvětleno v předchozí kapitole. Pokud tedy komunikační kanál funguje bez jakýchkoliv problémů, je velice snadné jednotlivé zařízení propojit s VMS.

Kamery, popřípadě ostatní prvky síťového videa, se do VMS softwaru zaregistrují pomocí IP adresy. VMS umí automaticky vyhledat připojená zařízení, pak už je pouze na uživateli, s kterými prvky chce svůj software spárovat. Za předpokladu, že je proces registrace úspěšný, je takřka nutností veškeré zařízení nejprve správně nakonfigurovat. Samotná konfigurace kamer je proveditelná dvěma způsoby, a to pomocí vestavěného webového rozhraní kamery, nebo pomocí VMS. Jednou z velkého množství výhod VMS je právě i rozšířená možnost konfigurace kamer, a proto je nastavení ve webovém rozhraní pouze okrajové řešení.

Při prvotním přidání kamery do systému se nejprve nastavuje uživatelské jméno a heslo. Pokud kamera nebyla nikdy používaná, nebo byl proveden reset do továrního nastavení, je nutné nastavit nové jméno a heslo. V opačném případě se pouze do kamery přihlásíme. Dále je nezbytné nastavit několik základních údajů, jako je aktuální datum a čas, časové pásmo, identifikační název kamery apod. Po úspěšném absolvování nezbytných nastavení je možné kameru umístit do oblasti, ze které bude snímat scénu. Podle vlastností snímané scény se poté prostřednictvím VMS konfigurují obrazové vlastnosti kamery. Do této kategorie spadá jas, kontrast, ostrost, hloubka barev, expozice, otočení obrazu o požadovaný úhel a mnoho dalších.

Dalším bodem procesu konfigurace kamer jsou tzv. video profily, které upřesňují vlastnosti video streamu. Uživatel si nastavuje vlastnosti těchto profilů podle svého uvážení. Jednotlivé VMS nabízí rozdílný počet profilů, pro vysvětlení budou jako příklad stačit 2 profily, které ponesou označení „Low“ a „High“.

Ve vlastnostech profilu se nastavuje zejména rozlišení, snímková frekvence, komprese a kompresní formát. Z názvu profilů je patrné, v jakých situacích je budeme chtít využívat. Profil Low bude využit pro kontinuální nahrávání a je tedy vhodné nastavení provést s ohledem na úsporu místa v uložišti. V nastavení proto volíme nízké rozlišení, snímkovou frekvenci a odpovídající kompresní formát. Profil High bude naopak pro případy, kdy dojde k nějaké konkrétní události, jak bude vysvětleno v následující kapitole. Pro co možná nejlepší kvalitu záznamu proto zvolíme maximální dostupné nastavení.

2.3 Správa a konfigurace událostí

Jednou z nejdůležitějších funkčních vlastností každého VMS softwaru je bezpochyby možnost správy a konfigurace událostí. Před pořízením VMS by si měl každý uživatel zjistit, co všechno software umožňuje a zdali dané funkce opravdu využije. Jednotlivé VMS se v této kategorii od sebe liší především v množství nabízených funkcí. Největší odlišnosti jsou převážně v možnostech videoanalýzy, která je buď přímo součástí VMS, nebo je s VMS svázána jako software třetí strany. Rozdíly mezi VMS nejsou dané pouze výrobcem softwaru, ale i jednotlivými edicemi. Obecně platí, čím dražší edici si pořídíme, tím více funkcí dostaneme. Příkladem lze uvést českou společnost ATEAS, jejichž VMS řešení je dostupné v 5 různých edicích.

Jak již bylo zmíněno v kapitole 1.1.1, za událost je považována předem definovaná situace, která může mít negativní dopad na zdraví či majetek člověka, případně jakýmkoliv způsobem ohrozit funkčnost celého systému. Abychom dokázali na tyto situace efektivně reagovat, je zapotřebí vhodná konfigurace prostřednictvím VMS. Jednotlivé události na úrovni VMS fungují na dvoufázovém principu spouštěče a následné akce, jenž budou popsány v následujících podkapitolách. Ke každé události je navíc možné nastavit vlastní časový plán, který určuje, kdy na danou událost software odpovídá. V časovém plánu se nastavuje zejména den, popřípadě určitá denní doba, podle režimového plánu podniku. V pracovní dny tak VMS reaguje na jiné typy událostí, než v době víkendu apod. Zaznamenané události je pak možné exportovat ve formě dokumentu a přenášet dle vlastního uvážení.

2.3.1 Spouštěče

Spouštěč (angl. Trigger) popisuje, co se musí stát, aby mohla být spuštěna navazující akční procedura. Uživatel si prostřednictvím VMS vytváří spouštěč, respektive určitou podmínku. Když daná podmínka nastane, VMS automaticky reaguje podle instrukcí, které jsou zadány v bodě akce.

Mezi základní spouštěče patří:

- videoanalýza obrazu,
- systémová chyba,
- signál z I/O,
- akční tlačítko.

Videoanalýza

Videoanalýzu můžeme charakterizovat jako soubor různých funkcí, které zkoumají živý obraz či záznam z kamer za účelem vyhledání specifické události. Do této kategorie spadá detekce pohybu, sabotáže kamery, zábran či překážek, rychlosti pohybujícího se cíle nebo zanechaného cizího předmětu. Dále funkce počítání objektů v obraze, analýza a rozpoznání tváře, rozpoznání registračního značek vozidel a mnoho dalších. Výhodou videoanalýzy živého obrazu je snížení nároků na pozornost operátora. V případě analýzy záznamu je to především úspora času, kdy operátor nemusí kontrolovat celý záznam. [11]

Analýzu obrazu mohou provádět 3 různé části VSS, a to samotná IP kamera, záznamové zařízení (např. NVR), nebo PC/server. Proces analýzy však klade vysoké nároky na výpočetní výkon, a proto na ně musí být daná platforma uzpůsobená. V dnešní době má řada IP kamer na trhu vestavěné alespoň základní analytické funkce, jako je detekce pohybu nebo sabotáže. U takových kamer je však třeba počítat s vyšší cenou, než za jakou se prodávají kamery bez videoanalýzy. Výhodou je nezávislost kamer na zbytku systému, tzn. pokud dojde k poruše jedné kamery, neovlivní to ostatní zařízení. Zákazník má také možnost přenechat analytické funkce záznamovému zařízení a pořídit si levnější variantu kamer. U takového řešení je ovšem riziko poruchy záznamového zařízení, kdy v případě jeho výpadku přicházíme o veškerou videoanalýzu. V situacích, kdy je nezbytné nasazení pokročilých videoanalytických funkcí, jako je rozpoznání obličeje nebo SPZ aut, není výpočetní výkon

kamer nebo záznamových zařízení přijatelný. Z toho důvodu se jako platforma používá dostatečně výkonný PC nebo server, jehož hardware je uzpůsoben vysokým požadavkům videoanalýzy. [11]

Pokud tedy dojde jedním z výše zmíněných zařízení např. k detekci pohybu v přednastavené zóně, VMS vykoná veškeré uživatelem zadané instrukce. Jedná se např. o upozornění operátora, aktivace nahrávání v nejvyšší kvalitě (resp. nejkvalitnějšího video profilu), zobrazení pohledu z dané kamery, a mnoho dalších. [11]

Systémová chyba

Jedná se o jakýkoliv typ problému spojený s chodem systému. Pokud daný problém vyvstane, hrozí nefunkčnost některých částí nebo dokonce celého VSS. Správně nakonfigurovaný VMS musí umět rozlišit typ systémové chyby a její stav neprodleně oznámit operátorovi. Mezi ty nejčastější patří nedostatek místa v uložišti, nepřístupný síťový disk nebo ztráta spojení s kamerou.

I/O

Tento typ spouštěče je určen pro signály, které VMS přijímá ze zařízení připojených na logické vstupy nebo výstupy kamer, případně expanzního I/O modulu. VMS tak může obdržet poplachovou informaci např. z kouřového detektoru a provést nezbytné úkony k odvrácení hrozícího nebezpečí. Základem je v těchto situacích spuštění alarmu a upozornění operátora, dále pak zobrazení pohledu kamery z místnosti, kde hrozí požár nebo otevření/uzavření dveří.

Akční tlačítko

Jedná se o specifický spouštěč, jež je manuálně ovládán operátorem. Uživatel má možnost si prostřednictvím VMS rozhraní vytvořit několik vlastních softwarových tlačítek, kterým lze přiřadit určité funkce. Jedním tlačítkem je také možné ovládat několik funkcí současně. Příkladem použití může být tlačítko určené pro střežení perimetru, které po stisknutí operátorem vyšle povel PTZ kamerám, aby se natočily do přednastavené pozice.

2.3.2 Akce

Jak již bylo zmíněno výše, pojem akce v sobě zahrnuje veškeré úkony, které VMS vykoná při aktivaci určitého spouštěče. K jednomu spouštěči je možné přiřadit vícero akcí, jež budou provedeny podle zadané posloupnosti.

Mezi základní typy akcí patří:

- zahájení nahrávání,
- vyvolání alarmu,
- odeslání zprávy,
- zobrazení pohledu z kamery,
- odeslání logické informace na výstup.

Zahájení nahrávání

Spuštění nahrávacího procesu je považováno za úplný základ a je vhodné téměř v každé situaci. Pokud už je systém nastaven na nepřetržité nahrávání, je možné alespoň upravit parametry kvality výsledného záznamu. V případě aktivace přiřazeného spouštěče je vhodné zahájit nahrávání v nejvyšší kvalitě pro usnadnění následného zkoumání záznamu.

Vyvolání alarmu

Tato akce slouží především pro upozornění operátora. Při aktivaci určitého spouštěče je zahájena poplachová procedura, která rozešle informaci do všech klientských stanic VMS. Oznámení o poplachu je prioritní, tzn. alarmový stav se zobrazí na popředí VMS rozhraní, nejčastěji ve formě vyskakovacího okna. K vizuálnímu upozornění je možné přidat i přehrání zvukového záznamu, aby se minimalizovala šance, že si operátor nevšimne změny stavu.

Odeslání zprávy

Funkce je vhodná zejména pro automatické upozornění kohokoliv, kdo nemá k dispozici okamžitý přístup do VMS, případně dané VMS není pod stálým dohledem operátora. Tento typ akce je vhodný přiřadit událostem s vysokou prioritou, aby byl v okamžiku aktivace spouštěče upozorněn např. i majitel objektu. Zpráva se odesílá většinou formou e-mailu nebo SMS, z čehož plyne nutnost Internetového připojení.

Zobrazení pohledu z kamery

Za předpokladu, že je na určité kameře detekována událost, je vhodné přenést pohled z kamery do popředí VMS rozhraní. Operátorovi je tak okamžitě poskytnuta vizuální podpora z místa události a může na vzniklou situaci lépe reagovat.

Odeslání logické informace na výstup

Pokud jsou do systému integrovány externí zařízení skrze logické výstupy, uživatel má možnost nakonfigurovat jejich ovládání pomocí VMS. Vyslání logické informace na výstup může být prováděno buď automaticky aktivací konkrétního spouštěče, nebo manuálně operátorem pomocí akčního tlačítka. Funkce je vhodná zejména pro otevírání dveří, rozsvěcení světel atd.

2.4 Administrace uživatelských práv

Při nasazení VMS v rozsáhlejším objektu s velkým množstvím kamer, kdy je zapotřebí dohled jednoho nebo více operátorů, jsou možnosti administrace uživatelských práv neocenitelné. Pochopitelně pokud si zákazník pořizuje jednodušší VMS např. pro malou prodejnu, stává se v konečném důsledku zároveň administrátorem i operátorem systému, a proto možnosti administrace pro něj nemají význam. Jelikož jsou ovšem VMS primárně vyvíjeny právě pro aplikace do objektů, kdy má k systému přístup více uživatelů, pokusíme se nyní charakterizovat jejich jednotlivé možnosti.

Obdobná situace, jako u jiných funkcí VMS, je i v oblasti managementu uživatelských práv, která je značně rozdílná podle výrobce či edice softwaru. Společným jmenovatelem veškerých VMS je však schopnost vytvoření jednotlivých úrovní oprávnění, ke kterým lze přiřadit množství uživatelů podle našich potřeb. Základní rozdělení uživatelských oprávnění je na 3 různé úrovně:

- administrátor,
- operátor,
- dozorce.

Administrátor

Role administrátora je ve všech verzích VMS podobná, neboť zaručuje neomezený přístup do celého systému, včetně přístupu ke všem kamerám a logickým vstupům a výstupům. Tato úroveň oprávnění je nadřazená ostatním úrovním, tzn. pouze pomocí administrátora můžeme přiřazovat práva jiným úrovním. Role administrátora je taktéž nezbytná ke konfiguraci ostatních funkcí VMS.

Operátor

Role operátora se už dle verze VMS liší, povětšinou však umožňuje přístup k veškerému živému i zaznamenanému videu. Tento přístup je omezen pouze na administrátorem určené kamery a logické I/O. Operátor má navíc přístup ke všem ostatním funkcím VMS, které ovšem nemůže nijak konfigurovat.

Dozorce

Dozorce má přístup pouze k aktuálnímu streamu z kamer, které jsou určeny administrátorem. Na rozdíl od operátora tak nemá možnost sledovat záznam a pochopitelně ani žádným způsobem provádět konfiguraci systému.

K jednotlivým rolím, respektive úrovním oprávnění, lze pak přiřazovat libovolné množství uživatelů. Jako příklad si uvedeme blíže nespecifikovaný VMS, jenž je spravován jedním administrátorem. Jelikož je v objektu zapotřebí nepřetržitý celodenní dohled, jsou do systému zakomponováni 2 operátoři, kteří mají na starost dohled v denní a noční dobu. Jelikož má administrátor možnost přiřadit ostatním uživatelům různá oprávnění, budou mít v tomto případě operátoři přístup do všech kamer a k jejich jednotlivým funkcím. Pro bezpečnost celého systému může navíc administrátor odebrat operátorům práva na export záznamu z kamer. Operátor si tedy může záznam prohlížet, ale nebude mu umožněno jej vynášet ven z objektu. Kromě operátorů bude do systému zahrnuto i několik uživatelů s oprávněním dozorce. Těm sice bude umožněn přístup do jednotlivých kamer, ale nebudou moci ovládat PTZ funkce nebo spouštět manuální nahrávání.

2.5 Správa uložiště

Jak již je z názvu patrné, termín správa uložiště v sobě zahrnuje veškeré procesy VMS, které se týkají ukládání, přesouvání a managementu dat. Na otázky kam, kdy a co se ukládá, uživatel (s odpovídajícím oprávněním) odpovídá pomocí konfigurace prostřednictvím VMS. Před spuštěním procesu nahrávání z kamer je tedy nejprve nutné stanovit, jakým způsobem bude záznam ukládán.

Základní nabídkou jednotlivých VMS je možnost volby, kam budeme ukládat záznam. V rozhraní VMS můžeme zvolit lokální disk umístěný v počítači, síťový disk NAS, případně jakýkoliv dostupný externí disk. Podle rozlohy VSS a kvality nahrávání z kamer je pochopitelně nutné počítat s jistým objemem dat, a proto by mělo zvolené uložiště mít dostatečnou kapacitu. Jakmile si uživatel zvolí výsledné uložiště, VMS mu automaticky nabídne možnost

alokace disku, což lze obecně charakterizovat jako přidělení omezených zdrojů. V prostředí VMS je tato funkce vhodná především v případech, kdy chceme ukládaným datům vymezit jen určitý prostor na disku. Na závěr se k vybranému disku přiřadí kamery, z kterých bude záznam ukládán právě na zvolený disk. Jednotlivé uložiště je také možné pojmenovat pro lepší přehlednost.

Standardem dnešních VMS je i dodatečná funkce ukládání, nazvaná „fail-over recording". Pojem fail-over znamená, že je záznam zároveň ukládán na dodatečné uložiště (např. paměťová karta v kameře) pro větší bezpečnost v případě selhání síťové infrastruktury. Pokud tedy nastane jakýkoliv problém, záznam se ukládá na paměťovou kartu. Po navrácení systému do původního funkčního stavu se záznam automaticky převede na hlavní uložiště

2.6 Systémové logy

Posledním bodem zájmu této práce v oblasti procesů VMS jsou systémové logy. Jedná se o základní funkci VMS, která slouží pro co možná nejlepší přehlednost celého systému a ke zpětnému dohledání jakýchkoliv změn. Pokud tedy uživatel např. přidá novou kameru, upraví uživatelské práva nebo vytvoří nové události, VMS automaticky zapisuje veškeré provedené změny a ukládá je do logů. Ke konkrétní změně je automaticky doplněn i datum a čas, někdy také krátká vysvětlivka. Veškeré logy může navíc uživatel exportovat formou textového dokumentu.

Systémové logy jsou na úrovni VMS vedeny formou tabulek. Pro větší přehlednost bývají rozděleny do několika kategorií, jako je např. alarm, událost, audit, info a podobně. Pokud VMS vyhlásí poplach na základě uživatelské konfigurace, operátor je většinou informován pomocí vyskakovacích oken a různých upozornění. Zároveň však VMS zapisuje informaci o poplachové události do logu. Operátor většinou nemá oprávnění zasahovat do konfigurace systému, a proto jsou veškeré logy zpětně dohledatelné v jakémkoliv časovém intervalu. Tato funkce tedy slouží pro komplexní bezpečnost systému a může být velice užitečná v případech aplikace VMS ve velkých objektech, kdy je softwarem obsluhován více operátory.

Jednotlivé VMS mají pochopitelně své vlastní řešení systémových logů, v zásadě se však v mnohém neliší. Na níže uvedeném obrázku si pro znázornění představí systémové logy v podobě řešení VMS Axis Camera Station. V logu můžeme spatřit zápis systémových změn, které se týkají přidání kamery, zahájení video streamu, spuštění manuálního nahrávání a

konfigurace událostí, konkrétně pak detekce pohybu. Od prvního pohledu je patrné, jaká změna byla provedena, kdy byla provedena, a kým byla provedena.

Alarms Events Audit

Time	Message	User	Computer
7.4.2016 11:41:19	Video streaming stopped from camera AXIS M1125	Martin-PC\Martin	MARTIN-PC
7.4.2016 11:41:08	Video streaming started from camera AXIS M1125	Martin-PC\Martin	MARTIN-PC
7.4.2016 11:41:05	Rule: Rule edited	Martin-PC\Martin	MARTIN-PC
7.4.2016 11:40:39	Motion detection settings for AXIS M1125 edited	Martin-PC\Martin	MARTIN-PC
7.4.2016 11:40:32	Video streaming stopped from camera AXIS M1125	Martin-PC\Martin	MARTIN-PC
7.4.2016 11:40:30	Manual recording stopped for AXIS M1125	Martin-PC\Martin	MARTIN-PC
7.4.2016 11:40:23	Manual recording started for AXIS M1125	Martin-PC\Martin	MARTIN-PC
7.4.2016 11:40:13	Video streaming started from camera AXIS M1125	Martin-PC\Martin	MARTIN-PC
7.4.2016 11:40:05	Recordings search in interval 7.4.2016 0:00:00 and 8.4.2016 0:00:00	Martin-PC\Martin	MARTIN-PC
7.4.2016 11:39:54	Camera: AXIS M1125 added	Martin-PC\Martin	MARTIN-PC

Obr. 10. Systémové logy

II. PRAKTICKÁ ČÁST

3 NÁVRH EVALUAČNÍHO SYSTÉMU PRO HODNOCENÍ VMS

V první kapitole praktické části diplomové práce se budeme zabývat tvorbou evaluačního systému, pomocí něhož se pokusíme o efektivní a přehledné ohodnocení vybraných VMS softwarů. Jak vyplývá z části teoretické, jednotlivé VMS řešení se od sebe v mnohém liší. Z toho důvodu je zapotřebí vytvořit takový systém, který dokáže pokrýt co možná nejširší oblast funkčních vlastností a zároveň bude snadno aplikovatelný na veškeré VMS.

Výsledné ohodnocení VMS bude vycházet z dílčích hodnocení, kterých software dosáhne v jednotlivých kategoriích. Součástí kategorií jsou dále individuální kritéria, která znázorňují množinu konkrétních funkčních vlastností daného VMS. Mimo těchto vlastností jsou do systému zahrnuty i oblasti, jež jsou při výběru vhodného softwaru neméně důležité, a sice uživatelské rozhraní, hardwarové nároky na provoz nebo výsledná cena. Celkový koncept evaluačního systému vychází z vlastních autorových poznatků, které získal během zpracování diplomové práce z mnoha různých zdrojů, jenž jsou angažovány v této oblasti. Jedná se především o školení a partnerské dny společnosti Axis, konzultace s několika distributory hodnocených VMS, nebo např. webový server IPVM.com, který sdružuje řadu výrobců, odborníků a distributorů téměř čehokoliv, co se týká IP videa. IPVM obsahuje široké spektrum odborných článků a recenzí na danou problematiku, navíc nabízí i možnost konzultace s ostatními členy prostřednictvím fóra. Server je však přístupný pouze osobám s placeným členstvím, které v tomto případě uhradila Fakulta aplikované informatiky.

