Monitorovací programy v bezpečnostních systémech

Monitoring programs in security systems

Václav Urbančík

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

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

Jméno a příjmení:	**Václav URBANČÍK**
Osobní číslo:	**A08696**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Monitorovací programy v zabezpečovacích systémech**

Zásady pro vypracování:

1. **Pojednejte o národní legislativní úpravě v oblasti shromažďování, uchování a archivace informací.**
2. **Popište požadavky na monitorovací softwarové produkty.**
3. **Analyzujte možnosti současných softwarových produktů v poplachových zabezpečovacích systémech.**
4. **Navrhněte varianty možného využití SW produktů v jednotlivých typech zabezpečovacích systémů.**
5. **Pojednejte o vývojových trendech v oblasti nasazení SW produktů v zabezpečovacích systémech.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KŘEČEK Stanislav. Příručka zabezpečovací techniky. 3. vyd. Praha: Critetus, 2006. 315 s. ISBN 80-902938-2-4.**
2. **UHLÁŘ, J. Technická ochrana objektů II. [učební text]. 1. vyd. Praha: Policejní akademie České republiky, 2005. 230 s. ISBN 80-7251-189-0.**
3. **Software pro ústředny EZS [online]. Brno: ADI Global Distribution, 2011 [citováno 2011-01-24]. Dostupné z URL [http://www.adiglobal.cz].**
4. **Integrace systémů budov- Var net Integral [online]. Třebíč: VARIANT Plus, 2011 [citováno 2011-01-24]. Dostupné z URL [http://www.variant.cz].**
5. **101/2000 Sb. Zákon ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů**
6. **499/2004 Sb. Zákon ze dne 30. června 2004 o archivnictví a spisové službě a o změně některých zákonů**

Vedoucí bakalářské práce: **Ing. Jan Valouch, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Tato práce se zabývá nasazením monitorovacích programů v poplachových zabezpečovacích systémech. Nejdříve je posouzena legislativní úprava používání monitorovacích softwarů ve vztahu ke shromažďování a archivaci získaných dat. Následuje představení základních typů monitorovacích softwarů, jejich analýza a komparace z hlediska jejich funkcí a možnosti využití v praxi. Stěžejní část práce představuje návrh možnosti vhodného nasazení monitorovacích programů jako softwarové nástavby ve vybraných typech poplachových zabezpečovacích systémů.

Klíčová slova: poplachové bezpečnostní a tísňové systémy, pult centralizované ochrany objektů, CCTV

ABSTRACT

This work deals with the deployment of monitoring programs in security alarm systems. At first, the legislature of the use of monitoring software in relation to collection and archiving of data is examined. Then an introduction of basic types of monitoring software, their analysis and comparison in terms of their functions and possibilities of practical use follow. The main part of the work is a proposal for possible deployment of appropriate monitoring programs as software extensions in certain types of security alarm systems.

Keywords: alarm security and emergency systems, alarm receiving centre, CCTV

Rád bych poděkoval mému vedoucímu bakalářské práce panu Ing. Janu Valouchovi, Ph.D. za pomoc a podporu při zpracování této bakalářské práce. Zároveň chci poděkovat své rodině a blízkým za jejich podporu po celou dobu mého studia.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně ……
podpis diplomanta

OBSAH

ÚVOD

Přesné vymezení pojmu „**bezpečnostní systém**“ je relativně problematické, i když při vyslovení tohoto pojmu si každý intuitivně představí, o co se jedná. Kdybychom vycházeli z definice pojmu „**ochrana**“ z našeho zabezpečovacího hlediska, tak by výklad tohoto pojmu zněl: Ochrana znamená stabilní, relativně předvídatelné prostředí, ve kterém může jedinec nebo skupina sledovat své cíle bez rušení a ohrožení, bez strachu z vměšování nebo násilí.[1] Takže takovýto bezpečnostní systém můžeme vnímat jako prostředek k dosažení tohoto stavu.

Vzhledem k dynamicky se rozvíjejícímu odvětví bezpečnosti v komerčním průmyslu a s tím spojenému využívání jednoúčelových i integrovaných poplachových zabezpečovacích systémů, je nutné se věnovat i otázce monitorování a řízení těchto systémů a to z hlediska uživatelského komfortu, servisních možností, integrace s nepoplachovými aplikacemi, ale zejména z důvodu zvýšení kvality zabezpečení a rychlosti zásahu obsluhy při vzniku mimořádných situací. Stále populárnější poplachové zabezpečovací systémy jsou pořizovány jak drobnými uživateli, tak velkými subjekty, a to od různých výrobců, kterých na trhu stále přibývá.

Poplachové zabezpečovací systémy jsou řízeny a programovány uživatelskými softwary – programy, na které je s narůstající potřebou rychle a bezpečně zpracovávat narůstající množství přijímaných informací na pulty centrálních ochran, vyvíjen tlak k rozvoji těchto uživatelských programů. Jednoznačným úkolem těchto uživatelských programů je jasně a přehledně zobrazovat přijaté zprávy tak, aby byl operátor schopen co nejrychleji reagovat na vzniklou událost a byl schopen co nejdříve přijmout příslušná bezpečnostní opatření.

Důležitým aspektem v této oblasti je i volba vhodného nadstavbového softwaru vzhledem k použitému poplachovému systému a to zejména z hlediska jeho rozsahu, místa použití, účelu, přenosu poplachových a poruchových informací nebo možností integrace.

Monitorovací softwary slouží právě k uspokojování potřeb např. bezpečnostních agentur při vzdáleném monitoringu stavu chráněných objektů. Mezi jejich přednosti by měla patřit komplexnost poskytovaných informací, maximální kapacita sledovaných míst, automatizace předávání informací, bezpečnost chodu systému spočívající například ve spolehlivosti systému a jeho možnosti provádět různá nastavení vzdáleně, skupinová práce a v neposlední řadě nezávislost na dodavatelích jednotlivých zařízení poplachových systémů. [2]

Tato práce bude mimo jiné právě zjišťovat a analyzovat jednotlivé možnosti vybraných základních softwarů. Bude je vyhodnocovat, vzájemně porovnávat a jednotlivé programy doporučovat pro možné instalace např. v rodinném domu či rozsáhlém objektu.