Potencionální uživatel hodnocených VMS tak může pomocí této práce získat dodatečné informace, které mohou být užitečné při procesu rozhodování a nákupu daného softwaru. Je však třeba mít na paměti, že veškeré hodnocení je čistě subjektivní a nemusí se zcela ztotožňovat s recenzemi jiných uživatelů nebo webových serverů, orientovaných na obdobnou problematiku.

V následujících částech práce si pomocí tabulky demonstrujeme jednotlivé kategorie a příslušné kritéria evaluačního systému, a pokusíme si objasnit, na jakém principu bude probíhat proces evaluace. Poté se již přesuneme ke konkrétní aplikaci zmíněného systému na vybrané VMS. Závěrem práce si představíme 2 konkrétní laboratorní úlohy, které budou součástí výuky v novém předmětu na téma kamerových systémů.

Tab. 3. Přehled kategorií a kritérií evaluačního systému

Kategorie	Kritéria
Monitoring a záznam	Možnosti živého pohledu Možnosti prohlížení záznamu Ovládání PTZ funkcí Možnosti nastavení obrazových a zvukových vlastností
Komunikace a podpora zařízení	Podpora zařízení Architektura a platformy Možnosti integrace s jinými systémy
Management a konfigurace událostí	Možnosti konfigurace událostí Inteligentní funkce
Administrace uživatelských práv	Možnosti administrace práv
Správa uložiště	Možnosti správy uložiště
Uživatelské rozhraní	Instalace Přehlednost a ovládání Lokalizace Technická podpora
Hardwarová náročnost	Provozní požadavky
Finanční náročnost	Licenční model a výsledná cena

3.1 Princip evaluačního procesu

Evaluační systém bude založen na bodovém ohodnocení jednotlivých kritérií v dané kategorii. Každé kritérium tedy obdrží určitý počet bodů, jehož rozpětí bude stupnice od 0 do 5. Bodům bude odpovídat také procentuální hodnota, která slouží pro zpětné převedení dílčích výsledků, jak si následně vysvětlíme v níže uvedeném příkladu.

Tab. 4. Procentuální hodnota bodového rozpětí evaluačního systému

Body	Procentuální hodnota
0	0 %
1	20 %
2	40 %
3	60 %
4	80 %
5	100 %

Každému kritériu bude navíc přiřazena procentuální váha, která se následně promítne i v celkovém hodnocení. Procentuální váha má za úkol reprezentovat důležitost daného kritéria a její konečný součet musí být vždy roven 100 %. Váha by měla taktéž zdůrazňovat rozpětí daného kritéria (např. Možnosti živého pohledu zahrnují mnohem více funkcí, než ovládání PTZ). Stejně jako výsledné hodnocení VMS, je i procentuální váha odrazem subjektivního pohledu na danou problematiku.

Jako příklad si uvedeme fiktivní ohodnocení blíže nespecifikovaného VMS v kategorii Monitoring a záznam. K dispozici tedy máme 4 různé kritéria, které nyní ohodnotíme příslušnými body. Po testování daného VMS jsme dospěli k závěru, že v možnostech živého pohledu software naprosto exceluje, a proto zmíněné kritérium hodnotíme pěti body. Naopak v možnostech prohlížení záznamu software nenabídl žádný nadstandard, výsledné hodnocení proto odpovídá lehkému nadprůměru tří bodů. Podobným způsobem přiřadíme body i ostatním kritériím.

V následující části evaluační tabulky je prezentován tzv. dílčí výsledek. Jedná se o hodnotu, která vychází z bodového ohodnocení, na které je aplikována procentuální váha. Po této aplikaci dostaneme číselnou hodnotu, kterou následně převedeme na procenta. Posledním krokem je součet dílčích výsledků, jejichž suma je pro nás konečné hodnocení dané kategorie.

Příklad výpočtu

35 % z 5 je 1,75.

Hodnota 1,75 odpovídá 35 % v bodovém rozsahu. Dílčí výsledek kritéria „Možnosti živého pohledu“ je tedy 35 %.

35 % z 3 je 1,05.

Hodnota 1,05 odpovídá 21 % v bodovém rozsahu. Dílčí výsledek kritéria „Možnosti prohlížení záznamu“ je tedy 21 %.

Podobným způsobem pokračujeme i u ostatních kritérií a na závěr sečteme jednotlivé dílčí výsledky. V tomto případě dostáváme po sečtení dílčích výsledků hodnotu 76 %, která reprezentuje celkové hodnocení v kategorii „Monitoring a záznam“. Průběh hodnocení zmíněné kategorie reprezentuje následující tabulka.

Tab. 5. Příklad ohodnocení VMS v dané kategorii

Kategorie	Kritéria	% váha	Bodové ohodnocení	Dílčí výsledek	Celkové hodnocení
Monitoring a záznam	Možnosti živého pohledu	35	5	1,75 ~ 35 %	**76 %**
	Možnosti prohlížení záznamu	35	3	1,05 ~ 21 %	
	Ovládání PTZ funkcí	20	4	0,80 ~ 16 %	
	Možnosti nastavení obrazových a zvukových vlastností	10	2	0,20 ~ 4 %	

4 KOMPARACE VYBRANÝCH VMS NA ZÁKLADĚ APLIKACE NAVRŽENÉHO EVALUAČNÍHO SYSTÉMU

V předchozí kapitole jsme zkonstruovali komplexní evaluační systém, jenž bude nyní aplikován na konkrétní VMS. Pro účely testování jsme zvolili celkem 4 různé softwary, které si v nadcházejících kapitolách krátce představíme a následně podrobíme testování ve všech kategoriích hodnotícího systému. Pro zachování alespoň částečné objektivity výsledné komparace VMS zvolíme takové softwary (resp. edice softwaru), které jsou si svou nabídkou funkčních vlastností podobné. Pochopitelně by ztrácelo smysl porovnávat základní edici jednoho VMS s nejlepší edicí druhého VMS. Dále je třeba si uvědomit, že charakteristika VMS v jednotlivých kategoriích bude spíše takovým průřezem dané oblasti, kde se pokusíme vyzdvihnout některé vybrané funkce a vlastnosti, ve kterých software vyniká nebo naopak ztrácí v porovnání s konkurencí. Podrobný výčet a charakteristika veškerých funkcí v dílčích kategoriích by vyžadoval mnohonásobně větší rozsah práce. Pro představu, manuály ke konkrétním VMS jsou v rozsahu 300 a více stran.

Ještě než se pustíme do testování zvolených softwarů, přiblížíme si metodiku testování a architekturu laboratoře. Hlavním uzlem komunikace je server umístěný v budově Vědecko-technického parku při UTB. Na serveru jsou skrze aplikaci VMware Workstation nainstalovány 4 tzv. „virtual machines“, na kterých běží operační systém Windows Server 2012 R2. Každý z nich je speciálně vyhrazen pro instalaci serverových aplikací konkrétních VMS. V laboratoři 54/209 jsou poté umístěny PC, na kterých budou umístěny klientské aplikace VMS, jež budou posléze připojeny právě ke zmíněným serverům. V průběhu testování byla laboratoř stále ve fázi budování, a proto bylo jako platformy pro klientské aplikace využito především autorova notebooku a stolního PC. Díky síti VPN bylo možné přistupovat na síť UTB i z domova a na dálku tak provádět administraci a konfiguraci VMS.

V poslední řadě je vhodné zmínit použité kamerové vybavení a také parametry serveru. Všechny kamery jsou značky Axis a konkrétně se jedná o modely: M 1125, P 1364, P 1435-LE, P 3225LVE, Q 1635, Q 6045-E a Q 3505-V. Uvedené modely nebudou dále více rozebrány, neboť z hlediska testování VMS se nejeví jako klíčové. Podrobné parametry kamer lze dohledat na webových stránkách společnosti Axis.

Server umístěný na Vědecko-technickém parku je model Dell PowerEdge 2900. Podrobnější parametry jsou uvedeny v následující tabulce.

Tab. 6. HW specifikace serveru Dell PowerEdge 2900

Komponent	Parametry
Procesor	Intel Xeon E5430 @ 2.66 GHz
Paměť RAM	8 GB
Diskové pole	RAID 10 a RAID 5 s kapacitou 512 GB

4.1 Axis Camera Station

Axis Camera Station (dále jen ACS) je profesionální VMS řešení od společnosti Axis Communications. Axis je největší světový dodavatel na trhu IP kamer a působí jako hybná síla v tomto odvětví tím, že průběžně uvádí inovativní síťové produkty založené na otevřené platformě. S pomocí globální sítě partnerů tak přináší svým zákazníkům vysokou hodnotu. Axis si zakládá na dlouhodobých vztazích se svými partnery, kterým poskytuje na stávajících i na nových trzích jak průlomové síťové produkty, tak i své znalosti. K dnešnímu datu má Axis více než 2.000 vlastních zaměstnanců ve více než 40 zemích na celém světě a spolupracuje se sítí více než 75.000 partnerů ve 179 zemích. [20]

V současné době společnost Axis nabízí poměrně pestrou škálu softwarových aplikací a utilit. Mezi ty nejvýznamnější z pohledu této práce pochopitelně patří dvě samostatné VMS, a to konkrétně AXIS Camera Companion a AXIS Camera Station. Pokud zákazník preferuje dohled ve formě cloudové služby, je vhodnější využít nabídky hostovaného videa. V případě, že zmíněná řešení nejsou vyhovující, se dále nabízí široké portfolio partnerských aplikací, jež jsou přizpůsobené specifickým požadavkům a nabízí variabilnější možnosti integrace.

Pro potřeby této práce byl zvolen již zmíněný Axis Camera Station, který bude součástí učebny 54/209 a bude využíván studenty při zpracování laboratorních úloh. Jedná se o pokročilý VMS, který by měl být schopen pokrýt požadavky zákazníků při aplikacích ve středně velkých podnicích. Testovaný software je od března roku 2016 dostupný v nejnovější verzi 5, která přinesla několik zásadních změn a vylepšení. Nadcházející kapitoly se proto budou věnovat aplikaci navrženého evaluačního systému na aktuální verzi Axis Camera Station 5. Výstupem testování bude přehledná tabulka, která bude reprezentovat výsledky ACS v dílčích kategoriích.

4.1.1 Evaluace ACS

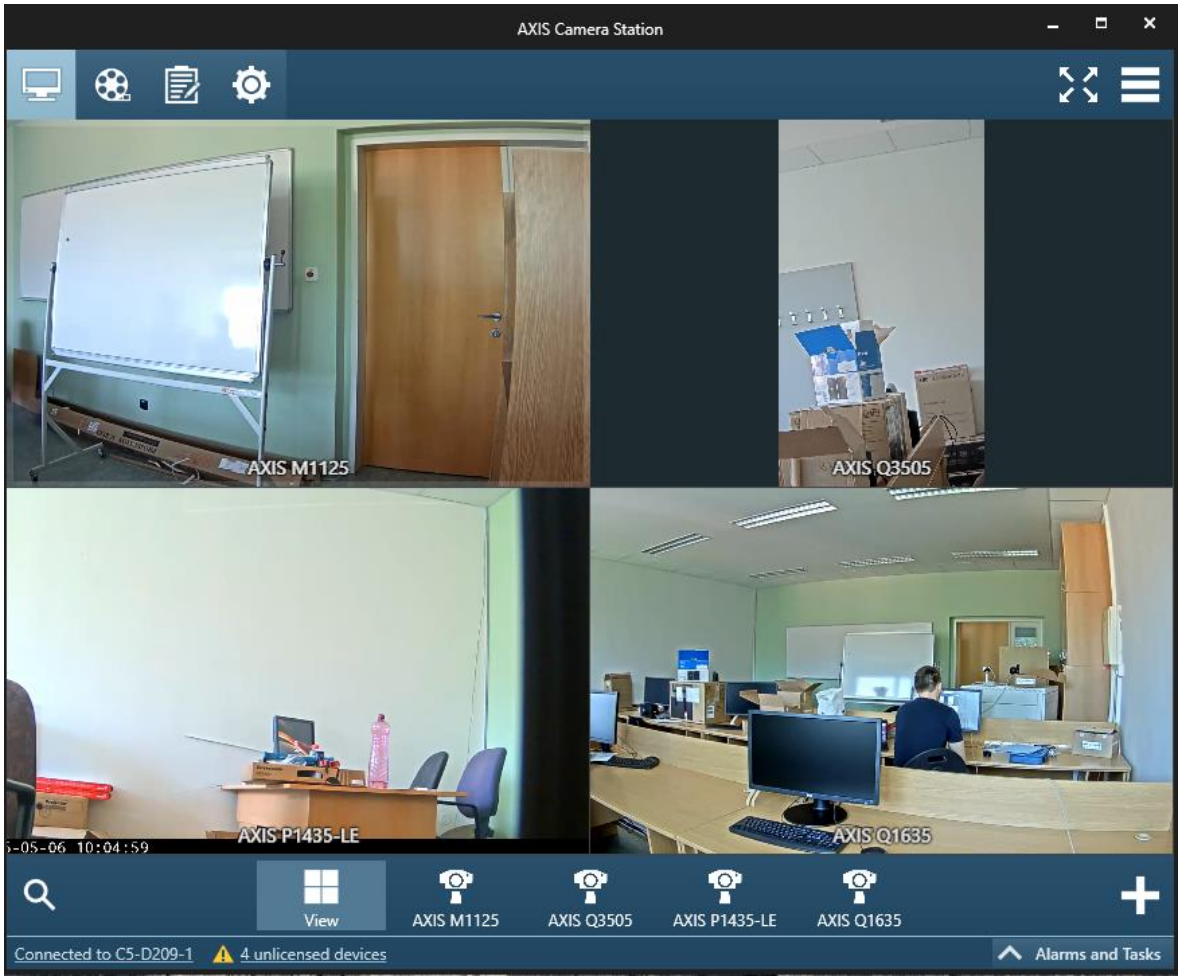
Monitoring a záznam

V kategorii monitoringu a záznamu ACS nabízí poměrně velké množství funkcí. Díky velice jednoduchému rozhraní se i naprostý nováček neztratí a dokáže systém nastavit i s minimálními zkušenostmi. Co se týče sledování live streamu, ACS umožňuje velice snadné přizpůsobení dohledové plochy pomocí různých funkcí, jako je libovolné přidávání kamer, vytváření sekvencí, rozdělení obrazu, či vytvoření map. Obzvlášť mapy jsou velice užitečnou funkcí, pomocí které do ACS nahrajeme např. půdorys nějakého objektu, a přímo do něj umístíme odkazy na kamery podle jejich umístění v objektu. Poté stačit kliknout na příslušnou ikonu kamery a ihned se nám zobrazí její pohled.

Nahrávání v prostředí ACS je rozděleno do 3 kategorií – manuální, motion (detekce pohybu) a kontinuální. Každou kategorii symbolizuje příslušná barva, která je poté zobrazena na časové ose při prohlížení záznamu. Díky tomu tak lze odlišit, která část záznamu byla nahrávána tím daným způsobem. S touto oblastí souvisí hlavně nastavování výsledné kvality záznamu, kdy se většinou kontinuálnímu nahrávání přiřazuje nižší kvalita, a naopak při detekci pohybu se aktivuje kvalita nejvyšší. Samotné vyhledávání v záznamech je velice snadné, ACS dále umožnuje na časové ose vymezit určitý úsek záznamu pomocí záložek, a tento úsek následně exportovat v libovolném formátu. K efektivnímu vyhledávání přispívá především funkce zvaná Smart Search, tedy chytré vyhledávání fungující na bázi třídění metadat. Pomocí Smart Search dokážeme najít konkrétní části záznamu, kdy došlo k nějaké předem definované události.

Ovládání PTZ funkcí kamer je pomocí ACS rovněž velice zjednodušené. Uživatel kameru polohuje pomocí šipek na klávesnici a myši, případně prostřednictvím virtuálního joysticku. Pro pohodlné a přesné ovládání je rovněž možné dokoupit Axis ovládací pult pro PTZ.

V možnostech nastavení obrazových a zvukových funkcí toho ACS moc nenabízí. Kromě přizpůsobení jasu, kontrastu, ostrosti, vyvážení bílé a otočení obrazu nenabízí žádné dodatečné funkce. Pokud tedy chceme kameru dále konfigurovat, je nezbytné to provádět prostřednictvím webového rozhraní. Za poslední zmínku stojí video profily, zmíněné v kapitole 2.2. ACS podporuje 3 video profily – Low, Medium a High, které reprezentují výslednou kvalitu videa. Profilům se dají upravovat parametry rozlišení obrazu, snímkové frekvence, úrovně komprese a kompresního formátu. Co se týče zvukových možností, ACS podporuje aktivaci mikrofonu jak při živém pohledu, tak při nahrávání.



Obr. 11. Dohledová plocha v ACS

Komunikace a podpora zařízení

ACS byl až donedávna omezen pouze na podporu kamer Axis. Od testované verze 5 již nabízí i podporu ostatních výrobců kamer, které podporují standard ONVIF profil S. Testování veškerých VMS však probíhalo pouze s kamerami AXIS, a proto tuto schopnost nemůžeme ověřit. Komunikace probíhala bezchybně, software dokázal kamery rozpoznat ve velice krátkém čase a jednoduše přiřadit do systému. Za menší nevýhodu lze považovat pouze podporu formátů M-JPEG a H. 264.

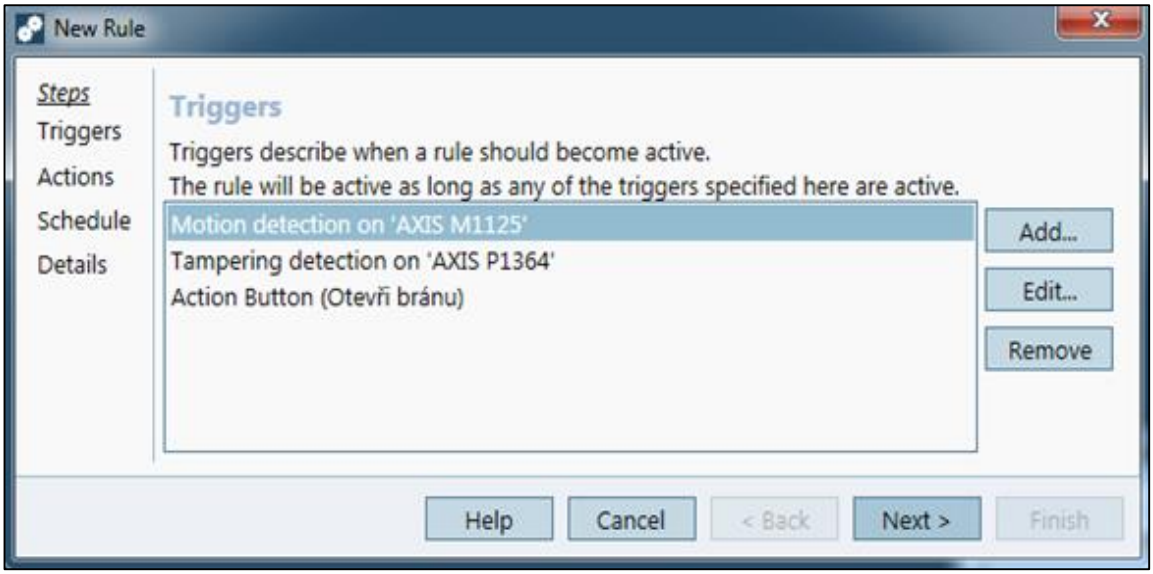
Jakožto většina pokročilých VMS, i ACS je koncipován na architektuře klient – server. Za výhodu v této kategorii se dá považovat možnost provozovat server i klienta na jednom uživatelském PC. ACS podporuje operační systémy pouze od Microsoftu, konkrétně Windows 10 Pro, Windows 8.1 Pro, Windows 7 Pro SP1, Server 2012, Server 2012 R2, Server 2008 a Server 2008 R2. Pokud uživatel není zběhlý ve zřizování a konfiguraci vlastní pracovní stanice, má možnost zakoupit předpřipravené stanice Axis, které jsou sestaveny přímo na

míru pro určitý počet kamer. Na těchto stanicích už je ACS předinstalován dodavatelem. Mimo PC nebo serveru je také ACS možné nainstalovat jako aplikaci na chytrý telefon, který podporuje OS Android ve verzi 4.2.2 nebo iOS 8.

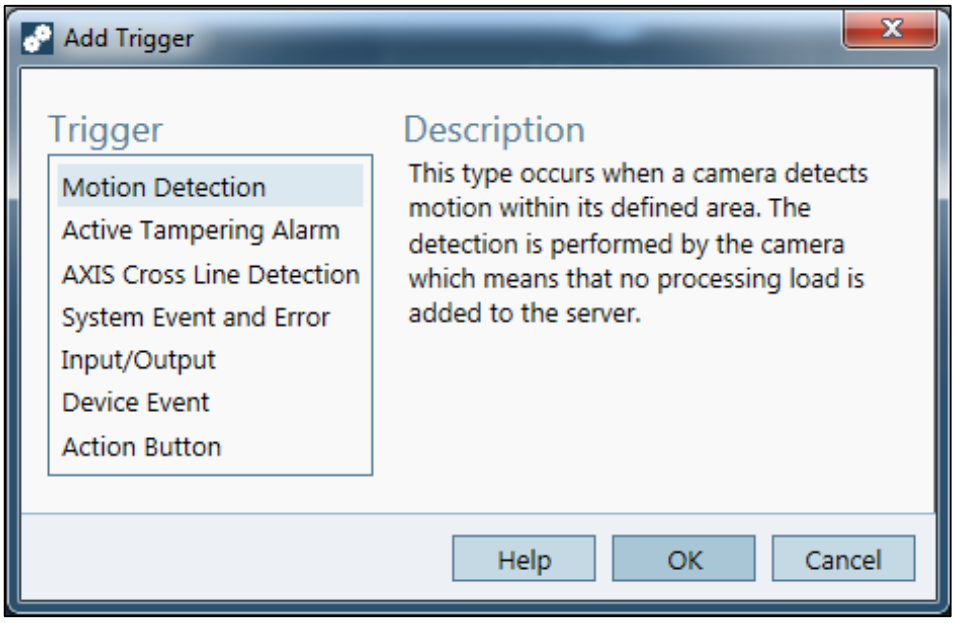
ACS je koncipován tak, aby jej bylo možné integrovat i s jinými systémy alespoň na základní úrovni funkcionality. K tomuto úkonu je zapotřebí expanzní model Axis, který umožnuje připojit různé zařízení na vlastní logické vstupy a výstupy, a poté se spárovat prostřednictvím ACS. Modul v současné době není součástí laboratoře 54/209 a nebyl testován.

Management a konfigurace událostí

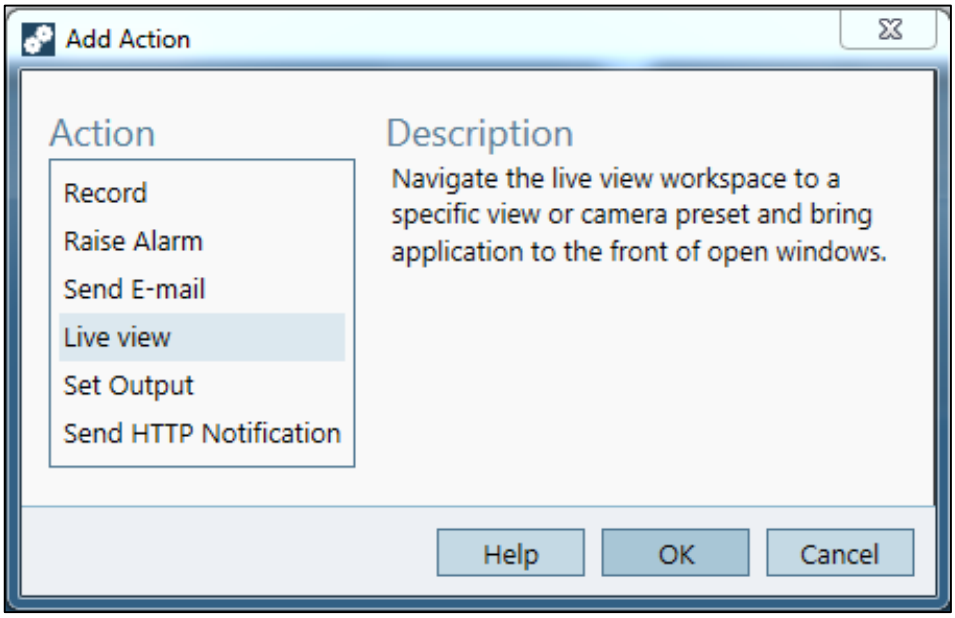
Konfigurace událostí probíhá v ACS na obdobném principu akce a spouštěče, jak je popsáno v kapitole 2.3. Proces nastavování je opět velice jednoduchý a přehledný, výsledné události je možné nastavit v průběhu několika minut. Pro účely testování jsme vyzkoušeli veškeré akce a spouštěče, vyjma logických I/O. Funkcionalita byla bezproblémová, software reagoval na podněty rychle a efektivně. Rozhraní událostí navíc obsahuje dodatečný popis jednotlivých akcí a spouštěč, aby uživatel věděl, co přesně nastavuje. Na následujících obrázcích lze spatřit přehled vytvořených událostí a samotný proces vytváření. Kladně lze hodnotit možnosti akčního tlačítka, jehož funkcionalita je velice univerzální.



Obr. 12. Přehled vytvořených událostí v ACS



Obr. 13. Vytvoření spouštěče v ACS



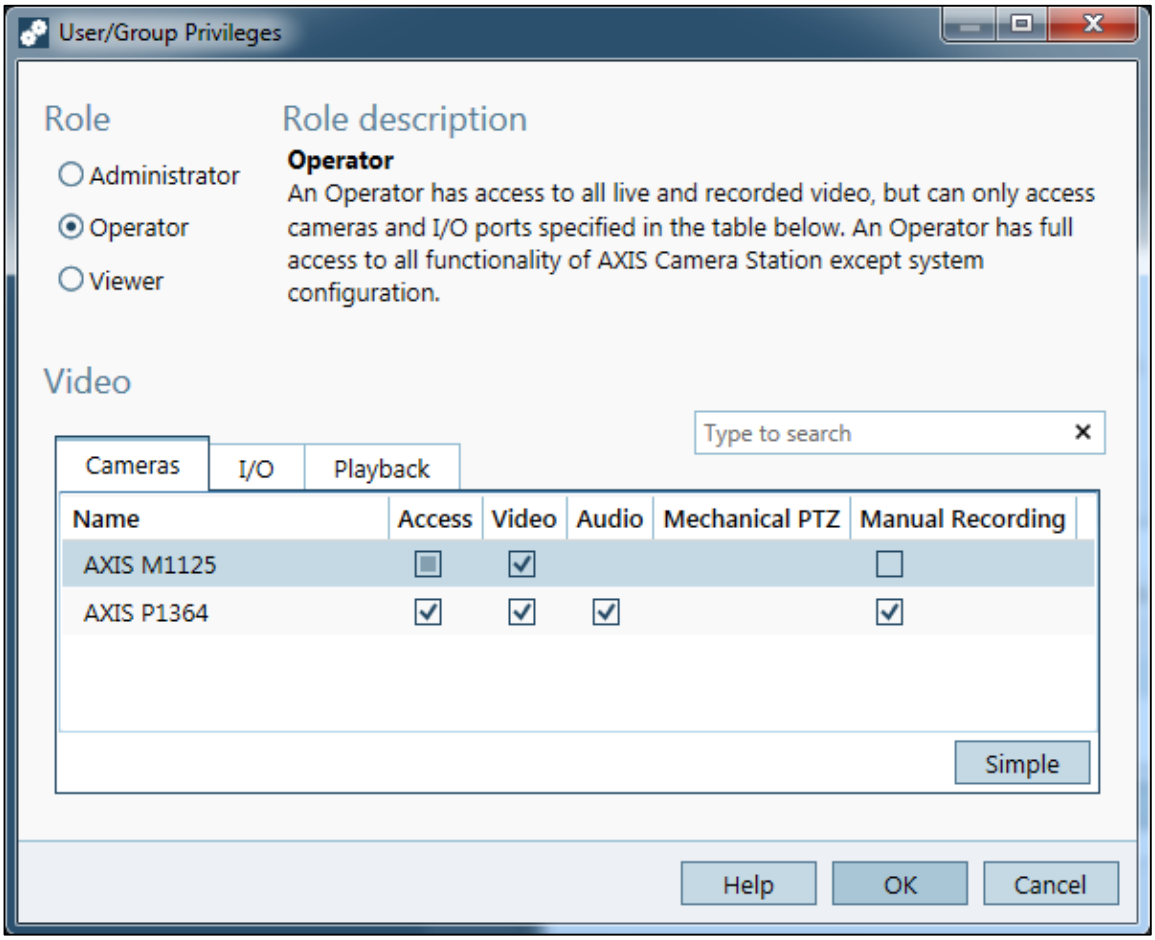
Obr. 14. Vytvoření následné akce v ACS

Inteligentní funkce v ACS jsou bohužel velmi omezené. Vyjma detekce pohybu, detekce sabotáže a překročení linie nenabízí software žádné další možnosti. Za výhodu ovšem můžeme považovat fakt, že zmíněné funkce jsou dostupné zdarma. Základní verzi detekci pohybu a sabotáže má většina Axis kamer zabudovanou již z výroby, uživatel má však možnost zdarma stáhnout vylepšenou verzi a nahrát ji do prostředí ACS. Při konfiguraci detekce překročení linie je nutné stáhnout softwarový modul z webových stránek Axis. Všechny 3 funkce byly v průběhu testování odzkoušeny pomocí několika kamer. Detekce pohybu i překročení linie byly velmi citlivé, software reagoval na sebemenší zachycený pohyb.

Detekce sabotáže fungovala bez problémů, software dokázal rozpoznat změnu pohledu kamery a v krátkém čase reagovat. Velkou nevýhodou ACS je ovšem nemožnost tyto funkce jakkoliv více konfigurovat. Software umožnuje pouze nastavit např. výseč pro detekci pohybu, ale nikde nelze nastavit citlivost snímání a další atributy.

Administrace práv

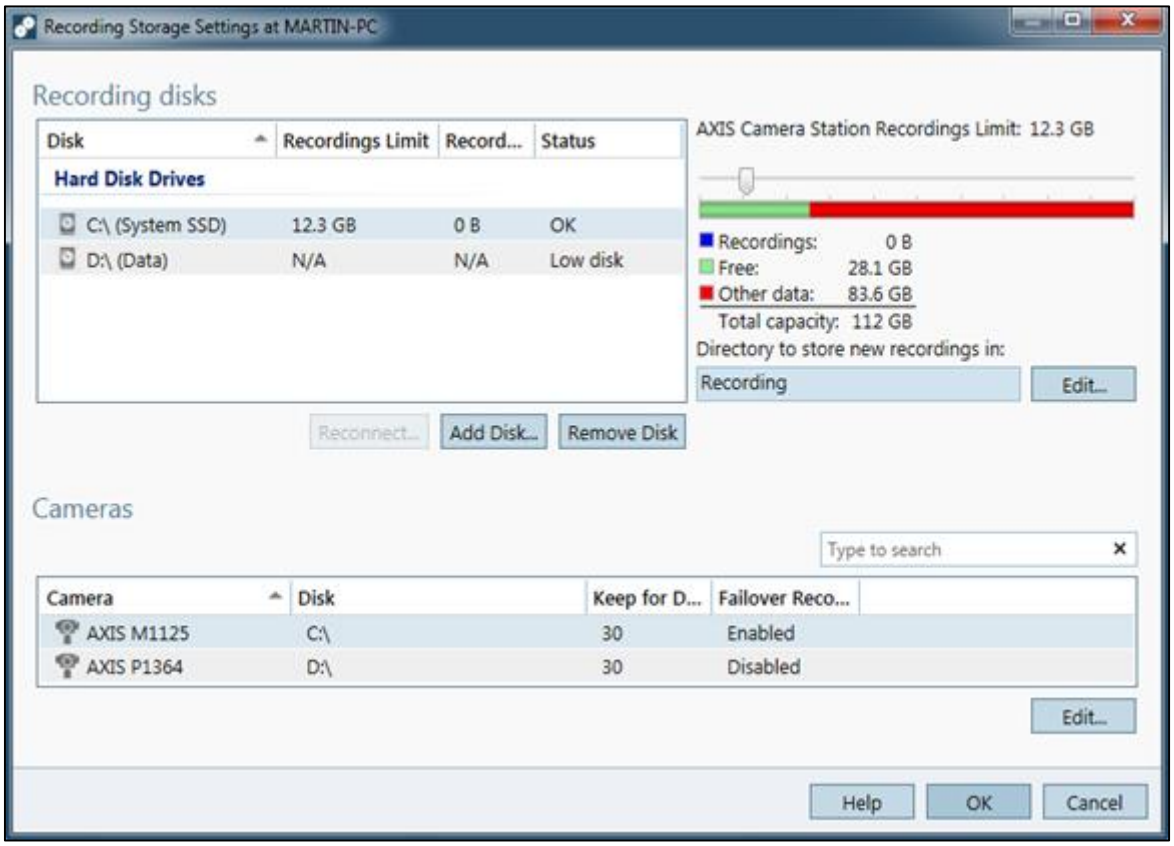
V této kategorii ACS umožňuje přidat libovolný počet uživatelů s rozdílným oprávněním. Uživatel s oprávněním administrátor má možnost do systému zavést nového uživatele nebo rovnou celou skupinu uživatelů. Těm pak může přiřadit oprávnění dalšího administrátora, operátora nebo dozorce, kterým lze nastavit přístup k jednotlivým funkcím. ACS je systematicky svázán s účty Windows, pokud tedy chceme přidat nového uživatele, musíme nejprve vytvořit nový účet ve Windows, a na ten poté odkázat pomocí ACS. Tato skutečnost však není nikde v rozhraní administrace práv objasněna. Díky tomu je tak celý proces poměrně zbytečně komplikovaný a nezkušený uživatel může mít v této oblasti problémy.



Obr. 15. Úprava oprávnění uživatele v ACS

Správa uložiště

Management uložišť je v prostředí ACS snadný a přehledný. Uživatel může velice rychle přiřadit jednotlivé disky a na nich alokovat část, která bude sloužit pro ukládání záznamu. ACS podporuje jak lokální, tak síťové disky NAS. Každé kameře v systému se vymezí konkrétní uložiště a nastaví se doba, po kterou se záznam uchová. Pokud je nějaký disk plný nebo nedostupný, ACS uživatele informuje prostřednictvím rozhraní managementu uložiště i pomocí vyskakovacích oken. Dodatečnou funkcí je aktivace fail-over nahrávání, které je však dostupné pouze při použití kompresního formátu H. 264. Jakožto i u většiny ostatních kategorií, je i ACS v oblasti správy uložiště v porovnání s konkurencí velmi zjednodušený. Za nevýhodu se dá považovat např. nemožnost nastavení cílové složky, kam se ukládají data celého záznamu. Složka se dá zvolit pouze přímo při exportu konkrétní části záznamu. Dále ACS nenabízí vytvoření archívů, jak je tomu u konkurenčních VMS.



Obr. 16. Správa uložiště v ACS

Uživatelské rozhraní

Instalace ACS je snadná a rychlá, software byl nainstalován v průběhu necelé minuty. Jediným místem, do kterého uživatel v průběhu instalace zasahuje, je volba instalace serveru i klienta či pouze klienta. Po instalaci následovala fáze přiřazení kamer, kdy software kameru rozpoznal v řádu několika sekund. Uživatelské rozhraní tak můžeme hodnotit jako velice přehledné, snadné a intuitivní. Ze všech testovaných VMS je rozhodně nejjednodušší na ovládání a poradí si s ním i méně zkušený uživatel. Na druhou stranu díky strohému konceptu je software v řadě kategoriích ochuzen o větší možnosti konfigurace. Další nevýhodou je také lokalizace ACS, která je v současné verzi 5 dostupná pouze v angličtině. Axis však přislíbil v nadcházející verzi 5. 01 podporu pro téměř 20 světových jazyků, včetně češtiny. Proces seznámení se s ACS je také zjednodušen, neboť Axis mimo klasického manuálu a vestavěné nápovědy v softwaru nabízí i několik video tutoriálu pro naprosté začátečníky. Video tutoriály uživatele provedou všemi kroky práce se systémem, od instalace až po závěrečné uvedení do provozu. Tutoriály jsou dostupné na stránkách Axis i na serveru Youtube, zatím ale pouze v angličtině.

Hardwarová náročnost

Hardwarové požadavky ACS závisí na celkové šířce pásma ze všech zdrojů. Datový tok z každého zdroje se liší dle složitosti scény a zvoleného nastavení (rozlišení, snímková frekvence, komprese, …). Doporučená HW konfigurace je vztažena na celkovou šířku pásma pro jeden server. Následující tabulky reprezentují HW nároky na ACS pro jednotlivé typy instalace. Společnost Axis uvádí u klíčových komponent i příklad konkrétního modelu. Pro určení přibližné HW náročnosti pro konkrétní instalaci slouží aplikace Site Designer.

Tab. 7. HW nároky ACS - instalace do 26 kamer - server i klient na jedné stanici [21]

Komponent	Požadavek
Procesor	Intel Core i5-4590 3.3 GHz
Paměť RAM	8 GB, DDR3-1600 MHz
Grafická karta	NVIDIA GTX 750 1 GB
Pevný disk	SATA 6 Gb/s 7200 RMP

Tab. 8. HW nároky ACS - instalace nad 26 kamer - ACS server [21]

Komponent	Požadavek
Procesor	Intel Core i7-4770 3.4 GHz
Paměť RAM	8 GB, DDR3-1600 MHz
Grafická karta	NVIDIA GTX 750 1 GB

Tab. 9. HW nároky ACS - instalace nad 26 kamer - ACS klient [21]

Komponent	Požadavek
Procesor	Inter Core i7-4770 3.4 GHz
Paměť RAM	8 GB, DDR3-1600 MHz
Pevný disk	SATA 6 Gb/s 7200 RPM

Finanční náročnost

ACS je možné vyzkoušet pro neomezený počet kamer po dobu 30 dní. Po této lhůtě je zapotřebí zakoupit kamerové licence dle aktuální licenční politiky, která prošla velkou obměnou právě od nové verze ACS 5. Pro jednotlivé připojené zařízení je nyní nutná pouze jedna licence a již nezáleží na počtu obrazových senzorů kamery nebo počtu kanálů enkodéru, jak tomu bylo v případě ACS 4. Tuto novinku ocení především uživatelé multisenzorových kamer nebo vícekanálových video enkodérů.

Tab. 10. Ceník jednotlivých typů licencí ACS

Typ licence	Cena (v Eurech)
Core Device	79
Universal Device	149

Core Device licence se zakupují do VSS čítajících maximálně 32 kamer. Použité kamery však musí být pouze značky Axis. Universal Device licence se zakupují pro VSS čítající 33 a více kamer. Pokud by chtěl uživatel do systému zahrnout i kameru od jiného výrobce, musí pro ni pořídit právě Universal Device licenci.

4.1.2 Evaluační tabulka a závěrečná rekapitulace VMS Axis Camera Station

Tab. 11. Evaluační tabulka ACS, část 1.

Kategorie	Kritéria	% váha	Bodové ohodnocení	Dílčí výsledek	Celkové hodnocení
Monitoring a záznam	Možnosti živého pohledu	35	4	1,40 ~ 28 %	**65 %**
	Možnosti prohlížení záznamu	35	3	1,05 ~ 21 %	
	Ovládání PTZ funkcí	20	3	0,60 ~ 12 %	
	Možnosti nastavení obrazových a zvukových vlastností	10	2	0,20 ~ 4 %	
Komunikace a podpora zařízení	Podpora zařízení	50	2	1,00 ~ 20 %	**45 %**
	Architektura a platformy	25	3	0,75 ~ 15 %	
	Možnosti integrace s jinými systémy	25	2	0,50 ~ 10 %	
Management a konfigurace událostí	Možnosti konfigurace událostí	70	3	2,10 ~ 42 %	**48 %**
	Inteligentní funkce	30	1	0,30 ~ 6 %	
Administrace uživatelských práv	Možnosti administrace práv	100	2	2,00 ~ 40 %	**40 %**
Správa uložiště	Možnosti správy uložiště	100	3	3,00 ~ 60 %	**60 %**

Tab. 12. Evaluační tabulka ACS, část 2.

Kategorie	Kritéria	% váha	Bodové ohodnocení	Dílčí výsledek	Celkové hodnocení
Uživatelské rozhraní	Instalace	10	5	0,5 ~ 10 %	**82 %**
	Přehlednost a ovládání	40	5	2,00 ~ 40 %	
	Lokalizace	20	2	0,40 ~ 8 %	
	Technická podpora	30	4	1,20 ~ 24 %	
Hardwarová náročnost	Provozní požadavky	100	1	1,00 ~ 20 %	**20 %**
Finanční náročnost	Licenční model a výsledná cena	100	3	3 ~ 60 %	**60 %**

Axis Camera Station je profesionální VMS, navržené pro aplikace ve středně velkých podnicích, které se nachází v jedné lokalitě. Jmenovitě jsou to např. školy, maloobchody, hotely, menší výrobní podniky atd. Mezi přednosti softwaru patří především uživatelské rozhraní, které je velmi přehledné a intuitivní. Také konfigurace veškerých funkcí je v prostředí ACS snadná a bez větších obtíží ji zvládne i nezkušený uživatel. ACS má i relativně dobře vyřešenou oblast monitoringu a záznamu, kde neschází žádné klíčové funkce.