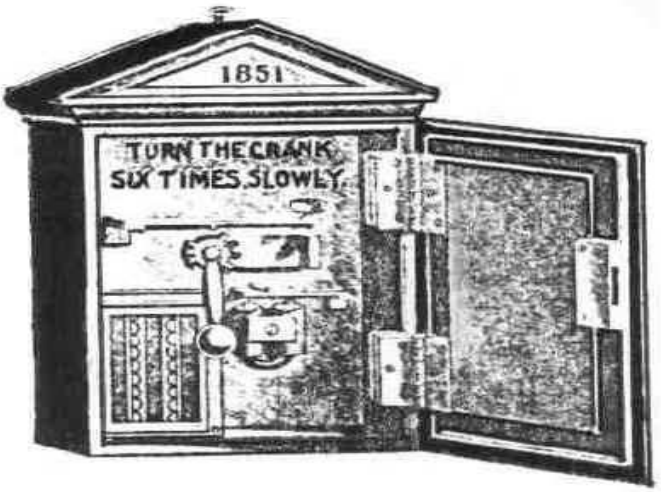
I. TEORETICKÁ ČÁST

1 HISTORIE

Monitorovací programy se vyvíjely a nadále vyvíjí souběžně s vývojem poplachových zabezpečovacích systémů. Potřeba ochrany před nebezpečím a s tím spojená potřeba signalizovat nebezpečí, když je bezpečnost ohrožena, provází lidstvo od věků, ale samotná historie uživatelských programů v poplachových zabezpečovacích systémech, tak jak je vnímáme dnes, není zase až tak dávná.Řekl bych, že je velmi mladá.

Samotnému zavedení monitorovacích programů předcházel vynález a vývoj poplachových zabezpečovacích systémů a zařízení. Zásadním krokem, který vedl k přenosu informací na dálku, byl vynález telegrafu v roce 1835. Jako první byl v praxi použit telegraf v roce 1844, kdy byla vytvořena telegrafní linka mezi Washingtonem a Baltimore. Pro signalizaci nebezpečí byl telegraf použit prvně hlavním inženýrem města New York panem Corneliusem Andersenem, kdy tento propojil požární hlásky telegrafem s centrálním stanovištěm. Toto centrální stanoviště bylo propojeno s jednotlivými požárními stanovišti. Tento způsob využití telegrafu nebývalým způsobem zkrátil dobu přenosu poplachového signálu od místa poplachu k nejbližší požární stanici.

Pokud bychom chápali zápis série teček a čárek primitivním zapisovačem na centrálním pultu, kdy tato činnost byla vyvolána zatažením za páku hlásiče, který roztočil vroubkované kolo a to prostřednictvím elektrického kontaktu vyslalo výše zmíněnou sérii teček a čárek, ve kterých byl obsažen individuální kód, můžeme vznik jakoby prvního uživatelského programu datovat do roku 1851. V tomto případě šlo o tzv. „volací skříňku“ (Obr. 1), která byla technickým vylepšením systému centralizace hlášení. Tento systém byl schválen v Bostonu v roce 1851 a již v roce 1854 bylo v tomto městě v provozu 42 těchto, jak bychom dnes řekli „**veřejných hlásičů**“.

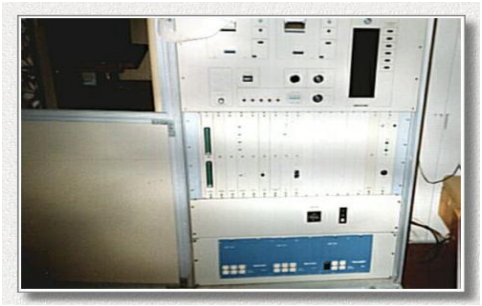


Obr. 1. Bostonský hlásič požáru z roku 1951 [3]

Teprve rozvoj elektroniky během a po druhé světové válce, zejména pak průmyslová výroba tranzistorů, následná miniaturizace elektronických zařízení a posléze rozvoj nových technologií vyvinutých pro potřeby kosmického průzkumu a v souvislosti s vietnamskou válkou, umožnily vznik nových druhů čidel, jejich elektronizaci a následnou komputerizaci, která vyvolala potřebu vývoje uživatelských programů. Právě výpočetní technika dosáhla v poslední době úrovně dovolující technickými prostředky nahrazovat některé činnosti, které dosud bylo možné zajišťovat výlučně lidskou silou, tedy vnímáním a myšlením.

V roce **1974** byl u Služby ochrany objektů VB v Příbrami zkušebně instalován první pult centralizované ochrany objektů (PCO). Nejprve byly napojeny čerpací stanice pohonných hmot (PHM), jeden peněžní ústav a sklady trhavin. Potom objekty obchodní sítě a objekty kulturního a památkového významu. Na základě vyhodnocení byl tento PCO rozšířen postupně do většiny krajských měst. Jednalo se o reléový linkový pult CENTR KM. Umožňoval napojení 120 objektů na teritoriu jedné telefonní ústředny. Během let přicházely do policejní výzbroje další PCO - RONA, TCP 60, **TRVZ** (Obr. 2 a Obr. 3) a GENOVA. V roce **1989** bylo na území Československa provozováno celkem 79 systémů centralizované ochrany se 7724 napojenými objekty. [4]

Obr. 2. PCO Tvrz dispečer [5]



Obr. 3. PCO Tvrz srdce [5]

Změna společenského a politického uspořádání po roce 1989 způsobila uvolnění podmínek pro rozvoj tohoto oboru i v České republice a od této doby dochází k masivnímu nárůstu potřeby poplachových zabezpečovacích systémů. Tento růst hlavně ovlivnily faktory jako rozvoj investiční výstavby, rozvoj bankovního sektoru, rozvoj pojišťovnictví, růst obecné kriminality a podobně. Objevují se poplachové zabezpečovací systémy jak tuzemských výrobců, tak systémy zahraniční výroby.

Obr. 4. První poplachový zabezpečovací systém firmy JABLOTRON

Tato situace na trhu s poplachovými systémy obecně zvyšuje konkurenci mezi výrobci, a ti se snaží nabízet zákazníkovi co nejlepší služby, mezi které mimo jiné patří právě dodání uživatelského programu. Tento tlak samozřejmě způsobuje, že se výrobci neustále snaží tyto programy zdokonalovat a přizpůsobovat podmínkám zákazníka.

2 LEGISLATIVNÍ RÁMEC MONITOROVACÍCH SOFTWARŮ V BEZPEČNOSTNÍCH SYSTÉMECH

Důležitým aspektem poplachových zabezpečovacích systémů je získávání citlivých dat a údajů. Tyto údaje a data jsou právě sledována a shromažďována pomocí monitorovacích softwarů na jednotlivá záznamová zařízení a dále uchovávaná. Ve velké míře jsou v těchto systémech shromažďovány převážně osobní údaje o fyzických osobách, ale rovněž o jejich pohybu a aktivitách ve střeženém prostoru a jeho okolí. Právě z důvodu vyvíjení se monitorovacích softwarů pro co nejsnažší a nejefektivnější provádění monitoringu např. bezpečnostní agenturou, dochází ke shromažďování a ukládání těchto dat. Na druhou stranu je tady právo na ochranu soukromí. V rámci poskytování služeb ochrany majetku a osob musí poskytovatel této služby např. bezpečnostní agentury splňovat povinnosti zakotvené v právních předpisech.

Následující podkapitoly obsahují výběr ustanovení právních předpisů, které řeší výše uvedenou oblast:

- Usnesení předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky č. 2/1993 Sb., listina základních práv a svobod ve znění ústavního zákona č. 162/1998 Sb.,
- Zákon č. 101/2000 Sb., o ochraně osobních údajů,
- Zákon č. 40/1964 Sb., občanský zákoník,
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím,
- institut mlčenlivosti.

2.1 Ústavní zákon č. 2/1993 Sb., listina základních práv a svobod ve znění ústavního zákona č. 162/1998 Sb.

- **ústavní zakotvení ochrany osobních údajů, právo na ochranu soukromí**

Předsednictví České národní rady dne 16. prosince 1992 vydalo Usnesení o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky (dále jen „LZPS“).

V této Listině základních práv a svobod jsou ukotvena mimo jiné práva na:

- *Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.*[1]
- *Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.* [2]
- *Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.* [3]

Obecně řečeno, tato vybraná ustanovení upravují princip ochrany lidské integrity. Nedotknutelnost směřuje proti zásahům ze strany veřejné moci i soukromých subjektů. Garantem nedotknutelnosti je stát.

2.2 Zákon č. 101/2000 Sb., o ochraně osobních údajů

Kromě potřeby starosti o fyzickou bezpečnost se objevuje fenomén ochrany osobních dat. Ochrana osobních údajů se stává jednou z personálních bezpečnostních požadavků.

V oblasti svobodného přístupu k informacím přijal parlament České republiky dne 4. dubna 2000 Zákon č. 101/1999 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Uvedený zákon **stanovuje právo** každého na **ochranu před neoprávněným zasahováním do soukromí.** Upravuje práva a povinnosti při zpracování osobních údajů. Ochrana osobních údajů je natolik citlivou otázkou, že uvedený zákon zřídil samostatný úřad pro ochranu osobních údajů. Tento zákon se mimo jiné vztahuje právě na fyzické i právnické osoby. Dle ustanovení zákona se citlivým údajem rozumí - *osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo*

[1] LZPS – Čl. 7 odst. 1

[2] LZPS – Čl. 10 odst. 2

[3] LZPS – Čl. 10 odst. 3

autentizaci subjektu údajů.[4] Obecně řečeno jde především o vysoce soukromé a intimní údaje, které by mohly být zneužity proti té osobě, které se týkají.

Jako příklad můžeme uvést rozsudek Městského soudu v Praze, který řešil žalobu cestovní kanceláře proti Úřadu pro ochranu osobních údajů, kdy ten uložil žalobci pokutu ve výši 400.000,- Kč mimo jiné za to, že v souvislosti se zpracováním osobních údajů svých klientů, jako správce osobních údajů shromažďoval osobní údaje v rozsahu, který byl nad rámec naplnění stanoveného účelu, uchovával osobní údaje, tj. rodné číslo a další údaje, i po ukončení doby, která byla nezbytná k účelu jejich zpracování. V tomto sporu Městský soud v Praze rozhodl ve prospěch žalovaného Úřadu pro ochranu osobních údajů a žalobu jako nedůvodnou zamítl.

Údaje uchovávané v záznamovém zařízení, ať obrazové či zvukové, jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní fyzickou osobu (tedy: informace z obrazových či zvukových nahrávek umožňují, byť nepřímo, identifikaci osoby). Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličej) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji uloženými v databázích je možná plná identifikace osoby. Osobní údaj pak ve svém souhrnu tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým, na snímku zachyceným, jednáním. [6]

Osobní údaje musí být uchovávány pouze po dobu nezbytně nutnou pro realizaci účelu shromažďování. Směrnice stanoví správci i povinnost informovat subjekt údajů o správci, zpracovaných údajích a účelu zpracování s ohledem na okolnosti zpracování. V případě sledovacích systémů to znamená hlavně informace o samotném sledování určitého prostoru, který by měl být jasně označen jako sledovaný, dále informace o provozovateli systému, možnosti přístupu k údajům. Výjimky z povinností správce jsou omezení nezbytná pro:

a) bezpečnost státu, obranu, veřejnou bezpečnost,
b) předcházení, odhalování a vyšetřování trestných činů nebo přestupků,
c) zajištění významného hospodářského či finančního zájmu státu či EU,
d) kontrolu výkonu veřejné moci,

[4] Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších přepisů - §4 písm. b)

e) ochranu práv a svobod subjektů údajů či jiných osob.

2.3 Zákon č. 40/1964 Sb., občanský zákoník

Mezi další právní předpis, který upravuje podmínky ochrany osobnosti, patří Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů, který svými ustanoveními definuje identifikaci fyzické osoby.

- *Fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy.* [5]
- *Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením.* [6]
- *Svolení není třeba, použijí-li se písemnosti osobní povahy, podobizny, obrazové snímky nebo obrazové a zvukové záznamy k účelům úředním na základě zákona.* [7]
- *Podobizny, obrazové snímky a obrazové a zvukové záznamy se mohou bez svolení fyzické osoby pořídit nebo použít přiměřeným způsobem též pro vědecké a umělecké účely a pro tiskové, filmové, rozhlasové a televizní zpravodajství. Ani takové použití však nesmí být v rozporu s oprávněnými zájmy fyzické osoby.* [8]

Podle výše citovaného ustanovení § 11 občanského zákoníku má fyzická osoba právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy. Především má však zde význam ustanovení § 12 odst. 1 občanského zákoníku, podle kterého písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením. Občanský zákoník pak v dalších odstavcích § 12 uděluje zákonné licence pro některé případy, ve kterých takového svolení není třeba – jde jednak o použití písemností osobní

[5] Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů - §11

[6] Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů - §12 odst. 1

[7] Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů - §12 odst. 2

[8] Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů - §12 odst. 3

povahy, podobizen, obrazových snímků nebo obrazových a zvukových záznamů k účelům úředním na základě zákona, dále pak se mohou podobizny, obrazové snímky a obrazové a zvukové záznamy pořídit nebo použít bez svolení fyzické osoby přiměřeným způsobem též pro vědecké a umělecké účely a pro tiskové, filmové, rozhlasové a televizní zpravodajství (avšak ani takové použití nesmí být v rozporu s oprávněnými zájmy fyzické osoby).