V ostatních kategoriích už software poněkud strádá. Velkou nevýhodou je především fakt, že ACS kromě Axis kamer nepodporuje jiné výrobce. Tato skutečnost sice byla zmírněna novou verzí ACS 5, kdy byla implementována podpora zařízení alespoň prostřednictvím ONVIF, nicméně v porovnání s konkurencí je to stále nedostatek. Navíc vzhledem k jednoduchému grafickému zpracování software vyžaduje poměrně výkonný hardware. Ve zbývajících kategoriích ACS dosahuje průměrných výsledků, v žádné ovšem nemá nějaké zásadní nedostatky. Finanční náročnost je v případě použití pouze kamer Axis přijatelná, nicméně pro kamery od jiných výrobců je vhodnější využít konkurenční VMS, které toho nabízí více za srovnatelnou cenu.

4.2 Axxon Next

Axxon Next je VMS řešení od společnosti AxxonSoft. Firma se řadí mezi přední vývojáře softwaru, který kombinuje ochranu informačního managementu na bázi IP, inteligentní analýzu obrazu a systém pro správu videa do celopodnikové platformy. AxxonSoft v současné době nabízí 2 produkty, a sice zmíněný VMS Axxon Next a dále Intellect Enterprise, charakterizovaný jako pokročilý software pro komplexní bezpečnost informačního managementu. AxxonSoft byl založen roku 2003 a ve svém portfoliu má více než 100 000 úspěšných projektů s implementací vlastního softwaru. Společnost má více než 2 500 partnerů a je členem fóra ONVIF. [22]

V nadcházejících částech této kapitole bude Axxon Next rovněž podroben testování ve všech vybraných kategoriích evaluačního systému. VMS je nyní dostupný v poslední verzi 4, zároveň však i v několika edicích, konkrétně Axxon Next Free, Start, Professional a Universe. Jednotlivé edice se od sebe liší v množství funkcí, počtu podporovaných kamer nebo počtu serverů. S tím pochopitelně koresponduje i výsledná cena softwaru. Mimo tyto klasické edice Axxon nabízí i demo verzi, která však není omezena funkcemi (až na výjimky, jako je detekce překročení linie), nýbrž časově. Demo verzi je možné testovat po neomezeně dlouho dobu, avšak pouze v časovém rozmezí od 8 ráno do 6 odpoledne. Mimo tento interval software není funkční a uživatel tak musí počkat nebo vyzkoušet verzi Free, která je sice zdarma, ale značně omezená funkcemi. Pro účely testování byla proto zvolena dotyčná demo verze, abychom mohli porovnat co nejvíce funkčních vlastností s ostatními VMS. Do budoucna se počítá i s umístěním již placené verze Axxon Next v laboratoři 54/209.

4.2.1 Evaluace Axxon Next

Monitoring a záznam

Axxon Next nabízí v kategorii monitoringu a záznamu značné množství funkcí, nicméně řada z nich je schována za lehce nevzhledným designem a rozložením jednotlivých prvků. Nezkušenému uživateli tak chvíli trvá, než objeví všechny možnosti softwaru a naučí se s nimi pracovat. Za velké plus se dají v této kategorii považovat možnosti vytváření dohledových ploch. Rozdělit plochu na několik části a v nich zobrazit pohledy z různých kamer je již v dnešní době standardem. Axxon k tomuto prvku navíc přidává možnost zobrazení vestavěného ukazatele stavu systému, přizpůsobitelného počítadla událostí nebo dialogového panelu. Také systém objektových map doznal v nové verzi Axxon Next řady vylepšení.

V současné době je systém postaven na tzv. interaktivních 3D mapách, tzn. uživatel má možnost si přizpůsobit pracovní plochu a nahlížet na půdorys objektu s umístěnými kamerami i v z jiné perspektivy, jak je uvedeno na demonstračním obrázku. V době testování byly mapy rovněž vyzkoušeny, ale vzhledem k omezeným možnostem laboratoře se pro demonstraci více hodí výňatek z video tutoriálu Axxon Next.

Obr. 17. Interaktivní 3D mapa Axxon Next [23]

Axxon Next dále nabízí plynulý přechod ze sledovací plochy rovnou do vybraných archívů, jejichž charakteristika bude uvedena v následujících částech práce. Samotné vyhledávání v záznamech opět poněkud trpí na nepřehledný design. Software sice umožnuje odlišit jednotlivé etapy záznamu podle barevného rozlišení a symbolických ikon, které reprezentují druh záznamu nebo jednotlivé události, nicméně svisle položená osa záznamu spíše komplikuje vyhledávání. Na druhou stranu ovládání PTZ funkcí kamer je v prostředí softwaru jednoduché a intuitivní. Uživatel může stiskem jednoho tlačítka vedle dohledové plochy zobrazit softwarový ovládací panel. Ten kromě ovládání PTZ umožnuje velice rychle spustit tzv. Patrol režim, ve kterém se definované kamery natočí do přednastavených pozic.

Nastavení obrazových a zvukových vlastností kamer v Axxon Next je nutné provádět na několika „místech“. V záložce managementu zařízení můžeme upravovat pouze výsledný profil video streamu, respektive přepínat mezi vysokou a nízkou kvalitou. V profilech se dá upravit pouze kompresní formát a přenosový protokol, nelze např. upravovat rozlišení nebo snímkovou frekvenci. Další parametry, jako je jas, kontrast nebo ostrost je nutné nastavovat přímo v sekci živého pohledu kamery, kdy po najetí myší do prostoru zobrazené scény se nabídne úprava vizualizace. Bohužel však není možné nastavit míru těchto parametru, např. kontrast nebo ostrost se dají přepínat pouze do polohy zapnuto nebo vypnuto, kdy se hloubka vlastnosti nastaví na maximální nebo minimální možnou hodnotu. Veškeré změny obrazových a zvukových vlastností je proto při použití Axxon Next provádět ve webovém rozhraní kamery.

Komunikace a záznam

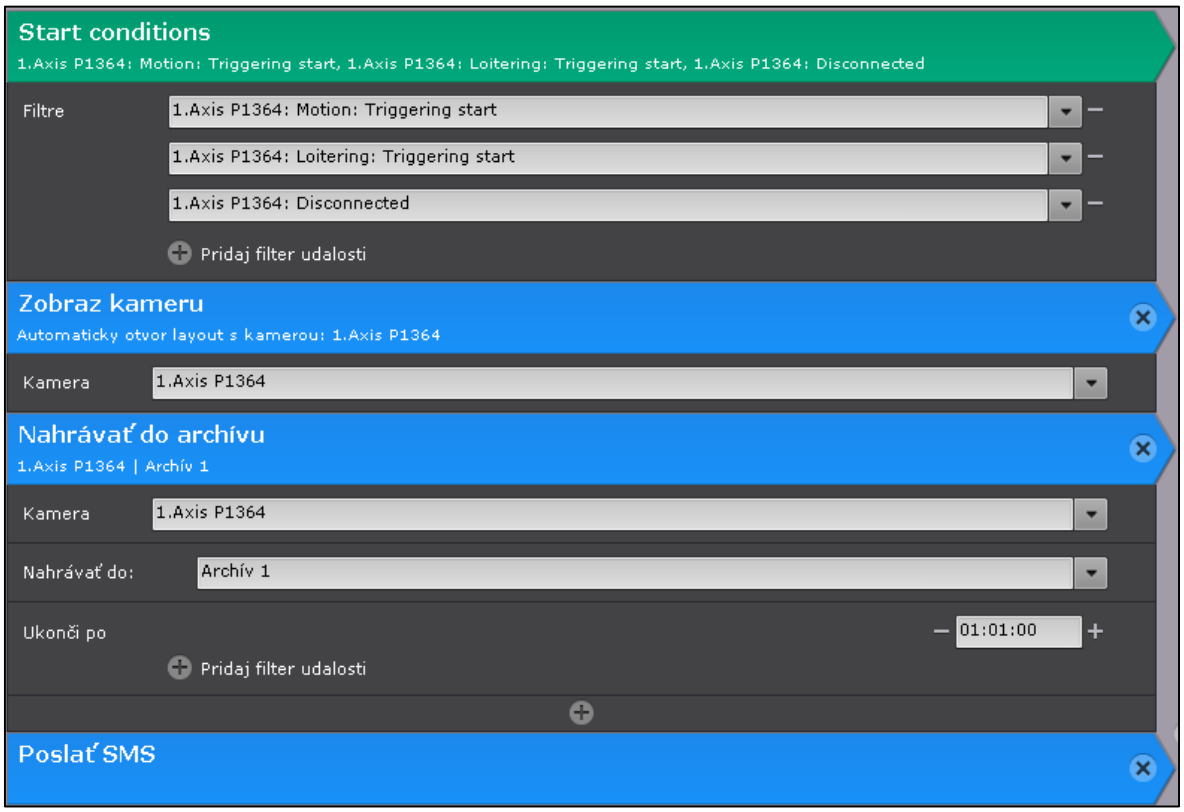
Axxon Next slibuje podporu více jak 6000 zařízení, z toho cca 1500 modelů pracujících na proprietárních protokolech a 4500 zařízení kompatibilní s ONVIF profilem S. Při testování softwaru s Axis kamerami problém nebyl, Axxon dokázal v poměrně krátkém čase kameru rozpoznat. Samotná registrace kamery do softwaru je již ovšem poměrně komplikovaná. V případě zapojení jedné kamery software rozpoznal 2 zařízení, jednu konkrétní Axis kameru s IP adresou z továrního nastavení a druhé nespecifikované zařízení, podporující standard ONVIF a s IP adresou přidělenou DHCP. Pokud chceme tuto kameru do systému přidat, musíme zvolit možnost, že se jedná o Axis kameru a ručně jí přepsat IP adresu na stejnou, jakou jí přiřadil protokol DHCP.

Axxon Next je centralizované VMS pracující na architektuře klient – server. Stejně jako ACS a Milestone, i Axxon umožnuje nainstalovat server i klienta na jednu pracovní stanici. Mezi podporované operační systémy patří Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows Server 2003, Server 2008, Home Server 2011 a Windows Server 2012. Podle všeho tak software není zatím možné provozovat na nových Windows 10. Software je navíc dostupný i pro mobilní zařízení s OS Android 4.1 a vyšší a iOS 7.0 a vyšší.

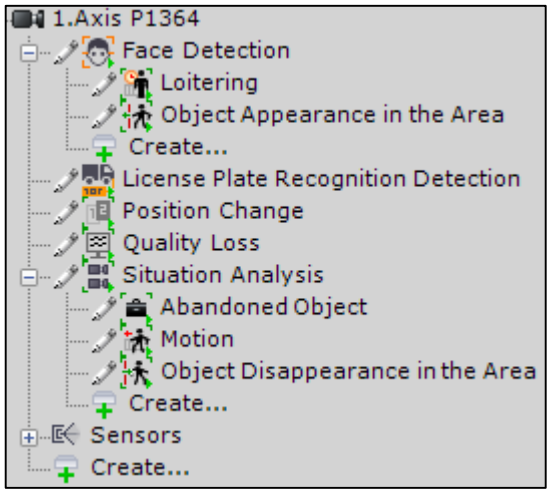
V případě integrace s jinými systémy je Axxon Next omezen pouze na možnosti logických I/O kamer. Pokud je s kamerou spárované nějaké zařízení, v prostředí Axxon Next můžeme nakonfigurovat, co a kdy se má dále stát viz Management a konfigurace událostí. Širší možnosti integrace zajišťuje společnost Axxon pomocí svého druhého produktu – Intellect Enterprise.

Management a konfigurace událostí

Oblast managementu a konfigurace událostí je v prostředí Axxon Next pojmenována jako programování. V podstatě jde ale o podobný systém, jako nabízí konkurence, tedy princip akce a spouštěče. V porovnání např. s ACS nabízí Axxon o něco více možností, na druhou stranu rozhraní není tak uživatelsky přívětivé a chvíli trvá, než se uživatel zorientuje. V průběhu testování byla vyzkoušena řada různých spouštěčů a akcí, software na většinu reagoval velmi pohotově. Axxon Next v porovnání s konkurencí velice příjemně překvapil v kategorii analytických funkcí. Veškeré funkce jsou přímo součástí softwaru a není nutné dodatečně instalovat další zásuvné moduly. Kromě klasiky jako je detekce pohybu nebo sabotáže software dokáže rozpoznávat například obličeje lidí nebo SPZ automobilů. Dále dokáže rozpoznat zanechaný předmět ve vyhrazeném prostoru, potulování podezřelých osob nebo odcizení hlídaného předmětu. Na všechny tyto funkce pak můžeme navázat prostřednictvím programování událostí, např. spojením rozpoznání obličeje a elektronického vrátníku, kdy software identifikuje obličej, předá informaci vrátníku a ten vpustí osobu do objektu. Konfigurace těchto funkcí však zabere poměrně hodně času a vyžaduje určitou znalost softwaru. Navíc některé funkce ještě potřebují trochu doladit, jmenovitě např. rozpoznávání SPZ, jež bohužel zatím funguje pouze pro značky několika konkrétních států.



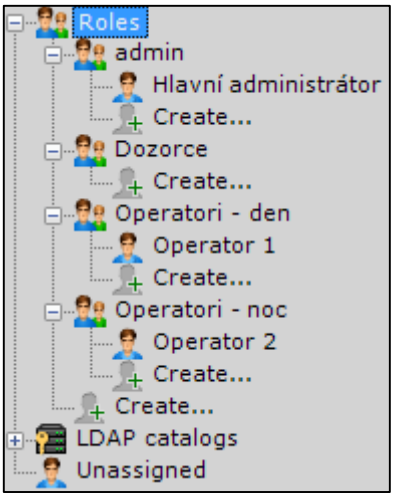
Obr. 18. Management událostí v Axxon Next



Obr. 19. Struktura konfigurace inteligentních funkcí kamer v Axxon Next

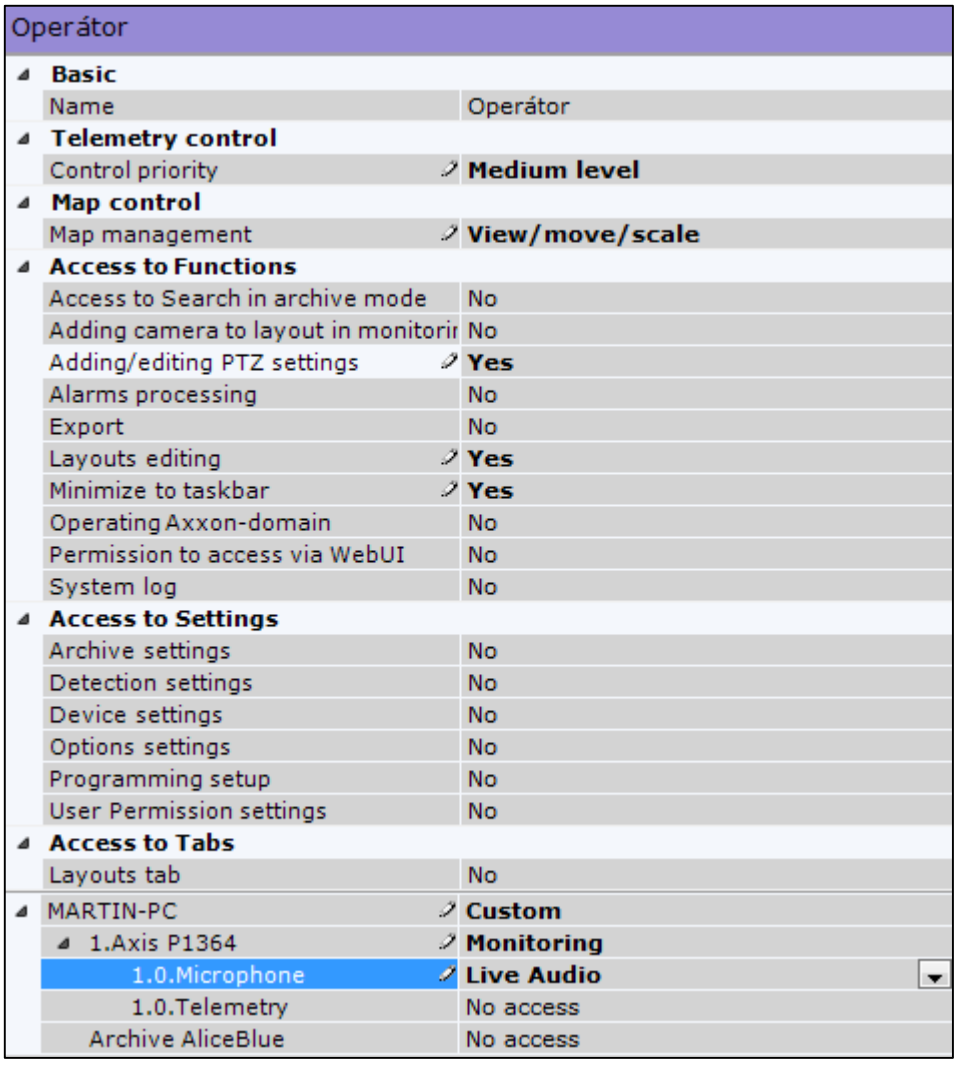
Administrace uživatelských práv

Axxon Next umožnuje vytvořit poměrně přehlednou strukturu uživatelů a uživatelských práv. Nejprve je nutné definovat role, tedy administrátor, operátor a podobně. Oproti ostatním VMS (např. ACS) však uživatel nemá tolik svázané ruce s managementem těchto rolí. Zmíněný ACS disponuje přímo třemi danými úrovněmi, kterým se posléze upravují práva. Role administrátora je v Axxon Next stejná, ovšem ostatní role už se dají libovolně vytvářet, upravovat a pojmenovávat podle osobní preference. Můžeme například vytvořit zvlášť několik druhu operátorů a dozorců podle režimu podniku, k nim přiřadit konkrétní uživatele a teprve poté jim upravovat práva. Software navíc podporuje autentizaci uživatelů pomocí protokolu LDAP, pomocí kterého je možné Axxon Next integrovat s již zaběhlou sítí evidence docházky v jiném systému. Na níže uvedených obrázcích lze spatřit příklad vytvořené uživatelské struktury a přidělování práv.



Obr. 20. Struktura uživatelů

v Axxon Next



Obr. 21. Přidělování práv uživatelům v Axxon Next

Správa uložiště

Oblast managementu a konfigurace uložišť funguje v prostředí Axxon Next na principu archívů, díky čemuž je celý proces vytváření a správy velice snadný a rychlý. Před veškerým ukládáním záznamu si tedy uživatel nejprve musí vytvořit a pojmenovat jeden či více archívů. Těmto archívům se poté přiřadí jednotlivé disky, ať už lokální či síťové, a na nich se podobně jako u konkurence manuálně alokuje část úložného prostoru. Posledním krokem je přiřazení konkrétních kamer, které budou nahrávat do zvoleného archívu. Axxon rovněž umožnuje provázání mezi archívy, např. archív 1 je možné využít jako dočasné zastoupení pro archív 2, a to pouze u konkrétních kamer. Uživatel si dále může nastavit, jak dlouho se mají data ukládat, vymezit ukládání pouze pro určitou snímkovou frekvenci dané kamery nebo nastavit délku před-načteného záznamu. Velice dobře je vyřešeno i exportování záznamu, kdy software nabízí přehledné nastavení výsledného formátu exportu.

Uživatelské rozhraní

Instalace VMS Axxon Next je velice jednoduchá a bez větších obtíží ji zvládne i nezkušený uživatel. Software automaticky nabídne stažení dodatečných ovladačů, bez kterých není zajištěna funkčnost systému. Jedinou volbou je v tomto procesu nabídka instalace pouze serveru, nebo serveru i klienta na jednu pracovní stanici. Po instalaci software nabídne, kterou edici softwaru chceme aktivovat.

Celkový vizuální dojem Axxon Next nepůsobí tak přívětivě, jako konkurenční VMS. Design softwaru je těžkopádný a přehlednost je v mnoha kategoriích značně chaotická, např. při zobrazení živého záběru. S tím souvisí i ovládání systému, kdy si uživatel opravu musí nějaký čas zvykat, případně nahlédnout do manuálu. Na druhou stranu software reaguje na provedené změny nebo požadavky poměrně rychle a bez větších obtíží i na slabším stroji. Axxon navíc umožnuje vytvoření tzv. Hot keys, kde si můžeme ovládání softwaru přizpůsobit pomocí klávesových zkratek.

Software je v současné době přeložen do 21 jazyků, mezi které patří např. i slovenština. Bohužel český překlad zatím dostupný není a stejně tak Axxon nemá své zastoupení technické podpory v Česku. Společnost Axxon navíc garantuje nezpoplatněnou technickou podporu pouze pro vyšší edice softwaru, tudíž pokud se uživatel rozhodne používat pouze edici Free, nemá na podporu nárok.