Pokud se podíváme na samotný souhlas záznamem dotčené osoby, tak ten nemusí být výslovný. Postačí, když je tento souhlas dovoditelný z okolností, za nichž se záznam uskutečňuje. O nevýslovný (konkludentní) souhlas se jedná tehdy, pokud je učiněn způsobem, který nevzbuzuje pochybnosti o tom, co chtěla dotčená osoba projevit.

Obrazový záznam – monitorování soukromých i veřejných prostor

Příkladem může být situace, kdy jsou televizními kamerami střežena veřejná prostranství. Při obecné známosti tohoto bezpečnostního opatření lze dovozovat, že fyzická osoba, která se na veřejném prostranství ocitne, souhlasí s pořízením svých obrazových snímků.

V případě monitorování soukromých prostor lze konkludentní souhlas dovozovat, je-li zřejmé, že dotčená osoba o monitorování věděla a zároveň s ním neprojevila nesouhlas. Jedná se například o situace, kdy prostory zabezpečené kamerovým systémem jsou označeny na viditelném místě jako monitorované, nebo kdy je osoba vstupující do těchto prostor na monitorování prokazatelně upozorněna, přičemž pořízení záznamu není touto osobou výslovně odmítnuto.

2.4 Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Zákon upravuje podmínky práva svobodného přístupu k informacím a stanoví základní podmínky jejich poskytování. Povinnost poskytovat informace vztahující se k jejich působnosti mají státní orgány, orgány územní samosprávy a veřejné instituce hospodařící s veřejnými prostředky. Žádat je může každá fyzická i právnická osoba. Zákon upravuje mj. náležitosti žádosti, způsob poskytování informací, omezení práva na informace, postup při podávání a vyřizování písemných žádostí, odvolání, hrazení nákladů.

Informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje povinný subjekt poskytne jen v souladu s právními předpisy, upravujícími jejich ochranu. [9]

Principem ochrany musí být, aby záznamy nedokumentující protiprávní jednání byly co nejrychleji smazány. Tento postup je z hlediska ochrany osobních údajů nejjistější a nejšetrnější vůči všem subjektům údajů. V případě záznamů ze sledovacích systémů totiž může být složité oddělit od sebe osobní údaje jednotlivých subjektů údajů. Jejich práva jako právo na přístup, právo na opravu či právo na vymazání údajů by pak spolu mohly vzájemně kolidovat. Realizace práva subjektu údajů na přístup pak může vést k určování dalších osob na záznamu zachycených s následkem získání jejich osobních údajů a tudíž k možnému neoprávněnému zásahu do jejich soukromí. Proto se jako vhodnější jeví právě co nejrychlejší zničení záznamu s osobními údaji všech zachycených subjektů. Zcela určitě je i v zájmu subjektů údajů, aby záznamy o jejich aktivitách byly likvidovány, než aby k nim sice měli přístup, ale byly uchovávány s často vysokými riziky zneužití. **V případě, že záznamy zachytí jednání porušující zákon, budou uchovány tak dlouho, jak budou potřeba k řádnému vyšetření zachycených protiprávních činů, při respektování práv zachycených osob.**

Princip omezeného předávání údajů - předávání osobních údajů shromážděných například policií by mělo být maximálně omezené a pouze v případě nutnosti za legitimním účelem stanoveným zákonem. Předané údaje by neměly být užity k jinému než vyžádanému účelu. Subjekt údajů má podle zákona právo na informace o zpracování osobních údajů, jeho rozsahu a účelu, kdo bude údaje zpracovávat a komu budou zpřístupněny a jak s nimi bude naloženo. Tyto informace musí subjekt údajů obdržet automaticky a nemusí o ně žádat. Požádat může navíc o konkrétní informace o zpracovávání svých osobních údajů a jejich využití pro činnost správce. Pokud má subjekt údajů podezření, že zpracování jeho osobních údajů je v rozporu se zákonem nebo neoprávněně zasahuje do jeho osobního a soukromého života, může požádat správce o vysvětlení, o odstranění vzniklého stavu a pokud mu není vyhověno, může se obrátit na Úřad pro ochranu osobních údajů. V případném soudním řízení má nárok na náhradu škody i jiné nemajetkové újmy vzniklé z neoprávněného nakládání s jeho osobními údaji.

[9]Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů - §8a

2.5 Institut mlčenlivosti

V českém právním řádu je zakotven Institut mlčenlivosti. Jde o zákonem nebo jiným předpisem stanovenou povinnost určené osoby chránit informace a skutečnosti, které jsou předmětem ochrany, a to tím způsobem, že o těchto informacích a skutečnostech zachová mlčenlivost.

V praxi se setkáváme s tím, že Institut mlčenlivosti je v konkrétních právních vztazích označován jako tajemství např. bankovní tajemství, lékařské tajemství apod. Ve skutečnosti jde ale o Institut mlčenlivosti, tedy o určitou konkrétní povinnost danou konkrétnímu objektu v souvislosti s výkonem jeho funkce nebo povolání. V případě institutu mlčenlivosti jsou předmětem ochrany zpravidla konkrétní informace a údaje o občanech, a proto i ochrana je zde koncipována zpravidla v zájmu jednotlivých občanů. Pro tento právní institut je velmi důležité definovat okruh osob, které mají povinnost zachovávat mlčenlivost, informace a skutečnosti tímto institutem chráněné, jakož i podmínky, za kterých se lze od povinnosti zachovávat mlčenlivost odchýlit.

Platná právní úprava České republiky (ČR) obsahuje řadu ustanovení, kterými je upravena mlčenlivost v různých právních vztazích. Jsou to především právní vztahy, ve kterých dochází k shromažďování a nakládání s daty a údaji občanů, zejména tedy právní vztahy v oblasti ochrany osobních údajů (§15 Zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů).

Zaměstnancům nebo osobám přicházejícím do styku s osobními údaji zákon ukládá mimo rámec organizačního řádu správce nebo zpracovatele povinnost zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací. Nedostatkem je to, že zákonem uložená povinnost mlčenlivosti nemá stanoven časový úsek, po který je třeba mlčenlivost zachovávat. V případě, že zaměstnanec je podřízen přísnějšímu institutu mlčenlivosti, než jak je definována, řídí se mlčenlivost speciálním zákonem, v tomto případě například zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Povinnosti mlčenlivosti je osoba zbavena v případě, že je to nezbytné k splnění informační povinnosti například dle zákona č. 40/2009 Sb., trestní zákoník. K prolomení povinnosti mlčenlivosti

může dojít pouze v případech, stanovených zákonem (poté se jedná o informační povinnost).

Aplikace některých vybraných právních předpisů na kamerové systémy.