Hardwarová náročnost

Společnost AxxonSoft uvádí v dokumentaci k Axxon Next pouze minimální a doporučené parametry grafické karty, respektive konkrétní modely karet. Pro získání údajů o parametrech CPU, RAM, disků a podobně je nutné využít hardwarového kalkulátoru, který je dostupný na webových stránkách AxxonSoft. Zmíněný kalkulátor byl využit pro simulování obdobného sestavení kamer, jako je v laboratoři 54/209.

Tab. 13. HW nároky Axxon Next – doporučené požadavky [24]

Komponent	Požadavek
Grafická karta	NVIDIA GeForce 200 a vyšší, ATI Radeon HD 5000 nebo AMD Radeon HD 6000 a vyšší

Tab. 14. HW nároky Axxon Next – minimální požadavky [24]

Komponent	Požadavek
Grafická karta	NVIDIA GeForce 7300LE a vyšší

Finanční náročnost

Vzhledem ke skutečnosti, že současná 4. verze VMS Axxon Next je dostupná v několika edicích, liší se i výsledná cena za pořízení softwarových licencí. Je však třeba mít na paměti, že jednotlivé edice nelze sloučit na jednom serveru, tedy každá licence potřebuje vlastní server. Bez ohledu na výrobce kamery si musí uživatel pořídit kamerové licence podle typu edice Axxon Next, který chce dále využívat. Pouze edice Axxon Next Free je zcela zdarma.

Tab. 15. Ceník jednotlivých typů licencí Axxon Next

Typ licence	Cena (v Eurech)
Start	40
Professional	75
Universe	165

4.2.2 Evaluační tabulka a rekapitulace VMS Axxon Next

Tab. 16. Evaluační tabulka Axxon Next, část 1.

Kategorie	Kritéria	% váha	Bodové ohodnocení	Dílčí výsledek	Celkové hodnocení
Monitoring a záznam	Možnosti živého pohledu	35	4	1,40 ~ 28 %	**60 %**
	Možnosti prohlížení záznamu	35	2	0,70 ~ 14 %	
	Ovládání PTZ funkcí	20	4	0,80 ~ 16 %	
	Možnosti nastavení obrazových a zvukových vlastností	10	1	0,10 ~ 2 %	
Komunikace a podpora zařízení	Podpora zařízení	50	5	2,50 ~ 50 %	**70 %**
	Architektura a platformy	25	3	0,75 ~ 15 %	
	Možnosti integrace s jinými systémy	25	1	0,25 ~ 5 %	
Management a konfigurace událostí	Možnosti konfigurace událostí	70	4	2,80 ~ 56 %	**86 %**
	Inteligentní funkce	30	5	1,50 ~ 30 %	
Administrace uživatelských práv	Možnosti administrace práv	100	3	3,00 ~ 60 %	**60 %**
Správa uložiště	Možnosti správy uložiště	100	4	4,00 ~ 80 %	**80 %**

Tab. 17. Evaluační tabulka Axxon Next, část 2.

Kategorie	Kritéria	% váha	Bodové ohodnocení	Dílčí výsledek	Celkové hodnocení
Uživatelské rozhraní	Instalace	10	5	0,5 ~ 10 %	**42 %**
	Přehlednost a ovládání	40	1	0,4 ~ 8 %	
	Lokalizace	20	3	0,6 ~ 12 %	
	Technická podpora	30	2	0,6 ~ 12 %	
Hardwarová náročnost	Provozní požadavky	100	4	4,00 ~ 80 %	**80 %**
Finanční náročnost	Licenční model a výsledná cena	100	4	4,00 ~ 80 %	**80 %**

Axxon Next je pokročilé VMS řešení od ruského výrobce AxxonSoft. Tento VMS vyniká obzvlášť v kategoriích managementu a konfigurace událostí, správy uložiště a hardwarových i finančních nárocích. Na rozdíl od ostatních VMS Axxon Next implementuje široké spektrum inteligentních funkcí přímo do softwaru. Díky této skutečnosti tak zákazník vyhledávající především tyto funkce razantně ušetří, neboť nemusí dokupovat nadstavbové moduly nebo licencovat aplikace třetích stran. Na druhou stranu konfigurace inteligentních funkcí není lehkou záležitostí a vyžaduje určité znalosti. Software také podporuje značnou řadu výrobců kamer a není tak náročný na výkon pracovní stanice, díky čemuž může snadněji nalézt své místo uplatnění. Zajímavá je i licenční politika Axxon Next, díky které lze software využívat v základní edici zdarma nebo v plné verzi po neomezeně dlouhou dobu, avšak pouze v určitých hodinách.

Zásadními neduhy trpí Axxon Next hlavně v oblasti uživatelského rozhraní. Na první pohled je patrné, že celkovému designu softwaru nebyla věnována taková pozornost, jakou by si zasluhoval. Tato skutečnost navíc značně zasahuje i do ostatních kategorií. I přes širokou škálu funkcí je poněkud problematické software správným způsobem konfigurovat a využít tak jeho plný potenciál.

4.3 Milestone XProtect

Společnost Milestone Systems, založená v roce 1998 se sídlem v Dánsku, patří mezi světové leadery v oblasti vývoje VMS. Portfolio produktů Milestone zahrnuje pokročilý VMS XProtect, dále pak Milestone Arcus, což softwarová platforma zabudovaná přímo v HW zařízeních, díky čemuž mohou partneři Milestone svým klientům nabízet řešení na míru. Milestone rovněž nabízí speciální sadu NVR zařízení s předinstalovaným VMS, zvané Milestone Husky, které jsou uzpůsobeny k menším aplikacím v dohledových videosystémech. Společnost také nabízí dohled ve formě placené služby Milestone Care. [25]

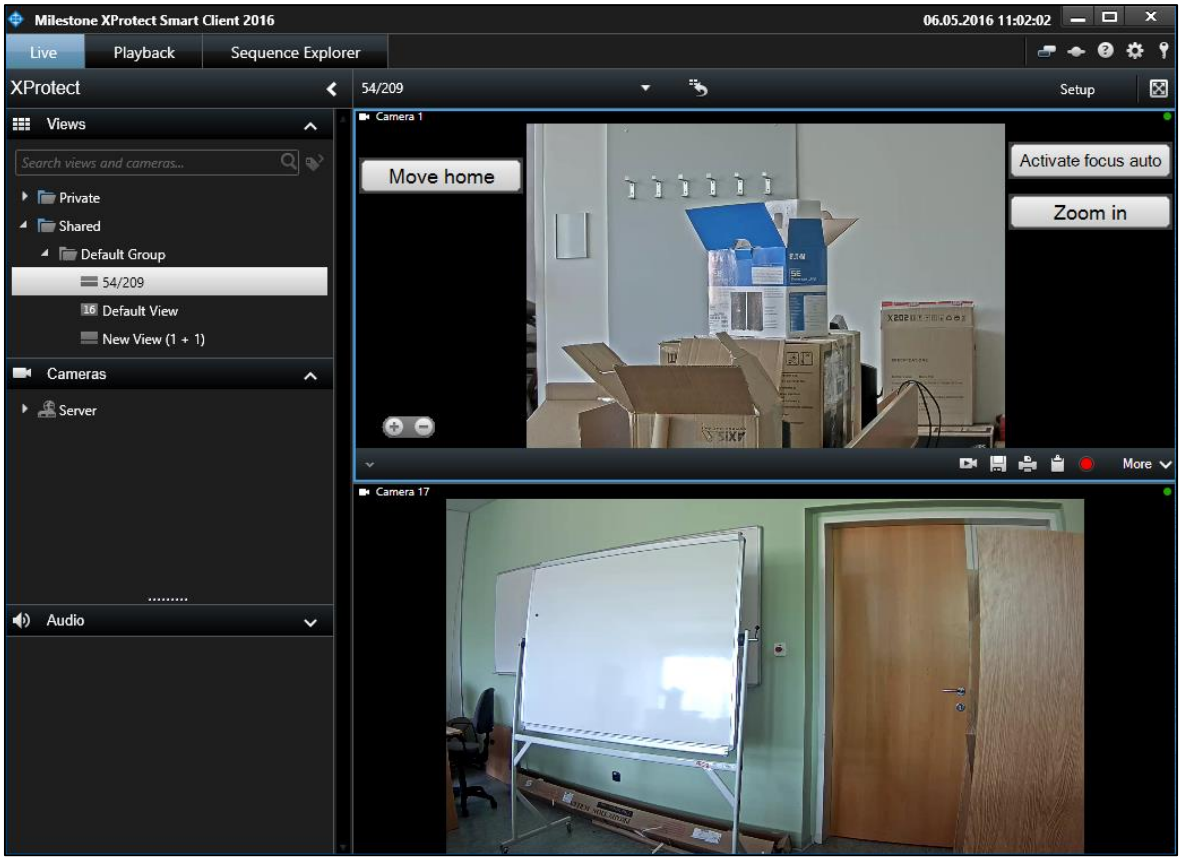
K následujícímu testování byl zvolen zmíněný VMS Milestone XProtect. Společnost tvrdí, že XProtect je kompatibilní s více jak 3 500 zařízeními od téměř 150 světových výrobců. Stejně jako konkurenční VMS, je i XProtect je nabízen v několika různých edicích. Konkrétně se jedná o XProtect Go, Essential, Express, Professional, Enterprise, Expert a Corporate. Srovnávací dokument veškerých parametrů těchto edic je dostupný na webových stránkách Milestone. Od verze Essential jsou také dostupné dodatečné zásuvné moduly, které skýtají další nadstandardní funkce. Jedná se např. o video analytiku, pokročilý management přístupu, podporu nejmodernějších video stěn a mnoho dalších. Některé z nich budou rovněž součástí testování. Pro odzkoušení softwaru Milestone jsme zvolili edici Professional, která je díky rozsahu funkčních vlastností považována za právoplatný nadstandard na poli VMS. Tato verze se rovněž bude nacházet v učebně 54/209. Velkou výhodou byl při realizaci testování fakt, že Milestone nabízí k veškerým edicím 30 – denní trial verzi zdarma, díky čemuž bylo možné software otestovat ještě před zakoupením licencí.

4.3.1 Evaluace Milestone XProtect

Monitoring a záznam

Veškeré prvky kategorie monitoringu a záznamu jsou zahrnuty v dohledové aplikaci XProtect, nazvané Smart Client. Aplikace obsahuje 4 oddělitelné záložky, jež jsou určené pro sledování živého obrazu, přehrávání záznamu, průzkum sekvencí a správu alarmů. V záložce živého obrazu software umožnuje přepínat mezi dvěma stavy – sledovacím a konfiguračním. V konfiguračním módu se zpřístupní možnosti nastavení pohledu, vytváření dohledových ploch, přidání map objektu nebo vytvoření klávesových zkratek. Další velice užitečnou funkcí jsou tzv. překryvná tlačítka. Jedna se o předdefinovaná funkční tlačítka, která lze

jednoduše přetáhnout přímo do záběru z kamery. Po stisknutí tlačítek se může např. manuálně spustit nahrávání, vymazat indikátor pohybu pro vybranou kameru, vymazat indikátor událostí pro danou kameru a mnoho dalších. S těmito tlačítky jsou rovněž provázány i možnosti ovládání PTZ funkcí, které lze také zvlášť vynášet přímo do obrazu. Do okraje dohledové plochy tak můžeme např. umístit tlačítko pro aktivaci automatického zaostření nebo pohybu do určitého směru či přednastavené pozice.



Obr. 22. Dohledová plocha v XProtect

Prohlížení záznamu je v XProtect také velice chytře vyřešeno. Svou zásluhu na tom beze sporu nese i povedený design uživatelského rozhraní. V záložce přehrávání se nabízí klasická časová osa pro dohledání záznamu. Dodatečnou funkcí je, podobně jako v ACS, Smart Search. Tato funkce dokáže vyhledávat a třídit záznam podle detekce pohybu. Úsek záznamu je rovněž barevně označen dle událostí a je možné jej kdykoliv jednoduše exportovat v jednom z nabízených formátů. V čem ale XProtect vyniká, je funkce zvaná „Sequence Explorer“, tedy průzkumník sekvencí. Průzkumník rozděluje záznam do několika libovolně dlouhých intervalů, což výrazně ulehčuje hledání konkrétní události v záznamu.

Nastavování obrazových a zvukových vlastností kamer neprobíhá v aplikaci Smart Client, nýbrž v Management Application. Kromě konfigurace celého systému se zde také upravují klasické parametry kamer (snímková frekvence, kompresní formát, jas, kontrast atd.).

Komunikace a podpora zařízení

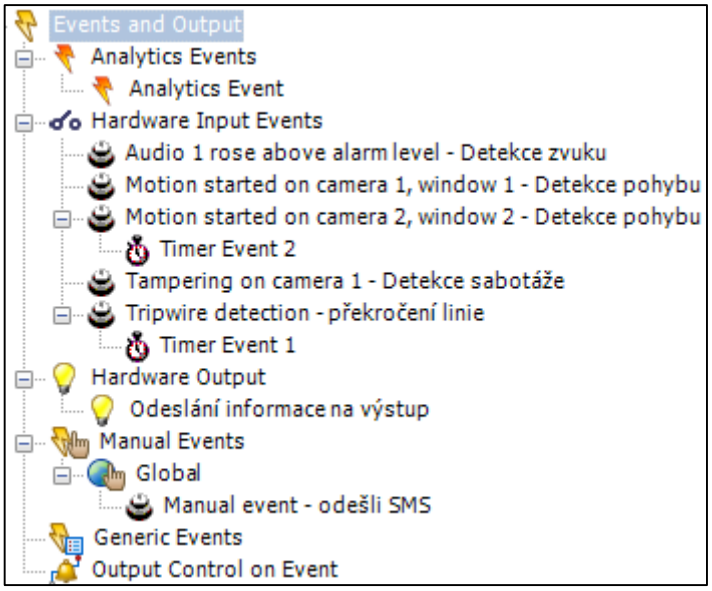
Jak již bylo zmíněno výše, XProtect by měl být kompatibilní s více jak 3 500 zařízeními. I když se tato suma může zdát jako velké číslo, před pořízením softwaru je každopádně vhodné nejprve zkontrolovat vzájemnou kompatibilitu s vlastněným hardwarem. A ačkoliv jsou společnosti Axis a Milestone spíše partneři, než konkurenti, některé z kamer Axis se nepodařilo se softwarem spárovat. Příčinou této skutečnosti je nejspíše fakt, že řada kamer v laboratoři 54/209 pochází z poslední výrobní řady a jsou tedy poměrně nové. Pokud XProtect dokázal kameru identifikovat, tak samotná registrace do softwaru už byla otázka několika sekund.

Co se týče architektury a platforem VMS XProtect, tak společnost Milestone volí poněkud odlišné řešení, než konkurence. Možnost instalace serveru na jednu pracovní stanici zůstává, nicméně XProtect má rozdělenou aplikaci pro dohled a konfiguraci systému. Zatímco např. ACS nebo AxxonNext nabízí veškeré možnosti správy systému a současně pohled z kamer v jedné uživatelské aplikaci, Milestone v zásadě používá Management Application pro správu a konfiguraci a Smart Client pro dohled nad VSS. K těmto aplikacím je ještě k dispozici XProtect Web Client, který slouží pro management systému pomocí webového prohlížeče. XProtect také umožnuje připojení přes chytrý telefon skrze aplikace Milestone Mobile Client. Mezi podporované OS patří Microsoft Windows 10 Pro & Enterprise, Windows 8.1 Pro, Windows 8 Pro & Enterprise, Windows 7 Ultimate & Pro & Enterprise, Server 2012, Server 2012 R2 a Server 2008 R2. Pro mobilní platformy pak Android 4, iOS 9.2 a Windows Phone 8.

Společnost Milestone označuje svoje VMS řešení jako otevřenou platformu, díky níž je možné software snadno integrovat s velkou řadou softwarových aplikací třetích stran. Milestone v současné době spolupracuje se značným množstvím renomovaných firem, mezi které patří např. AGORA (informační management fyzické ochrany), Agent VI (video analytika), Bosch (přístupové systémy), Hewlett Packard (servery), Dell (uložiště) a mnoho dalších. Kompletní seznam partnerských řešení je možné nalézt na webových stránkách společnosti Milestone.

Management a konfigurace událostí

Management a konfigurace událostí probíhá prostřednictvím Management Application. Rozhraní je v tomto případě velmi podobné Axxon Next. Celá oblast událostí je rozdělena do několika kategorií, konkrétně analytické události, události logických I/, manuální události a několik dalších. Do jednotlivých kategorií lze poté přiřazovat vytvořené události a těm poté upravovat parametry. Uvedený obrázek slouží jako příklad struktury událostí.



Obr. 23. Struktura konfigurace událostí v XProtect

Vzhledem k tomu, že software je uzpůsoben k integraci s jinými softwary, toho sám v této kategorii tolik nenabízí. Software má zabudované pouze základní funkce, jako je detekce pohybu, sabotáže, překročení linie nebo detekce zvuku. Pokud chce uživatel využívat pokročilé řešení, má k dispozici několik variant zásuvných modulů přímo od společnosti Milestone. XProtect Professional v současné době umožnuje instalaci 8 různých modulů, jenž slouží např. k rozpoznávání SPZ, čárových kódu, vylepšenému managementu přístupu nebo k ověřování obchodních transakcí. Kromě zmíněných modulů je rovněž možné software integrovat s partnerskými video analytickými softwary třetích stran.

Administrace uživatelských práv

Proces administrace probíhá prostřednictvím aplikace Management Application. Struktura uživatelů a pravomocí je velmi jednoduchá, v podstatě se jedná jen o systém 2 rolí, a sice administrátor a „základní uživatel“, anglicky „Basic user“. Administrátorů může být libovolný počet a mohou být rozmístěni do libovolně vytvořených skupin. Navíc také mají samozřejmě přístup ke všem funkcím a konfiguraci celého systému. Základní uživatel poté

může být vytvořen pouze prostřednictvím VMS, nebo je možné jej svázat s účtem Windows. Po procesu vytvoření zbývá přidělit jednotlivé oprávnění a zařadit uživatele do skupiny, případně pojmenovat atd. Níže uvedený obrázek z důvodu šířky obsahuje stránky pouze část kategorií, ve kterých se přidělují práva.

User and Function Access Summary:

User Name	User Type	Live	Playback	Setup	Edit Shared Views	Edit Private Views	Administrator Access	Access to Cameras
Operátor 1	Basic	☑	☐	☐	☑	☑	☐	All Cameras

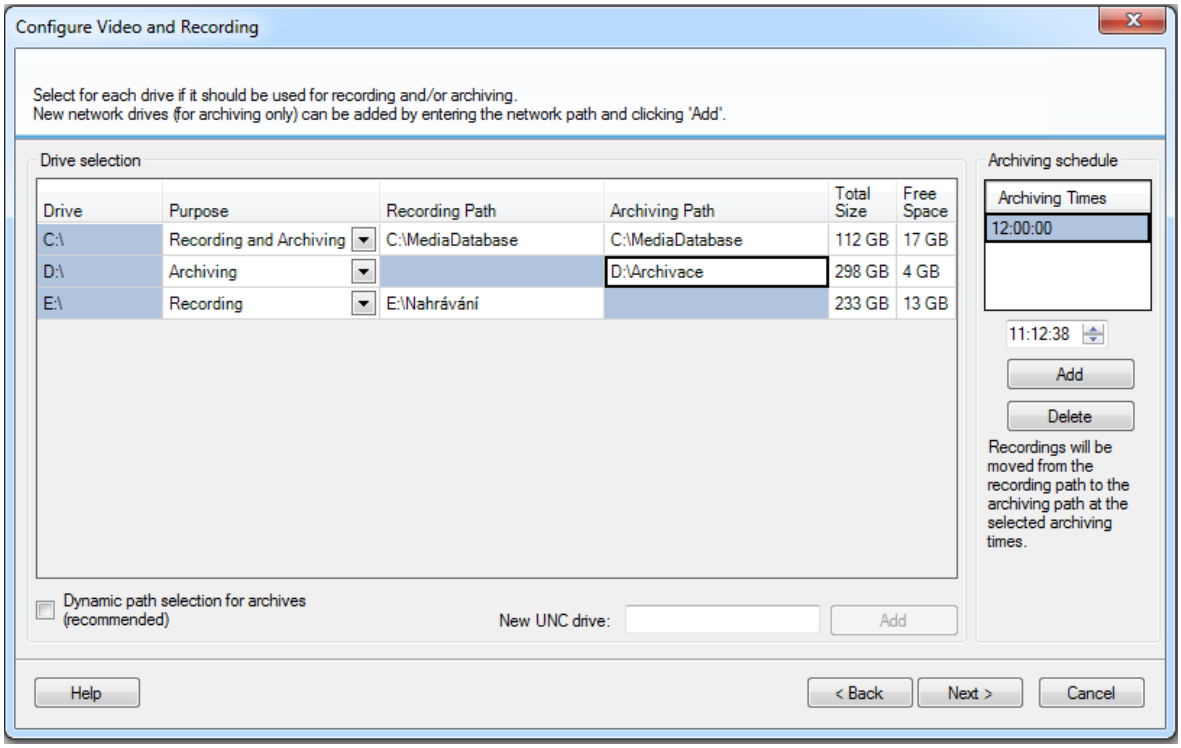
Camera and Feature Access Details:

Camera	Live	PTZ	PTZ Presets	Manage Presets	Output	Events
Axis M1125	☑	☑	☑	☐	☐	☑
Camera 2	☑	☑	☐	☐	☐	☑
Camera 3	☑	☐	☑	☐	☑	☐
Camera 4	☑	☐	☑	☑	☐	☑
Camera 5	☑	☑	☐	☐	☑	☐
Camera 6	☑	☑	☑	☑	☑	☑
Camera 7	☑	☑	☑	☑	☑	☑

Obr. 24. Přidělování uživatelských práv v XProtect

Správa uložiště

Konfigurace úložného prostoru pro záznam probíhá v XProtect na první pohled odlišněji, než u konkurenčních VMS. Celý proces je svázán i s vytvářením video profilů, tedy parametrů živého pohledu a výsledného záznamu. Nejprve tedy vybraným kamerám nastavíme hodnoty snímkové frekvence a metodu spuštění nahrávání (nepřetržité nebo dle události) a až poté přiřadíme libovolné uložiště. XProtect rozděluje typ uložiště podle účelu, tedy pro nahrávání a archivaci. Oba typy je rovněž možné zahrnout do jednoho uložiště. Součástí konfigurace je také časový plán, ve kterém se stanoví čas archivace. Jedná se o proces přesouvání dat z uložiště pro nahrávání do cílové složky pro archivaci.



Obr. 25. Správa uložiště v XProtect

Uživatelské rozhraní

Instalační soubor XProtect Professional má přibližně třikrát větší velikost než ostatní VMS, z čehož vyplývá podstatně delší doba instalace. Software si také automaticky doinstaluje potřebné ovladače. Při instalaci si rovněž můžeme zvolit, které komponenty chceme nainstalovat. Kromě klasického výběru VMS serveru a klienta je navíc k dispozici Event Server, který slouží pro management veškerých informací z událostí, alarmů, map a statusu systému. Pro případ využívání mobilního nebo webového klienta je také nutné nainstalovat Mobile Server. Software je dostupný v celkem 30 světových jazycích, včetně češtiny. Tento výčet se ovšem týká pouze dohledové aplikace Smart Client. V případě konfigurační Management Application je na výběr pouze z 12 jazyků, mezi kterými se čeština nenachází.

Přehlednost softwaru je i díky konceptu rozdělení na několik částí na vysoké úrovni. Design Management Application je jednoduchý a účelný. Naopak Smart Client se chlubí povedeným grafickým zpracováním, které je také zároveň velice přehledné. Uživatelské rozhraní je intuitivní, klíčové prvky jsou vhodně rozmístěné a i v případě minimálních znalostí softwaru je možné XProtect pohodlně ovládat. Pouze v kategorii technické podpory v České republice XProtect zatím poněkud pokulhává. Veškeré požadavky jsou odesílány do hlavního sídla v Dánsku. Milestone však nabízí velké množství různého edukačního materiálu a manuálů k softwaru.

Hardwarová náročnost

Milestone v kategorii HW nároků udává pouze minimální požadavky pro rozběhnutí VMS. Ty se dále dělí na několik druhů v závislosti na typu instalace.

Tab. 18. HW nároky XProtect Professional – souhrnné požadavky [26]

Komponent	Požadavek
Procesor	Intel Pentium 4 @ 2,4 GHz a vyšší
Paměť RAM	8 GB
Grafická karta	Nespecifikovaný model podporující rozlišení 1024x768 a 16-bitovou barevnou hloubku a vyšší

Tab. 19. HW nároky XProtect Professional – Smart Client s SW dekódování [26]

Komponent	Požadavek
Procesor	Blíže nespecifikovaný Intel Core 2 Duo
Paměť RAM	1 GB
Grafická karta	Nespecifikovaný model podporující rozlišení 1024x768, 16-bitovou barevnou hloubku a DirectX 9.0 a vyšší

Tab. 20. HW nároky XProtect Professional – Smart client s HW dekódování [26]

Komponent	Požadavek
Procesor	Blíže nespecifikovaný Intel CPU s technologií QuickSync
Paměť RAM	1 GB
Grafická karta	Nespecifikovaný model podporující rozlišení 1280x1024, 32-bitovou barevnou hloubku a DirectX 11.0

Finanční náročnost

Milestone využívá pro svůj software 3 typy softwarových licencí, které se dále dělí dle použité edice VMS. V zásadě se jedná o tzv. „Base license“, „Hardware license“ a „Add-on license“. Base license, neboli základní licence, slouží k registraci softwaru XProtect. Jak už bylo zmíněno výše, veškeré edice XProtect jsou k dispozici v 30-denní zkušební verzi. Po uplynutí této lhůty je však nutné zakoupit licenci k softwaru. Hardwarové licence se pak pojí přímo k jednotlivým zařízením, kdy každé zařízení zakomponované do VMS musí mít svou vlastní licenci. Poslední kategorií jsou tzv. Add-on licence, které se vztahují k zásuvným modulům XProtect. Vzhledem k množství modulů a k nim vztahujících se cen nebudou veškeré údaje uvedeny. V konečném hodnocení se promítne pouze cena za edici Professional.

Tab. 21. Ceník Base licencí Milestone XProtect

Typ licence	Cena (v Eurech)
Essential	79
Express	159
Professional	499
Enterprise	1 999
Expert	1 999
Corporate	2 523

Tab. 22. Ceník Hardware licencí Milestone XProtect

Typ licence	Cena (v Eurech)
Essential	39
Express	79
Professional	149
Enterprise	199
Expert	199
Corporate	269

4.3.2 Evaluační tabulka a rekapitulace VMS Milestone XProtect Professional

Tab. 23. Evaluační tabulka XProtect, část 1.

Kategorie	Kritéria	% váha	Bodové ohodnocení	Dílčí výsledek	Celkové hodnocení
Monitoring a záznam	Možnosti živého pohledu	35	5	1,75 ~ 35 %	**96 %**
	Možnosti prohlížení záznamu	35	5	1,75 ~ 35 %	
	Ovládání PTZ funkcí	20	5	1,00 ~ 20 %	
	Možnosti nastavení obrazových a zvukových vlastností	10	3	0,3 ~ 6 %	
Komunikace a podpora zařízení	Podpora zařízení	50	4	2,00 ~ 40 %	**85 %**
	Architektura a platformy	25	4	1,00 ~ 20 %	
	Možnosti integrace s jinými systémy	25	5	1,25 ~ 25 %	
Management a konfigurace událostí	Možnosti konfigurace událostí	70	2	1,40 ~ 28 %	**46 %**
	Inteligentní funkce	30	3	0,90 ~ 18 %	
Administrace uživatelských práv	Možnosti administrace práv	100	5	5,00 ~ 100 %	**100 %**
Správa uložiště	Možnosti správy uložiště	100	4	4,00 ~ 80 %	**80 %**

Tab. 24. Evaluační tabulka XProtect, část 2.

Kategorie	Kritéria	% váha	Bodové ohodnocení	Dílčí výsledek	Celkové hodnocení
Uživatelské rozhraní	Instalace	10	3	0,30 ~ 6 %	**72 %**
	Přehlednost a ovládání	40	4	1,60 ~ 32 %	
	Lokalizace	20	4	0,80 ~ 16 %	
	Technická podpora	30	3	0,90 ~ 18 %	
Hardwarová náročnost	Provozní požadavky	100	4	4,00 ~ 80 %	**80 %**
Finanční náročnost	Licenční model a výsledná cena	100	1	1,00 ~ 20 %	**20 %**

VMS XProtect Professional je produkt nabízený dánskou společností Milestone. Včetně této edice tak Milestone nabízí celkem 6 možných variant svého softwaru, jejichž úkolem je pokrýt co možná nejširší rozsah instalací. Pro testování byla proto vybrána verze Professional, která je v mnoha aspektech podobná ostatním hodnoceným VMS. V porovnání s konkurencí tak software naprosto vyniká hlavně v kategoriích monitoringu a záznamu, komunikaci a podpory zařízení a administraci uživatelských práv. Svou zásluhu na tom nese především chytře vyřešené rozhraní dohledové aplikace, která kombinuje povedený design s množstvím užitečných funkcí. Vzhledem ke konceptu otevřené platformy se uživatelům rovněž nabízí celá řada možností integrace. Navíc I přes pěkné grafické zpracování zůstává software relativně nenáročným na výpočetní výkon pracovní stanice.

Pouze v kategoriích managementu a konfigurace událostí a finanční náročnosti XProtect poněkud strádá. Aplikace pro správu událostí již není tak přehledná, jako aplikace dohledová, a celý proces konfigurace událostí je zbytečně komplikovaný a nepřehledný. Navíc v této kategorii software nenabízí žádné nadstandardní funkce, které by se nenalézaly u konkurence. Stejně tak vzhledem k licenční politice Milestone je výsledná cena softwaru razantně vyšší, než u ostatních VMS s podobným rozsahem funkčních vlastností.

4.4 ATEAS Security

Společnost ATEAS CZ s.r.o. je, dle jejich vlastních slov, ryze českou softwarovou společností zaměřenou na oblast IP bezpečnostních technologií s dlouholetou tradicí v oblasti softwarového vývoje, implementace otevřených standardů a výroby vysoce optimalizovaných řešení, což oceňují zákazníci napříč všemi sektory. Jejich hlavním produktem je VMS ATEAS Security, který společnost charakterizuje jako komplexní video dohledové řešení pro profesionální IP VSS. ATEAS Security je taktéž dodáván v několika edicích pro efektivní pokrytí rozsahu instalace. V zásadě se jedná o ATEAS Security Start, Home, Professional Light, Professional a Unlimited. Komparační tabulku jednotlivých edic lze nalézt na webových stránkách společnosti ATEAS. [27]

Pro účely testování byla vybrána verze Unlimited. Jedná se o nejpokročilejší edici softwaru s největším rozsahem funkčních vlastností a s možností připojení neomezeného počtu kamer a serverů. Tato verze bude rovněž studenty využívána při zpracování laboratorních úloh v učebně 54/209.

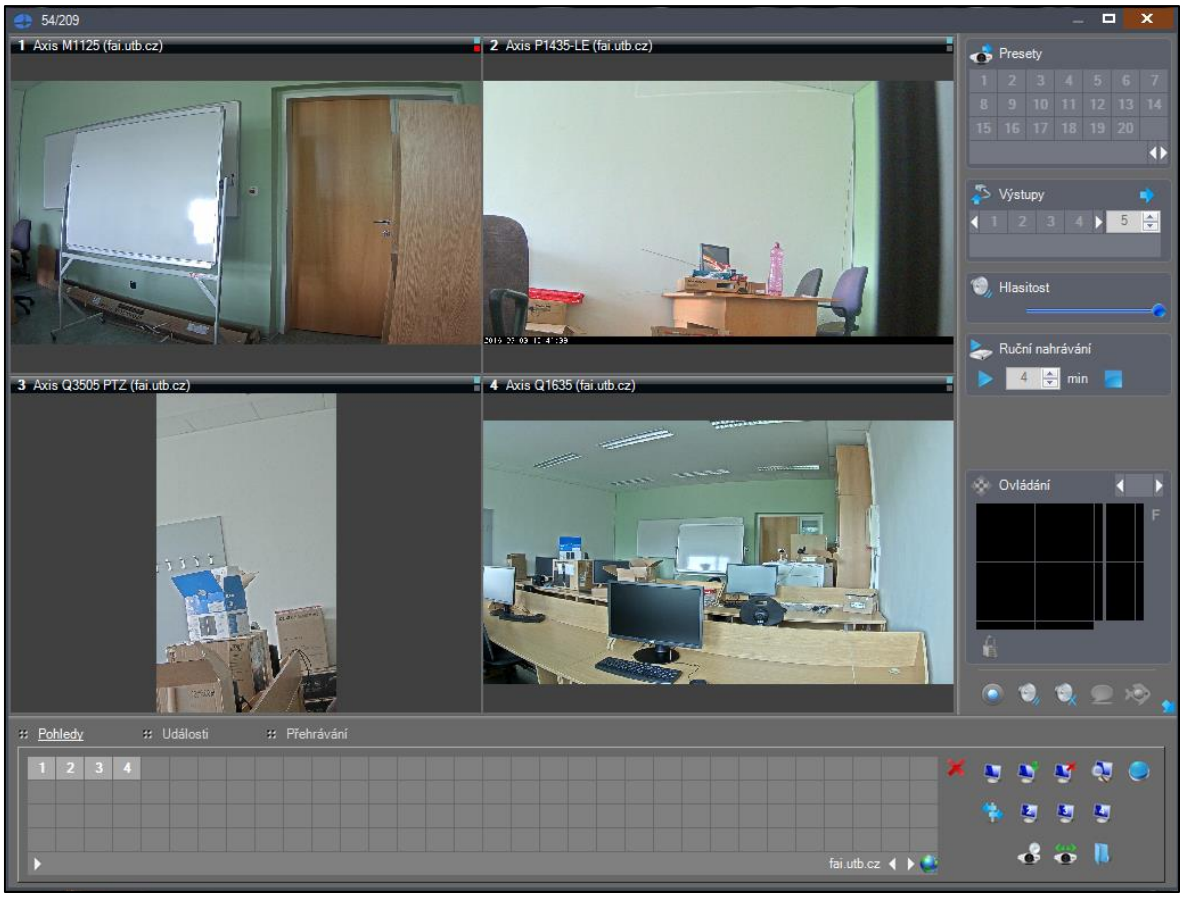
4.4.1 Evaluace ATEAS Security

Monitoring a záznam

ATEAS Security nabízí relativně jednoduché rozhraní živého pohledu se značným množstvím funkcí. Řada z nich je ovšem reprezentována pouze ikonami na spodní liště, a proto není na první pohled patrné, o které funkce se jedná. Samotné vytváření pohledů je velice prosté, software nabízí předdefinované dlaždice o určitém počtu políček pro kamerové pohledy, případně si může uživatel vytvořit vlastní rozvržení nebo aktivovat tzv. dynamický pohled, který automaticky uzpůsobí dohledovou plochu počtu kamer. Pokud má uživatel práva administrátora, smí navíc vytvořené pohledy sdílet napříč ostatními klientskými stanicemi. Nicméně manipulace s objektovými mapami není v prostředí ATEAS Security intuitivní jako u konkurence a vyžaduje větší znalosti softwaru.

Prohlížení a manipulace se záznamem je v prostředí ATEAS Security rozděleno do dvou sekcí. V dohledovém okně je umístěn přímý odkaz na zjednodušené přehrávání záznamu, kde je zobrazena jednoduchá časová osa a tlačítka pro přehrávání. Vybraný interval záznamu je možné okamžitě exportovat díky vestavěnému manažeru stahování sekvencí. Pro přesnější manipulaci se záznamem slouží samostatné okno, nazvané jednoduše „Záznam“. Zde lze na kalendářním plánu spatřit dny a hodiny, kdy byl záznam proveden. Po zvolení konkrétního

data nebo času se dále zobrazí další okno, kde je možné záznam rozdělit na libovolné intervaly podle minut a poté je exportovat opět skrze manažera stahování. Kromě klasického vyhledávání lze rovněž vyhledávat pomocí metadat, kterými je záznam opatřen v případě aktivace událostí. Dodatečnými funkcemi je deník poplachů a vestavěný přehrávač uložených scén.



Obr. 26. Dohledová plocha v prostředí ATEAS Security

Ovládání PTZ funkcí je provázáno s rozhraním živého pohledu. Nejprve je ovšem nutné funkce povolit v nastavení dané kamery, a teprve poté kameru smíme ovládat. Ovládací panel bohužel není moc povedený, manipulace s kamerami je zbytečně komplikovaná a poněkud nepřesná.

V sekci administrace kamer také software obsahuje nastavení obrazových a zvukových vlastností. U obrazových parametrů, jako je snímková frekvence, komprese nebo rozlišení, lze nastavit parametry na hodnotu „implicitní“ a „vlastní“. Implicitní hodnoty jsou hodnoty nastavené přímo v kameře. Při zvolení položky „vlastní“ software automaticky nabídne výběr z přednastavených hodnot. Kromě těchto základních parametrů lze také upravit parametry datového toku nebo aktivovat rozšířenou vyrovnávací paměť pro plynulé video.

Komunikace a podpora zařízení

Společnost ATEAS ve svých propagačních materiálech uvádí podporu kamer od řady výrobců, jako jsou např. Axis, Sony, Vivotek, Panasonic a další. Konkrétní číslo podporovaných zařízení nebo výčet veškerých výrobců bohužel k dispozici není. Od verze ATEAS Security 4 je však deklarována podpora zařízení prostřednictvím standardu ONVIF. Vzhledem ke skutečnosti, že ATEAS patří mezi partnery společnosti Axis, se nevyskytl v případě testování ATEAS Security pomocí Axis kamer žádný problém. Software dokázal velice rychle rozpoznat výrobce i model kamery. K přehledné registraci kamer do systému také slouží barevné odlišení, které modrou barvou reprezentuje kamery komunikující pomocí proprietárního protokolu, zatímco červená barva reprezentuje standard ONVIF.

ATEAS Security je ve své podstatě centralizované VMS s klasickou architekturou klient – server. Některé prvky architektury se však liší dle konkrétní edice softwaru. V každé edici ATEAS Security je nutné provést instalaci 3 základních aplikací – ATEAS Administrator, Security Server a Observer. ATEAS Administrator je systémový server, který slouží k centrálnímu přihlašování do systému a řízení událostí. ATEAS Security Server je kamerový server, jenž slouží ke komunikaci s kamerami, řízení toku videa nebo vyhodnocování událostí v systému. Poslední aplikací je ATEAS Observer je klientská aplikace s uživatelským rozhraním, které slouží k plnému přístupu do systému a jeho administraci. V závislosti na edici softwaru jsou pak tyto aplikace rozmístěny na určený počet pracovních stanic. Například edice Start vyžaduje instalaci obou serverových aplikací i klienta na jeden cílový počítač. Testovaná verze Unlimited však nepodléhá omezením, a proto bylo možné nainstalovat ATEAS Administrator a Security Server na server umístěný ve Vědecko-technickém parku a klientskou aplikaci Observer na počítače v laboratoři 54/209.

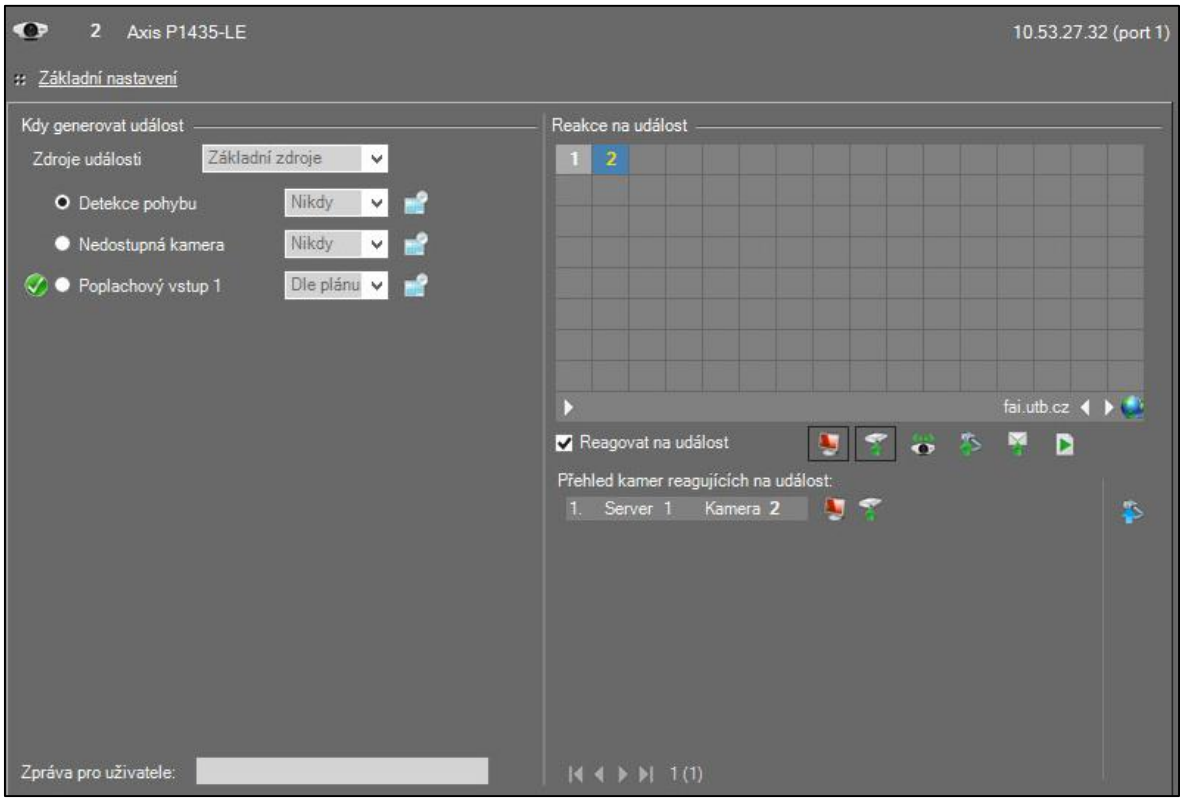
Produkty systému ATEAS Security je možné nainstalovat na zařízení s operačním systémem Windows XP, Vista, 7, 8, 10 a dále také Windows Server 2003, 2008 a 2012 bez rozdílu jeho subverze či edice. Co se týče mobilní platformy, tak se udává podpora Windows Mobile 5 & 6, Windows Phone od verze 7.5, iOS od verze 4.3 a Andoird od verze 2.2.