Kamerový systém – CCTV (z anglické zkratky „Closed Circuit Television“) – představuje uzavřený okruh s přesně definovaným počtem účastníků, určený k přenosu vizuální případně zvukové informace a dělíme jej na část snímací, část přenosovou, část zobrazovací, část ovládací a příslušenství na monitorovací straně. Problematiku systému CCTV a jeho jednotlivých částí řeší norma ČSN EN 50132. Občas se setkáváme s použitím termínu „ průmyslová televize “. V současnosti není tento termín již zcela přesný a to z toho důvodu, že se v dřívějších dobách opravdu jednalo o uzavřené televizní okruhy, ke kterým byl přístup obvykle pouze z jednoho dohledového pracoviště. V dnešní době se vývoj ubírá trochu jiným směrem. Od pomaloběžných videorekordérů (TIME LAPSE) nahrávajících na kazety VHS se ustupuje a přechází k digitálním videorekordérům (DVR), využívající pro záznam dat pevných disků (HDD) známých z výpočetní techniky, což má samozřejmě spoustu výhod. Provedením digitalizace obrazu můžeme přenášet digitalizovaný obraz prostřednictvím počítačových sítí a Internetu. Zde se již nejedná v pravém slova smyslu o zmíněné uzavřené televizní okruhy, ale o otevřenou platformu vzdáleného dohledu nad kamerovými systémy. Vzdálený přístup přes internet a po veřejné síti musí být samozřejmě z hlediska zabezpečení přiměřeně ošetřen.

Z původního CCTV zbývá tedy pouze fakt, že obrazový signál ze systému CCTV není určen pro veřejnost, ale pouze pro uživatele s oprávněným přístupem. Systémy CCTV slouží ke sledování živé scény snímané průmyslovými kamerami a k záznamu obrazu z těchto kamer. Systémů CCTV se využívá převážně k ochraně majetku a bezpečnosti osob. Prostřednictvím CCTV lze z jednoho stanoviště monitorovat rozsáhlé objekty. Prostřednictvím připojení systému CCTV k Internetu lze kontrolovat dění z jakéhokoli místa na světě, kde máte přístup k Internetu. Pokud obraz z kamer též nahráváme, je možné zpětně prohlížet nahraný záznam. A zde se dostáváme ke zmíněné aplikaci výše uvedených právních předpisů.

Zásady provozování kamerového systému z hlediska zákona o ochraně osobních údajů:

a) Provozování kamerového systému je považováno za zpracování osobních údajů, pokud je vedle kamerového sledování prováděn záznam pořizovaných záběrů, nebo jsou v záznamovém zařízení uchovávány informace a zároveň účelem pořizovaných záznamů, případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním. Samotné kamerové sledování fyzických osob není zpracováním osobních údajů podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších přepisů, protože postrádá úroveň podmínek pro zpracování údajů ve smyslu §4 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších přepisů. To však nevylučuje aplikaci jiných právních předpisů, zejména ustanovení občanského zákoníku upravujícího podmínky ochrany osobnosti.

b) Údaje uchovávané v záznamovém zařízení, ať obrazové či zvukové, jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní fyzickou osobu (tedy: informace z obrazových či zvukových nahrávek umožňují, byť nepřímo, identifikaci osoby). Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličej) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby. Osobní údaj pak ve svém souhrnu tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým na snímku zachyceným jednáním.

c) Zpracování osobních údajů provozováním kamerového systému je přípustné:

- v rámci plnění úkolů uložených zákonem (např. Policii České republiky); v těchto případech je třeba dbát ustanovení příslušného zákona,
- dále je toto možné na základě řádného souhlasu subjektu údajů; to však je prakticky realizovatelné ve velmi omezených případech, kdy je možné jednoznačně vymezit okruh osob nacházejících se v dosahu kamery,
- užití kamerového systému však je možné i bez souhlasu subjektu údajů s využitím ustanovení §5 odst. 2 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších přepisů.

d) Povinnosti správce při provozování kamerového systému vybaveného záznamovým zařízením:

- kamerové sledování nesmí nadměrně zasahovat do soukromí. Kamerový systém je možno použít zásadně v případě, kdy sledovaného účelu nelze účinně dosáhnout jinou cestou (např. majetek je možno chránit před odcizením uzamčením místnosti). Dále je vyloučeno užití kamerového systému v prostorách určených k ryze soukromým úkonům (toalety, sprchy). Je ovšem možné řešení, kdy subjekt údajů má na výběr z alternativ (např. lze monitorovat prostory šatny plaveckého stadionu za předpokladu, že je vymezen prostor pro převlékání, který není kamerami sledován),
- specifikace sledovaného účelu. Je třeba předem jednoznačně stanovit účel pořizování záznamů, který musí korespondovat s důležitými právem chráněnými zájmy správce (např. ochranou majetku před krádeží). Záznamy tak mohou být využity pouze v souvislosti se zjištěním události, která poškozuje tyto důležité, právem chráněné zájmy správce. Přípustnost využití záznamů pro jiný účel musí být omezena na významný veřejný zájem, např. boj proti pouliční kriminalitě,
- je třeba stanovit lhůtu pro uchovávání záznamů. Doba uchovávání dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému. Uchovávaná data by měla být uchovávána v rámci časové smyčky např. 24 hodin, pokud jde o trvale střežený objekt, nebo případně i dobu delší, v zásadě ne však přesahující několik dnů, nejde-li o pořizování záznamů policejním orgánem podle zvláštního zákona, a po uplynutí této doby vymazána. Pouze v případě existujícího bezpečnostního incidentu by měla být data zpřístupněna orgánům činným v trestním řízení, soudu nebo jinému oprávněnému subjektu,
- je třeba řádně zajistit ochranu snímacích zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy, před neoprávněným nebo nahodilým přístupem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním, viz §13 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších přepisů,
- subjekt údajů musí být o užití kamerového systému vhodným způsobem informován (např. nápisem umístěným v monitorované místnosti), viz §11 odst. 5 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších přepisů, nejde-li o uplatnění zvláštních práv a povinností vyplývajících ze zvláštního zákona,

- je třeba garantovat další práva subjektu údajů, zejména právo na přístup k zpracovávaným datům a právo na námitku proti jejich zpracování, viz §1 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších přepisů,
- zpracování osobních údajů je třeba registrovat u Úřadu pro ochranu osobních údajů, nejde-li o uplatnění zvláštního práva či povinností vyplývajících ze zvláštního zákona, viz §18 odst. 1 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších přepisů. [7]

Jednou ze základních povinností správce je v souladu s §5 odst. 1 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů stanovit účel, k němuž mají být osobní údaje zpracovávány. Kamerový systém je technický prostředek (způsob), kterým jsou osobní údaje zpracovávány, nikoli účel, jak se v mnoha případech správci mylně domnívají. Je tedy nutné, aby každý, kdo se rozhodne provozovat kamerový systém, jednoznačně stanovil účel (např. ochrana majetku), pro který hodlá osobní údaje z pořizovaných záznamů zpracovávat. V zásadě je kamerový systém možné použít pouze v případě, kdy sledovaného účelu nelze účinně dosáhnout jinou cestou.

Zároveň je nutné upozornit na skutečnost, že oznamovací povinnost se podle §16 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších přepisů, vztahuje pouze na správce. Ten je v §4 písm. j) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších přepisů, definován jako subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za ně. Na zpracovatele definovaného podle §4 písm. k) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších přepisů, který na základě smluvního vztahu uzavřeného se správcem pouze technicky zajišťuje instalaci, provoz, údržbu a opravy kamerového systému, se oznamovací povinnost nevztahuje.

Tak jako řada jiných vynálezů či technologií, jsou i kamerové systémy jak využitelné, tak zneužitelné. Je třeba hledat cesty k tomu, aby kamery a jiné sledovací systémy mohly být všeobecně vyžívány pro legitimní účely prevence kriminality, ochrany osob, majetku a jiného veřejného či soukromého zájmu, který převáží nad právem sledovaných osob na ochranu jejich soukromí, současně důsledným prosazením legislativních a technických opatření vyloučit nebo na minimum omezit možnosti jejich zneužití k indiskrétnímu sledování lidí.

Dílčí závěr

Předchozí kapitola popisuje, kterých zákonů a předpisů se problematika poplachových zabezpečovacích systémů a jejich monitorování dotýká. Můžeme konstatovat to, že například ve výše popsaném příkladu použití monitorovacího software ve spojení s provozem kamerového systému s možností záznamu je z hlediska dnešní legislativy velmi problematickou záležitostí. Tato činnost skrývá mnohá úskalí a může ovlivňovat samotný vývoj a použití monitorovacích softwarů.

3 MONITOROVACÍ SOFTWARE BEZPEČNOSTNÍCH SYSTÉMŮ

Obecný význam nadstavbové části poplachových zabezpečovacích systémů tzn. softwaru v poplachových zabezpečovacích systémech, spočívá hlavně ve zjednodušení komunikace mezi bezpečnostními prvky systému a např. majitelem střeženého objektu nebo pracovníky dohledového centra. Dále spočívá v získání názornějšího přehledu o situaci ve střeženém objektu, zejména v rozsáhlejších aplikacích, zkrácení doby reakce a následného zásahu na základě vyhodnocení vzniklé situace a tím zvýšení celkové bezpečnosti střeženého objektu.

3.1 Obecné vlastnosti

3.1.1 Význam

Monitorovací softwary mají velký význam v celkovém zvýšení úrovně zabezpečení střežených objektů. Tohoto zvýšení dosahují svou přehledností, možností znázorňování nepřeberného množství zobrazovaných informací v reálném čase například z míst, která jsou narušena a o možnosti ihned rozhodovat o následných krocích ať už zásahové skupiny nebo možnosti kontaktování policie.

Další z významných vlastností je možnost integrace technologií v poplachových zabezpečovacích systémech a tím nutnost přizpůsobení výrobců softwarů na potřeby této integrace. Integrace spočívá v tom, že v dnešní době zákazník požaduje vytvoření uceleného bezpečnostního systému, který obsahuje například poplachový systém PZS, protipožární signalizace EPS, přístupový systém ACS, docházkový systém, návštěvní systém, řízení výtahů, průmyslová televize CCTV, technické řízení budov, řízení parkoviště, vnější obvodová ochrana, prodejní automaty, řízení vytápění, řízení klimatizace, řízení osvětlení a další. Takový systém se většinou označuje pojmem Integrovaný bezpečnostní systém (Integrated Security Management Systems – ISMS), neboť svými komplexními funkcemi pokrývají všechny požadavky organizací na podnikovou bezpečnost nebo zákazníka na bezpečnost domácnosti.

3.1.2 Funkce

Vytváří vizuální prostředí mezi obsluhou a poplachovým zabezpečovacím systémem. Tyto programy by se daly chápat jako prostředník v komunikaci.

Mezi základní funkce patří například:

- zobrazování a ukládání poplachových zpráv (místo, čas, druh poplachu apod.)
- přehledné vedení sledovaných objektů v databázi
- tisk sestav pro zákazníky (např. historie činnosti obsluhy, historie hlášení poplachového zabezpečovacího systému)
- dálkové vytváření uživatelských oprávnění a přístupových práv
- dálkové online nastavování poplachových zón
- zobrazování poplachu na monitoru, na mapě, zvuková signalizace, posílání e-mailu
- ovládání pohybu kamery, zapnutí světel, spuštění nahrávání a další

3.1.3 Přínos

Obecně řečeno jedním z přínosů takovýchto monitorovacích programů v poplachových zabezpečovacích systémech je zvýšení komfortu pro ty, co s těmito monitorovacími systémy pracují. Tato komfortnost spočívá hlavně v přehlednosti pro obsluhující personál a jednoduchosti zobrazovaných informací. Dalším přínosem je nepochybně velký objem a rozsah poskytovaných informací o střeženém a sledovaném objektu či prostoru. Tím, že tyto monitorovací softwary jsou schopny zahrnout do svého sledování nepřeberné množství poplachových zabezpečovacích systémů instalovaných na velkém množství různých objektů, přispívají nemalou měrou ke zvýšení bezpečnosti ve společnosti.

3.2 Požadavky

Zde se dostáváme k některým základním požadavkům, které by monitorovací programy v poplachových zabezpečovacích systémech obecně měly splňovat.

3.2.1 Seznam monitorovaných míst v objektu (zařízení)

Monitorovací programy musí umět zobrazovat co největší počet monitorovacích zařízení obsažených v bezpečnostním systému jako je například stav požárních hlásičů, docházkový systém apod.

3.2.2 Seznam monitorovaných objektů

Mezi další obecné požadavky patří schopnost monitorovacího programu obsluhovat a zobrazovat i několik střežených objektů v reálném čase.

3.2.3 Historie událostí

V dnešní době již patří uchovávání dat, ať už se jedná například o data z docházkového systému nebo bezpečnostního systému, mezi běžné požadavky kladené na monitorovací software.

3.2.4 Kompatibilita

Na monitorovací programy jsou kladeny nároky, aby bylo možné tyto programy použít v co nejširším okruhu poplachových zabezpečovacích systémů od různých výrobců. Výrobci monitorovacích programů si uvědomují, že zákazník má právo výběru a bude chtít svůj systém propojit s komponenty různých dodavatelů, a proto je potřeba, aby software byl kompatibilní.