Společnost ATEAS dále uvolňuje svůj soubor nástrojů pro integraci (nazývaný SDK – Software Development Kit), pomocí kterého je možné přistupovat k video datům kamer a video serverů připojených ke kamerovým serverům ATEAS. SDK se skládá z programových knihoven poskytující funkcionalitu pro přístup ke kamerovému systému ATEAS, z ukázkových

programů a implementací knihoven v různých vývojářských nástrojích včetně zdrojových kódů a přeložených variant aplikací a dále také z dokumentace tříd v SDK knihovnách.

Management a konfigurace událostí

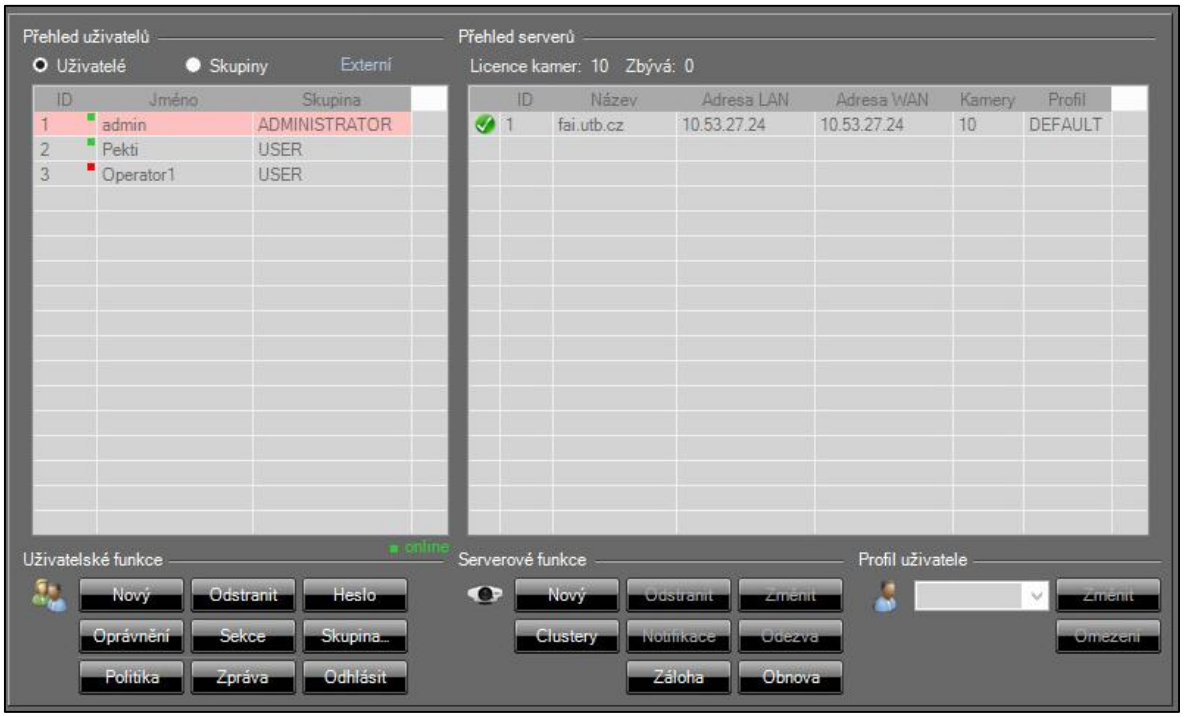
Oblast managementu a konfigurace událostí je umístěna v sekci administrace kamer, konkrétně v záložce „Události“. Zde máme na výběr zdroje událostí, ke kterým se pak přiřadí určené kamery. Zdroje událostí se dále dělí na několik kategorií podle povahy (základní zdroje, serverové zdroje, vlastní zdroje, poznávací značky, analýza a složené zdroje). K základním zdrojům patří vestavěné funkce kamer např. detekce pohybu, odpojená kamera nebo poplachový vstup. Detekce pohybu patří také do serverových zdrojů, v tomto případě je však využíván výpočetní výkon serveru. Mezí vlastní zdroje dále patří např. detekce zvuku či sabotáž kamery. Kategorie poznávacích značek, jak už z názvu vyplývá, má na starost rozpoznávání registračních značek vozidel. K využívání této funkce je však nutné zakoupit dodatečný modul ATEAS Security LPR Engine. Společnost ATEAS slibuje podporu mnoha desítek různých národních i jiných systémů poznávacích značek vozidel. V neposlední řadě kategorie analýzy zahrnuje inteligentní funkce dostupné z analytických softwarů třetí strany. Složené zdroje pak kombinují výše uvedené kategorie dohromady. K jednotlivým událostem lze poté přiřadit časový plán aktivace a dle principu následných akcí také nastavit, co se má v případě dané událostí stát. Na výběr je zobrazení aktuálního pohledu z kamery, aktivace záznamu, aktivace logického výstupu, upozornění e-mailem nebo spuštění webového prohlížeče s přednastavenou adresou. Nespornou výhodou ATEAS Security je možnost konfigurace některých základních typů událostí, jako je např. detekce pohybu. Software velice snadno umožnuje nastavit práh citlivosti i dobu adaptace samotné detekce.



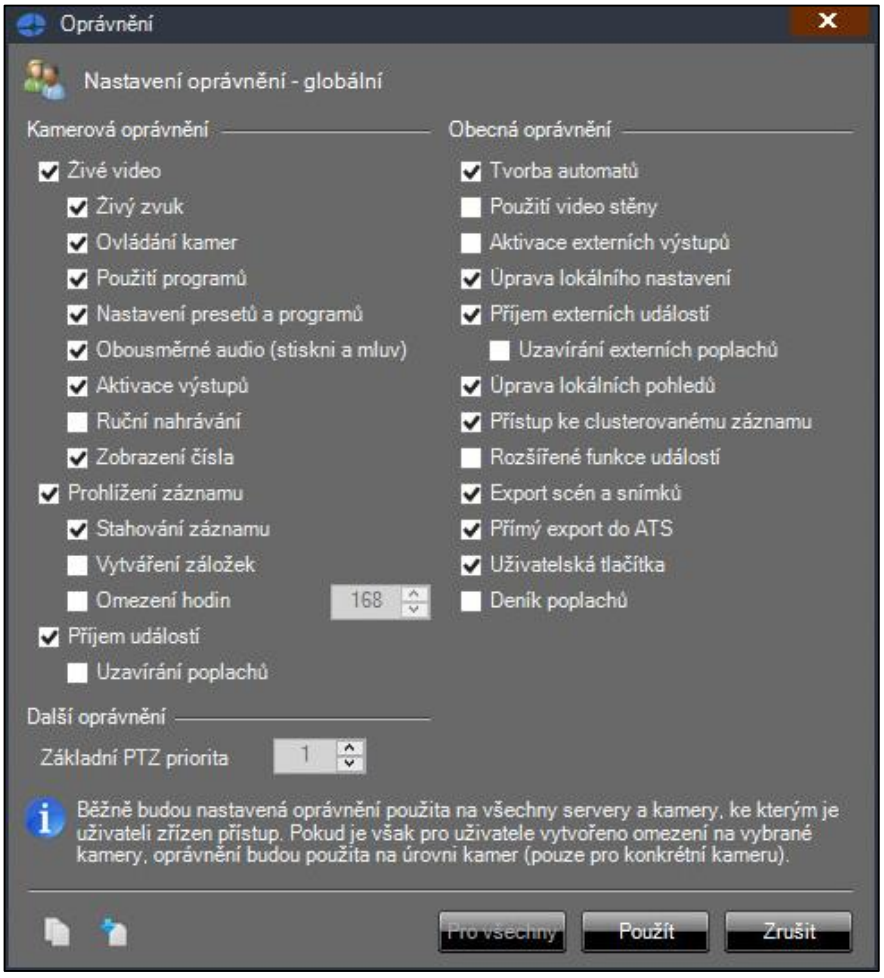
Obr. 27. Management událostí v ATEAS Security

Administrace uživatelských práv

Proces vytváření nových uživatelů a přiřazování oprávnění je v prostředí ATEAS Security poměrně nenáročnou záležitostí. Software odlišuje pouze 2 systémové role, a sice Administrátora a „obyčejného“ uživatele, nazvaného jednoduše „USER“. Na obr. Můžeme vidět okno administrace ukazující přehled veškerých uživatelů a serverů, do kterých jsou uživatelé připojeni. Zelené a červené označení u jednotlivých uživatelů symbolizuje online nebo offline stav uživatelů. Software navíc umožnuje měnit i dodatečné atributy přihlašování, jako je délka nebo platnost hesla v záložce „Politika“. Dále je také prostřednictvím administrace možné velice snadno odeslat zprávu či upozornění vybranému uživateli nebo skupině. Vzhledem k rozměrům jsou názorné obrázky z této kategorie umístěny na následující straně.



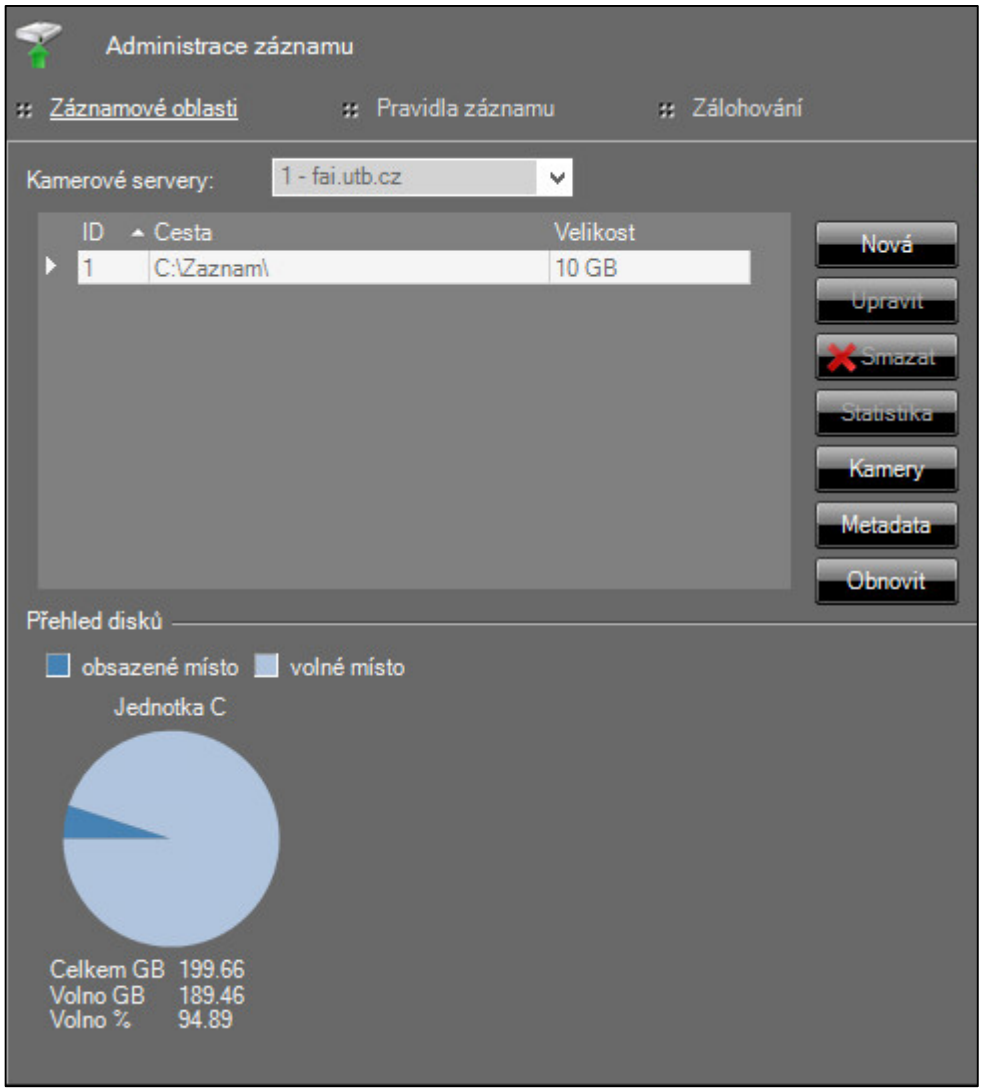
Obr. 28. Administrace uživatelů v ATEAS Security



Obr. 29. Přiřazování uživatelských práv v ATEAS Security

Správa uložiště

Oblast správy uložišť je v prostředí ATAS Security pojmenována jako administrace záznamu. Aby mohl na serveru probíhat záznam, musí být vytvořena záznamová oblast a kamery musí mít přiřazeny pravidla záznamu. Pomocí rozhraní administrace můžeme vytvořit libovolný počet záznamových oblastí, kterým alokujeme část místa z konkrétních disků. Po vytvoření záznamové oblasti lze v záložce „Pravidla záznamu“ upravit dodatečné parametry záznamu, jako je časový plán, snímková frekvence nebo aktivace nahrávání pouze při výskytu poplachu. V záložce „Zálohování“ se poté upravují pravidla zálohování pro archivaci záznamu. . Za nadstandardní funkce se v této oblastí považuje možnost zapnutí pokročilého šifrování AES a nastavení archivace metadat.

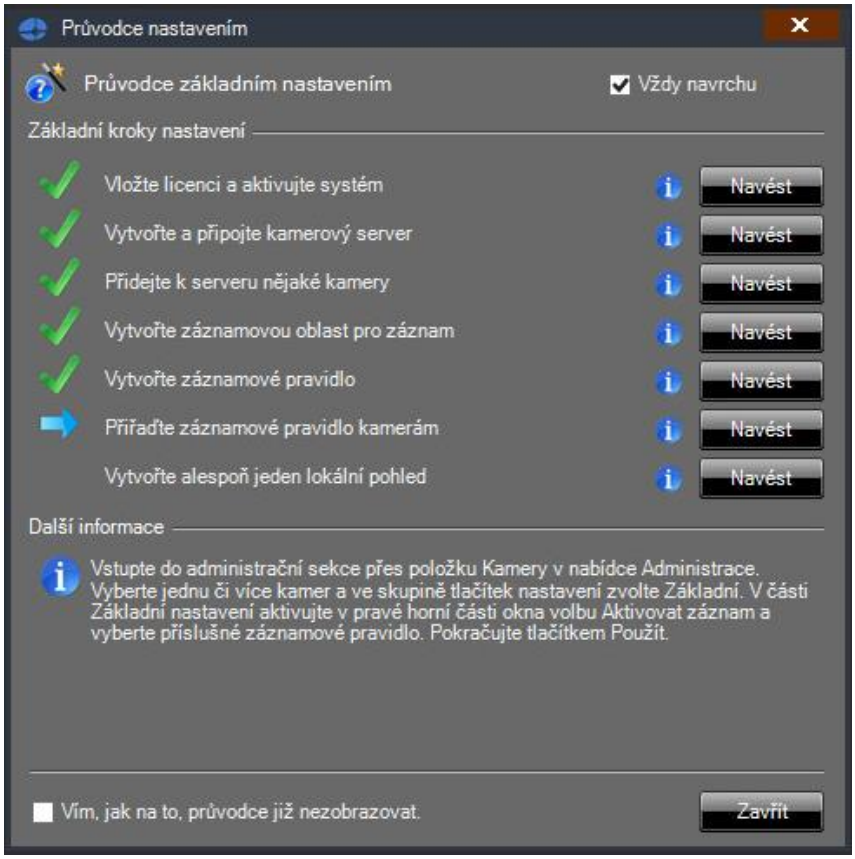


Obr. 30. Správa uložiště v ATEAS Security

Uživatelské rozhraní

Instalace ATEAS Security probíhá, na rozdíl od konkurence, v mnoha ohledech odlišně. Po spuštění instalačního souboru se automaticky spustí webový prohlížeč s odkazem na jednotlivé kroky instalace. ATEAS nás tak provádí celým procesem a dává nám možnost výběru instalace konkrétních prvků systému. Ve webovém rozhraní je také umístěn odkaz na manuál ve formátu pdf.

Design klientské aplikace je relativně neokázalý. Celé rozhraní pracuje na principu hlavní lišty, která slouží jako rozcestník k jednotlivým segmentům dohledu a konfigurace systému. Díky kompletní české lokalizaci je však pohyb v prostředí softwaru intuitivní a k základnímu rozběhnutí systému postačí i minimální znalosti. Při konfiguraci pokročilých funkcí už ATEAS Security naráží na limity svého uživatelského rozhraní a v určitých oblastech je již zkušenost se softwarem nutná. Naštěstí ATEAS Security také obsahuje vestavěného průvodce prvotním nastavením, který uživatele provede krok po kroku při prvním spuštěním programu. Kromě češtiny jsou dále k dispozici 4 další jazyky. Poskytování technické podpory nebo zaškolení obsluhy je plně v kompetenci proškolených instalačních partnerů společnosti ATEAS.



Obr. 31. Průvodce nastavením ATEAS Security

Hardwarová náročnost

Společnost ATEAS nikde ve svých materiálech neuvádí minimální ani doporučené hardwarové požadavky na provoz svého softwaru. Vestavěná nápověda ATEAS Security obsahuje pouze zmínku o akceleraci softwaru pomocí grafické karty, která je vhodná v případě dekompresi formátu H.264. Jedinou podmínkou je běh softwaru na OS Windows 7 a vyšší a také grafická karta alespoň na úrovni Intel HD 4000 a vyšší. Pro otestování náročnosti běhu softwaru tak byl využit vestavěný ukazatel vytížení HW, který je součástí klientské aplikace VMware Workstation, nazvané vSphere. Dle ukazatele software vykazoval, až na drobné výkyvy, přibližně podobnou HW náročnost, jako VMS Axxon Next nebo XProtect.

Finanční náročnost

Licenční politika ATEAS Security je v mnoha ohledech jednodušší, než u konkurenčních VMS. V zásadě existuje jen jeden typ licence, který se liší v závislosti na použité edici softwaru. Pro odzkoušení vlastností softwaru je také možné využít edici ATEAS Security Start, jež je k dispozici zcela zdarma.

Tab. 25. Ceník jednotlivých typů licencí ATEAS Security

Typ licence	Cena (v Korunách český)
Home	800
Professional Light	1 000
Professional	2 400
Unlimited	2 400

K dispozici je také nadstavbový modul LPR Engine s koncovou cenou 45 960 Kč, která je počítána pro jednu kameru. Za další kamery je nutné připlatit 5 960 Kč za kus. Uvedené ceny nemusí být vždy definitivní, licence je v některých případech možné zakoupit ve výhodnějších multilicenčních balíčcích.

4.4.2 Evaluační tabulka a rekapitulace VMS ATEAS Security Unlimited

Tab. 26. Evaluační tabulka ATEAS Security, část 1.

Kategorie	Kritéria	% váha	Bodové ohodnocení	Dílčí výsledek	Celkové hodnocení
Monitoring a záznam	Možnosti živého pohledu	35	3	1,05 ~ 21 %	**54 %**
	Možnosti prohlížení záznamu	35	3	1,05 ~ 21 %	
	Ovládání PTZ funkcí	20	1	0,20 ~ 4 %	
	Možnosti nastavení obrazových a zvukových vlastností	10	4	0,40 ~ 8 %	
Komunikace a podpora zařízení	Podpora zařízení	50	3	1,50 ~ 30 %	**75 %**
	Architektura a platformy	25	5	1,25 ~ 25 %	
	Možnosti integrace s jinými systémy	25	4	1,00 ~ 20 %	
Management a konfigurace událostí	Možnosti konfigurace událostí	70	4	2,80 ~ 56 %	**68 %**
	Inteligentní funkce	30	2	0,60 ~ 12 %	
Administrace uživatelských práv	Možnosti administrace práv	100	3	3,00 ~ 60 %	**60 %**
Správa uložiště	Možnosti správy uložiště	100	3	3,00 ~ 60 %	**60 %**

Tab. 27. Evaluační tabulka ATEAS Security, část 2.