3.2.5 Jednoduchost

Monitorovací programy by měly uživateli těchto programů nabízet jednoduchost spočívající v obsluze a intuitivním ovládání daného softwaru, včetně co největší přehlednosti zobrazených údajů.

3.2.6 Technické normy

I když poplachové zabezpečovací systémy patří do kategorie výrobků, které by mohly ve zvýšené míře ohrozit zdraví nebo bezpečnost osob, majetek nebo životní prostředí, popřípadě jiný veřejný zájem, tak tato práce se zabývá využitím monitorovacích programů v bezpečnostních systémech, tzn. softwarovým zobrazením činnosti poplachového zabezpečovacího systému. Tuto problematiku samostatně žádná norma neřeší. Určité souvislosti bychom mohli najít v části normy **ČSN EN 50131-1 ed.2 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky** a v normě **ČSN CLC/TS 50398 - Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky**.

V části normy ČSN EN 50131-1 ed.2 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1: Systémové požadavky jsou mimo jiné řešeny systémové požadavky na poplachové zabezpečovací systémy. V části **funkčních požadavků** jsou řešeny takové požadavky jako například:

- detekce
- paměť událostí
- časové závislosti
- indikace

Právě tyto a další požadavky musí splňovat samotné zařízení poplachového zabezpečovacího systému (např. PZS, klávesnice s displejem), ale může je splňovat, respektive současně zobrazovat použitý monitorovací software.

Dílčí závěr

V předcházející kapitole jsme se zaměřili na to, co by měl monitorovací software použitý v poplachových zabezpečovacích systémech nabízet uživateli, který jej využívá ve svých službách. Shrnuli jsme jak význam těchto programů, tak požadavky na tyto softwary. Při výběru softwaru uživatelem jsou na vlastnosti jako jednoduchost obsluhy, seznam monitorovaných míst, paměť událostí apod. kladeny velké nároky. Mezi další takové požadavky patří možnost integrace více různých systémů ve střeženém objektu a jejich sledování.

II. PRAKTICKÁ ČÁST

4 PRAKTICKÁ ČÁST

Na světovém trhu je k dispozici několik softwarových nástrojů pro účely monitorování poplachových zabezpečovacích systémů. Tato část práce řeší problematiku monitorovacích softwarů, analyzuje vlastnosti vybraných základních typů monitorovacích softwarů používaných v poplachových zabezpečovacích systémech jejich vlastnosti.

4.1 Program TEGAL

Prvním programem, kterým se budeme zabývat je program **TEGAL od české dceřinné firmy Honeywell, spol. s r.o. - Security Products**. Tento jednoduchý program Je určen pro správce systému PZS, pracovníky ostrahy, bezpečnostní techniky a řídící pracovníky. Umožňuje sběr údajů z různých zabezpečovacích nebo požárních ústředen např. Ademco-Microtech (**Galaxy**), **DSC**, **Rokonet** (Orbit Pro), **Aplex**, **ESSER** a dalších. Při použití s ústřednami GALAXY umožňuje i export dat pro jednoduchou docházku. Nasbíraná data je možné jednoduše zálohovat v podobě textového či databázového souboru nebo je jednoduše vytisknout na tiskárně. Pomocí výkonných filtrů je možné provádět libovolnou analýzu dat – do samostatného okna jsou vloženy jen události uživatelem vybraného typu (např. všechny poplachy). V samostatném okně „Evidence přítomnosti“ je možné sledovat pohyb osob v objektu v závislosti na poslední použité čtečce či pouhou přítomnost / nepřítomnost osob. K programu TEGAL není možné současně připojit více technologií s výstupem RS-232[10]. Program TEGAL je možné provozovat i v síťovém režimu. Na jednom počítači jsou data sbírána do databáze (**PC SBĚRAČ**) a na ostatních počítačích v síti je možné data sledovat a provádět analýzu (**PC PROHLÍŽEČ**). [8]

4.1.1 Určení programu

Hlavní cíl a určení programu TEGAL je možné shrnout do těchto bodů:

1. **záznam událostí**

- program je určen k záznamu a monitorování událostí z ústředen PZS a EPS,
- připojení technologií přes port RS – 232,

[10] Výstup RS-232 - rozhraní pro přenos informací a pro komunikaci dvou zařízení

- možnost definování vlastní ústředny (obecného zařízení) jako zdroje dat,
- nastavitelná rychlost a parametry přenosu na sériovém portu,
- podpora hardwarového bufferu[11] pro sběr dat on-line přes softwarový protokol,
- podpora hardwarového bufferu pro sběr dat off-line tzn. Počítač je uživatelem vypínán, záloha při výpadku počítače (výpadek elektrického proudu),
- PC s připojenou technologií pracuje jako tzv. "sběrač",
- pomocí počítačové sítě LAN je možné prohlížet nasbíraná data programem TEGAL v režimu "prohlížeč".

2. analýza a reporty dat

- pro účely analýzy a vytváření zpráv existuje tzv. extrakt úplného provozního deníku,
- umožňuje vytvořit zprávu obsahující pouze vybrané události,
- extrakt provozního deníku se vytváří aplikací sady filtrů na úplný provozní deník,
- filtry extraktu jsou nezávislé na sadě filtrů pro úplný provozní deník,
- možnost definice pokročilých filtrů s využitím zástupných znaků či regulárních výrazů,
- třístupňová filtrace v extraktu,
- vyfiltrované události jsou v extraktu i v úplném provozním deníku barevně vyznačeny (pozadí/text),
- filtrace událostí mezi dvěma daty,
- zobrazení pouze událostí vyhovujících filtrům (volitelné),
- možnost definice víceřádkových filtrů,
- fulltextové vyhledávání řetězce v extraktu provozního deníku.

3. monitoring

- program lze využít pro jednoduché monitorování aktivit systému,

[11] Hardwarový buffer – externí zařízení umožňující ukládání dat

- při příchodu vyfiltrované události do úplného provozního deníku je možné vyvolat bitmapu a zvuk (soubor *.wav),
- filtrem lze spustit libovolný program se zadanými parametry,
- při příchodu vybraných událostí je možné odeslat e-mail nebo SMS zprávu na mobilní telefon (tato funkce však vyžaduje úzkou spolupráci všech pracovníků informačních technologií (IT) a závisí na bezpečnostních požadavcích v IT).

4. docházka

- vyhodnocování dat z ústředen PZS umožňuje sledování evidence přítomnosti osob či kompletní zpracování docházky,
- tři základní režimy pro monitorování přítomnosti a docházky,

a) sledování pohybu osob po objektu (zjištění, kterou čtečkou prošla osoba naposledy)
b) režim dvě čtečky (jednoduchá docházka s využitím příchodové a odchodové čtečky) + sledování pohybu osob po objektu
c) režim docházkový terminál (k ústředně je připojen docházkový terminál DT 2000, na kterém lze zadávat důvody příchodu a odchodu) + sledování pohybu osob po objektu,

- sledování přítomnosti osob v objektu (pouze pro bod b) a c)),
- z exportovaných docházkových dat je možné zpracovávat plnohodnotnou docházku zaměstnanců specializovaným programem POWERKEY,
- docházková data je možné exportovat ve formě textového souboru (*.TXT) do libovolného vlastního docházkového programu nebo ve formě speciálního šifrovaného souboru do programu POWERKEY,
- z on-line přijímaných událostí je možné provádět on–line export docházkových událostí,
- online export docházkových událostí + online evidence přítomnosti osob,
- možnost manuálního exportu docházkových dat - ruční zadání prvního a posledního dne,
- uživatelé karet jsou evidováni v tzv. tabulce kódů, její obsah je možné tisknout a zálohovat stejně jako všechny ostatní databáze, možnost exportu databáze ve formě TXT souboru,

- uvedené funkce jsou pouze u vybraných typů ústředen.

4.1.2 Další parametry a možnosti programu

Mezi další možnosti a parametry programu patří:

- prakticky neomezený počet ukládaných událostí,
- automatická záloha dat na začátku kalendářního měsíce,
- barevné zvýraznění definovaných událostí,
- možnost filtrace pouze vybraných událostí,
- tisk událostí on-line a na povel do souboru nebo na tiskárnu,
- dálkový přístup k databázi z více počítačů v síti LAN,
- zabezpečení programu pomocí databáze operátorů s různými přístupovými právy,
- záznam práce obsluhy s programem,
- široký rozsah nastavení komunikačních parametrů,
- 32 bitové řešení programu (Windows 95, 98 SE, 2000, NT, XP).

4.1.3 Instalace programu

Podmínky instalace programu:

Program TEGAL je určen k provozu v počítačové síti, a tím jeho instalace není zcela triviální. Uživatelé mohou mít různé typy počítačových sítí s různě uspořádanými prostředky a programu je třeba sdělit, jak má tyto prostředky využívat. Je rovněž třeba zajistit další hardwarové a softwarové předpoklady pro korektní funkci programu.

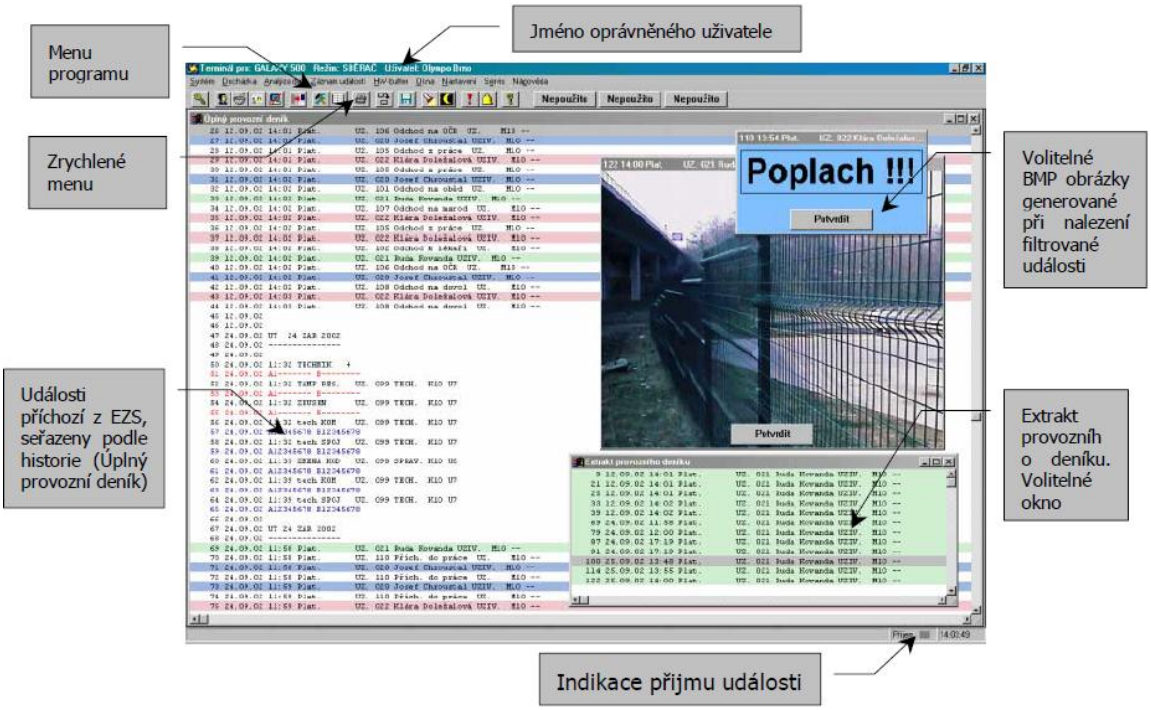
Během standardní instalace probíhající v prostředí Windows se nainstaluje vlastní program TEGAL, vytvoří se potřebná adresářová struktura, nainstaluje se databázová podpora BDE32, a ovladače HW klíče. Po dokončení instalace je nutné počítač restartovat. Před provedením restartu se musí dbát na to, aby byl v paralelním portu počítače zasunut hardwarový klíč. Po provedené instalaci je nutné naplánovat, jak bude program používán, zda v síti nebo samostatně, a kde budou uloženy jednotlivé druhy dat. Po provedené rozvaze je třeba všechny změny sdělit programu TEGAL a programu BDE. Pro úspěšné zahájení běhu programu je důležitá nejen korektně ukončená instalace programu, nastavení programu BDE administrátor, ale také určitá nastavení přímo v programu TEGAL (režim, sériový port a typ ústředny).

Ovládání programu

Program TEGAL je tvořen programovým menu pro vyvolání jednotlivých funkcí programu. Tlačítkem F10 se aktivuje menu a pomocí šipek již volíme požadovanou funkci. Stejně tak je možné vyvolat danou funkci pomocí kombinace kláves "Alt" a klávesy podle písmena vyznačeného na položce podtržítkem. Stejně jako menu slouží k vyvolání jednotlivých funkcí také panel tlačítek s nejpoužívanějšími funkcemi. Práce s programem je velmi jednoduchá, program je vybaven klasickým Windows rozhraním s roletovými menu a pro rychlý přístup k vybraným funkcím je k dispozici tlačítková lišta (Obr. 5) s bublinovou nápovědou, případně funkční klávesy F1 - F10.