Kategorie	Kritéria	% váha	Bodové ohodnocení	Dílčí výsledek	Celkové hodnocení
Uživatelské rozhraní	Instalace	10	5	0,50 ~ 10 %	**66 %**
	Přehlednost a ovládání	40	2	0,80 ~ 16 %	
	Lokalizace	20	4	0,80 ~ 16 %	
	Technická podpora	30	4	1,20 ~ 24 %	
Hardwarová náročnost	Provozní požadavky	100	3	3,00 ~ 60 %	**60 %**
Finanční náročnost	Licenční model a výsledná cena	100	5	5,00 ~ 100 %	**100 %**

ATEAS Security je produktem české společnosti ATEAS. Software oproti konkurenci nijak zvlášť nevyniká v žádné konkrétní kategorii, na druhou stranu ale také netrpí (až na několik výjimek) zásadními neduhy a nedostatky. Vyzdvihnout můžeme především zdařilou architekturu a širokou škálu podporovaných platforem, přehlednou instalaci, kompletní českou lokalizaci včetně manuálů nebo koncovou cenu produktu. Cenová politika ATEASu je vzhledem k nabízeným funkcí velice přívětivá a v poměru cena/výkon tak jednoznačně předčí ostatní hodnocené VMS. Software také nabízí poměrně široké možnosti integrace, konfigurace událostí nebo nastavení obrazových a zvukových vlastností.

Jedinou vadou na kráse tak zůstává uživatelské rozhraní softwaru, které se ovšem v mnoha kategoriích značně rozchází. Instalace a prvotní nastavení softwaru je velmi zjednodušené díky vestavěnému průvodci. Nicméně jakákoliv složitější manipulace a konfigurace už vyžaduje určité znalosti nebo použití manuálu. Veškeré materiály k softwaru navíc i vzhledem k značnému obsahu nezahrnují některé důležité údaje, jako jsou např. hardwarové nároky. Za zmínku také stojí nepovedený ovládací panel PTZ funkcí kamer nebo těžkopádný design webových stránek ATEAS, který se však pochopitelně nepromítl do celkového hodnocení.

4.5 Závěrečná komparace hodnocených VMS

Tab. 28. Závěrečná komparace hodnocených VMS

Kategorie	Axis Camera Station	Axxon Next	Milestone XProtect	ATEAS Security
Monitoring a záznam	65 %	60 %	96 %	54 %
Komunikace a podpora zařízení	45 %	70 %	85 %	75 %
Management a konfigurace událostí	48 %	86 %	46 %	68 %
Administrace uživatelských práv	40 %	60 %	100 %	60 %
Správa uložiště	60 %	80 %	80 %	60 %
Uživatelské rozhraní	82 %	42 %	72 %	66 %
Hardwarová náročnost	20 %	80 %	80 %	60 %
Finanční náročnost	60 %	80 %	20 %	100 %
Celkové hodnocení	**53 %**	**70 %**	**72 %**	**68 %**

S přihlédnutím na uvedenou tabulku můžeme konstatovat, že celkové hodnocení vybraných systémů pro správu videa je přibližně podobné. Jedinou odchylkou je tak VMS Axis Camera Station, který v současné době ještě nemůže zcela konkurovat ostatním hodnoceným softwarům. Nicméně je nutné si uvědomit fakt, že společnost Axis je více zaměřená na distribuci kamer a ostatních prvků IP VSS. Zmíněný VMS je tak spíše dodatečným produktem, a proto

nejspíše nedosahuje takových kvalit, jako konkurenční produkty. Oproti tomu jsou společnosti AxxonSoft, Milestone i ATEAS specializovány především na vývoj softwarových řešení. Navíc vzhledem k rychlému rozvoji kamerových technologií a s nimi spojených skutečností lze předpokládat, že v průběhu několika let se situace na trhu může razantně změnit.

Mimo testovaných VMS je dnes na trhu dostupná celá řada produktů, jenž jsou neustále vyvíjeny a inovovány, aby dokázaly udržet krok s aktuálními trendy VSS a požadavky zákazníků. Volbě vhodného VMS by tak mělo předcházet důkladné zhodnocení produktu v co možná největším spektru nabízených funkcí, aby výsledná aplikace byla co nejvíce efektivní. Koncový zákazník by si měl před pořízením VMS položit několik zásadních otázek, jako např.: Kolik kamer se nachází v systému? Jaká je technologie kamer? Bude VMS kamery podporovat? Je zapotřebí centralizovaný nebo decentralizovaný systém? Jaký bude počet zobrazovacích stanic? Místní nebo vzdálená instalace? A mnoho dalších. V návaznosti na tyto otázky také musí počítat s jistou finanční i hardwarovou náročností, která může v případě rozsáhlých instalací VSS dosahovat výrazných hodnot. Na druhou stranu pokud na VMS nejsou kladeny vysoké požadavky a jedná se pouze o menší aplikace v řádu několika kamer, zcela postačí využití levnějších nebo dokonce bezplatných variant těchto produktů.

5 NÁVRH LABORATORNÍCH ÚLOH

FAKULTA APLIKOVANÉ INFORMATIKY **Protokol ze cvičení k předmětu Kamerové systémy**	
Datum:	Jméno a příjmení:
Známka:	Laboratorní úloha V – Axis Camera Station

Materiály k nastudování:

- Technická příručka Axis
  Dostupná z: http://www.axis.com/gb/en/learning/web-articles/technical-guide-to-network-video
- Manuály a dokumentace Axis Camera Station
  Dostupné z: http://www.axis.com/cz/cs/products/axis-camera-station/support-and-documentation
- Video tutoriály Axis Camera Station
  Dostupné z: http://www.axis.com/cz/cs/products/axis-camera-station/tutorials
- Diplomová práce na téma Komparativní studie funkčních vlastností video management platforem

Zadání úlohy

Teoretická část

1. Definujte pojem systém pro správu videa (VMS) a pojednejte o jeho významu ve vztahu k oblasti dohledových videosystémů.
2. Popište rozdíly mezi centralizovaným a decentralizovaným řešením VMS a uveďte jejich konkrétní platformy.
3. Stručně objasněte princip komunikace mezi kamerami a VMS
4. Pojednejte o problematice licenční politiky VMS.

Praktická část

1. Přidělené kamery nejprve uveďte do továrního nastavení. Tento úkon lze provést dvěma způsoby:

   a) Pomocí resetovacího tlačítka přímo na kameře. Kameru odpojte od napájení, stiskněte a držte tlačítko. Nyní opět připojte síťový kabel a tlačítko stále držte po dobu asi 15 sekund.

   b) Pomocí webového rozhraní kamery. Do webového prohlížeče napište IP adresu kamery a přihlaste se. Vstupte do sekce Setup -> System Options -> Maintenance a resetujte kameru. IP adresu kamery zjistíte pomocí programu IP utility.
2. Spusťte program Axis Camera Station a seznamte se s jeho prostředím.
3. Přidejte určené kameru do systému pomocí automatického vyhledávání nebo manuálně pomocí IP adresy a nastavte nové heslo. V dalším okně zvolte možnost „I want to configure this later“ a přiřaďte záznamovou oblast.
4. Vstupte do sekce Live View. Zde prozkoumejte možnosti softwaru, vytvořte nové pohledy a přizpůsobte dohledovou plochu dle vlastního uvážení. Finální pohled pomocí funkce Print Screen zobrazte v protokolu.
5. V sekci Video and Audio Settings upravte parametry profilů dle vlastního uvážení. Dále v sekci Event Configuration přiřaďte vytvořený profil manuálnímu nahrávání a přejděte do Live View. Zde spusťte pomocí „REC“ manuální nahrávání a vytvořte záznam o délce 1 minuty. Poté proveďte změnu profilu manuálního nahrávání a opět vytvořte záznam o stejné délce. V sekci Recordings poté záznamy exportujte a v protokolu uveďte komparaci výsledné kvality a velikosti souborů.
6. V sekci Event Configuration vytvořte novou událost na základě detekce pohybu. Prozkoumejte možnosti reakce softwaru a událost otestujte.
7. Seznamte se s funkcemi a ovládáním PTZ kamer. Pomocí sekce PTZ vytvořte nové presety a spárujte je s libovolnou událostí pomocí Event Configuration. Vytvořené pravidla otestuje.
8. Seznamte se s možnostmi softwaru v sekci User Permissions. Vytvořte nového uživatele, přiřaďte mu práva dle vlastního uvážení a prověřte jejich funkčnost.
9. Prozkoumejte možnosti sekce systémových logů. Vybranou část logů poté exportujte a vložte do protokolu.
10. Poreferujte o své zkušenosti s Axis Camera Station a popište jeho silné a slabé stránky.

FAKULTA APLIKOVANÉ INFORMATIKY **Protokol ze cvičení k předmětu Kamerové systémy**	
Datum:	Jméno a příjmení:
Známka:	Laboratorní úloha VI – ATEAS Security

Materiály k nastudování:

- Manuál ATEAS Security
  Součástí programu ATEAS Observer -> sekce Nápověda -> Nápověda offline
- Webové stránky ATEAS
  Dostupné na http://www.ateas.net/
- Diplomová práce na téma Komparativní studie funkčních vlastností video management platforem

Zadání úlohy

Teoretická část

1. Definujte pojem událost ve vztahu k systémům pro správu videa (VMS) a pojednejte o jejím významu.
2. Objasněte pojem metadata a vysvětlete jejich účel v procesu vyhledávání a třídění záznamu.
3. Vyjmenujte alespoň 10 konkrétních zdrojů událostí a stručně popište jejich princip.
4. Uveďte, na základě jakých kritérií by měl dle Vašeho názoru koncový zákazník vybírat konkrétní VMS produkt.

Praktická část

1. Přidělené kamery nejprve uveďte do továrního nastavení. Tento úkon lze provést dvěma způsoby:

   a) Pomocí resetovacího tlačítka přímo na kameře. Kameru odpojte od napájení, stiskněte a držte tlačítko. Nyní opět připojte síťový kabel a tlačítko stále držte po dobu asi 15 sekund.

   b) Pomocí webového rozhraní kamery. Do webového prohlížeče napište IP adresu kamery a přihlaste se. Vstupte do sekce Setup -> System Options -> Maintenance a resetujte kameru. IP adresu kamery zjistíte pomocí programu IP utility.
2. Spusťte program ATEAS Observer a seznamte se s jeho prostředím.
3. Vstupte do sekce Administrace a přidejte do systému určené kamery. Nastavení nového jména a hesla je nutné provést prostřednictvím webového rozhraní kamery.
4. Vstupte do sekce Mé pohledy. Zde prozkoumejte možnosti softwaru, vytvořte nové pohledy a přizpůsobte dohledovou plochu dle vlastního uvážení. Vyzkoušejte také funkce interaktivních map pomocí zadaného půdorysu. Finální pohled pomocí funkce Print Screen zobrazte v protokolu.
5. Pomocí administrace záznamu vytvořte novou záznamovou oblast a prozkoumejte možnosti pravidel záznamu a zálohování.
6. V sekci administrace kamer nastavte na vybrané kameře novou událost na základě detekce pohybu a prozkoumejte možnosti reakce softwaru. Parametry detekce pohybu se dále upravují v administraci kamer -> pohyb.
7. Seznamte se s funkcemi a ovládáním PTZ kamer. V dohledovém okně vytvořte nové presety a vyzkoušejte funkce autotracking a patrolling.
8. V sekci administrace uživatelů vytvořte nového uživatele a přidělte mu práva. Poté pomocí administrace pohledů vytvořte sdílené pohledy a vyzkoušejte je pod nově vytvořeným uživatelem.
9. Vyzkoušejte funkci manažera stahování v sekci záznamu a inteligentní vyhledávání Smart Search. Generujte poplach na základě vytvořené události a deník poplachů exportujte.
10. Poreferujte o své zkušenosti s ATEAS Security a popište jeho silné a slabé stránky.

ZÁVĚR

Účelem diplomové práce bylo seznámit potencionálního čtenáře s problematikou video management systémů a provést komparaci několika vybraných softwarů na základě navrženého evaluačního systému. Nejprve však bylo nutné objasnit jejich význam ve vztahu k hierarchicky nadřazené oblasti dohledových videosystémů, čemuž se věnuje především první kapitola teoretické části. Zde je uvedena charakteristika a pohled aktuálních norem na VMS, dále pak jednotlivé funkční celky, strukturu a také platformy těchto softwarových aplikací.

V navazující kapitole jsou poté rozebrány základní procesy, jež jsou realizovány právě prostřednictvím VMS, a na základě kterých je i také následně vytvořen zmíněný hodnotící systém. Pozornost je věnována především komunikaci, jež je chápána jako stěžejní proces probíhající mezi VMS a ostatními prvky VSS. Díky tomuto rozboru bylo zjištěno, že dnešním koncovým uživatelům je velice nápomocen globální standard ONVIF, jenž se velkou měrou zasluhuje o zkvalitnění interoperability mezi prvky síťového videa. Další částí této kapitoly se pak věnují spíše konkrétněji zaměřeným oblastem, jako jsou např. management událostí v prostředí VMS nebo administrace uživatelských práv.

Praktická část se v první kapitole zaobírá tvorbou komplexního evaluačního systému, kterého je posléze využíváno v rámci hodnocení jednotlivých VMS. Úkolem bylo navrhnout takové metody hodnocení, jež budou schopny pokrýt co možná nejširší rámec funkčních vlastností, ale zároveň budou aplikovatelné na předmětné VMS. Kompozice evaluačních kritérií je průsečíkem poznatků relevantní odborné literatury a názorů odborné veřejnosti řešené problematiky.

Následující kapitoly jsou poté věnovány aplikaci navrženého hodnotícího systému na VMS Axis Camera Station, Axxon Next, Milestone XProtect a ATEAS Security. Tyto softwary byly po dobu několika měsíců testovány na rozličných platformách za stejných laboratorních podmínek, které byly simulovány prostřednictvím virtualizačního nástroje. Závěrečná kapitola práce je vyhrazena tvorbě laboratorních úloh pro podporu výuky předmětu Kamerové systémy, jež bude v blízké době vyučován na Fakultě aplikované informatiky Univerzity Tomáše Bati.

Zadané téma diplomové práce se z počátku jevilo jako velmi komplexní. Byla tedy zvolena metoda dekompozice problému na dílčí částí, což vyústilo ve zdárné naplnění jednotlivých cílů zadání a dosažení přínosu požadovaného vedoucím práce.

SEZNAM POUŽITÉ LITERATURY

[1] ČSN EN 62676-1-1. Dohledové videosystémy pro použití v bezpečnostních aplikacích. Část 1-1: Systémové požadavky - Obecně. Praha: ÚNMZ, 2014.

[2] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012, 386 s. ISBN 978-80-87500-19-4

[3] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.

[4] Základní rozdělení kamerových systémů. In: *ELNIKA plus, s.r.o.* [online]. Praha, 2016 [cit. 2016-04-30]. Dostupné z: http://www.elnika.cz/elnika.php?link=cz/kucharka/rozdeleni-kamerovych-systemu

[5] Srovnání CCTV technologií. In: *NejKam.cz* [online]. Benešov, 2015 [cit. 2016-04-30]. Dostupné z: https://www.nejkam.cz/srovnani-cctv-technologii/

[6] CAPUTO, Tony C. Digital video surveillance and security. Boston: Butterworth-Heinemann/Elsevier, 2010, xvii, 333 p. ISBN 18-561-7747-5.

[7] Technical guide to network video. *Axis Communications* [online]. Lund, 2016 [cit. 2016-04-30]. Dostupné z: http://www.axis.com/gb/en/learning/web-articles/technical-guide-to-network-video

[8] What is a Video Wall? In: *Pixell* [online]. Lafayette, 2015 [cit. 2016-04-30]. Dostupné z: http://www.pixell.com/what_is_a_vw.htm

[9] MXInstaller. MOBOTIX: The 10 Things Beginners Should Know. In: Youtube [online]. Zveřejněno 24. 03. 2015 [cit. 2016-04-30]. Dostupné z: https://www.youtube.com/watch?v=8v5PBZW7us0

[10] IP Surveillance Starter Guide. In: *Auckland Security Cameras* [online]. Auckland, 2013 [cit. 2016-04-30]. Dostupné z: http://www.aucklandsecuritycameras.com/support-files/2013_ip_video_surveillance_guide_version_1_2.pdf

[11] Standardizace protokolů a videoanalýza. In: *STASANET: bezpečnostní technologie* [online]. Praha: Stasa s.r.o., 2012 [cit. 2016-04-30]. Dostupné z: http://www.stasanet.cz/Standardizace-protokolu-a-videoanalyza/

[12] *Onvif: The IP-based Security Standard* [online]. San Ramon: Onvif, 2016 [cit. 2016-04-30]. Dostupné z: http://www.onvif.org/

[13] *Physical Security Interoperability Alliance* [online]. Santa Clara: Santa Clara Consulting Group, 2015 [cit. 2016-04-30]. Dostupné z: http://psialliance.org/index.html

[14] Model protokolu TCP/IP. In: *Microsoft TechNET* [online]. Redmond: Microsoft, 2016 [cit. 2016-04-30]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc786900(v=ws.10).aspx

[15] ČSN EN 62676-2-1: Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 2-1: Video přenosové protokoly – Obecné požadavky. Praha: ÚNMZ, 2014.

[16] Web Services. In: *Ustav výpočetní techniky: Masarykova univerzita* [online]. Brno, 2006 [cit. 2016-04-30]. Dostupné z: http://dior.ics.muni.cz/~makub/soap/Martin-Kuba_WebServices_Datakon2006_clanek.pdf

[17] ČSN EN 62676-2-3: Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 2-3: Video přenosové protokoly - Implementace vzájemné spolupráce IP systémů založeněna síťových (web) službách. Praha: ÚNMZ, 2014.

[18] PAŽOUREK, Tomáš. *Webové služby v architektuře REST na platformě .NET*. Brno, 2012. Bakalářská práce. Masarykova univerzita.

[19] BERÁNEK, Petr. *Digitální video v praxi*. 1. vyd. Brno: UNIS, 2001, 264 s. ISBN 80-860-9763-3.

[20] O společnosti Axis. *Axis Communications* [online]. Lund, 2013 [cit. 2016-04-30]. Dostupné z: http://www.axis.com/cz/cs/about-axis

[21] Support and Documentation. *Axis Communications* [online]. Lund (Sweden), 2016 [cit. 2016-04-30]. Dostupné z: http://www.axis.com/ca/en/products/axis-camera-station/support-and-documentation

[22] What is Axxon? *AxxonSoft* [online]. Moskva, 2016 [cit. 2016-04-30]. Dostupné z: http://www.axxonsoft.com/company/

[23] ITV | AxxonSoft. Interactive 3D Map. In: Youtube [online]. Zveřejněno 24. 07. 2012 [cit. 2016-04-30]. Dostupné z https://www.youtube.com/watch?v=f6A2zPVum1A

[24] Recommended hardware platforms for Server and Client. *Axxon Soft* [online]. Moskva, 2016 [cit. 2016-04-30]. Dostupné z: https://doc.axxonsoft.com/confluence/display/next40en/Recommended+hardware+platforms+for+Server+and+Client

[25] Our company. *Milestone Systems* [online]. Kodaň, 2016 [cit. 2016-04-30]. Dostupné z: https://www.milestonesys.com/company/our-company/

[26] Manuals and guides. *Milestone Systems* [online]. Kodaň, 2016 [cit. 2016-04-30]. Dostupné z: https://www.milestonesys.com/support/manuals-and-guides/

[27] Společnost ATEAS CZ s.r.o. *ATEAS Security* [online]. Praha, 2016 [cit. 2016-04-30]. Dostupné z: http://ateas.net/?content=company

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Axis Camera Station
AES	Advanced Encrypting Standard
AHD	Analog High Definition
ARP	Adress Resolution Protocol
BNC	Bayonet Neill-Concelman
CCTV	Closed Circuit Television
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DVR	Digital Video Recorder
EPS	Elektrická požární signalizace
Gb	Gigabit
GB	Gigabyte
GHz	Gigahertz
GPS	Global Positioning System
GPU	Graphic Processing Unit
HD	High Definition
HD-CVI I	High Definition Composite Video Interface
HDD	Hard Disk Drive
HDMI	High Definition Multimedia Interface
HD-SDI I	High Definition Serial Digital Interface
HD-TVI I	High Definition Transport Video Interface
HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol

HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
I/O	Input/Output
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MHz	Megahertz
NAS	Network Attached Storage
NVR	Network Video Recorder
ONVIF	Open Network Video Interface Forum
OS	Operační systém
PC	Personal Computer
PoE	Power over Ethernet
PSIA	The Physical Security Interoperability Alliance
PTZ	Pan-Tilt-Zoom
PZTS	Poplachové zabezpečovací a tísňové systémy
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol
REST	Representational State Transfer
RPM	Revolutions per Minute
RTP	Real-time Transport Protocol

RTSP	Real-time Streaming Protocol
SD	Secure Digital
SDHC	Secure Digital High Capacity
SDK	Software Development Kit
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Service Pack
SPZ	Státní poznávací značka
SW	Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTB	Univerzita Tomáše Bati
UTP	Unshielded Twisted Pair
VGA	Video Graphics Array
VMS	Video Management System
VSS	Video Surveillance System
WSDL	Web Services Description Language
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK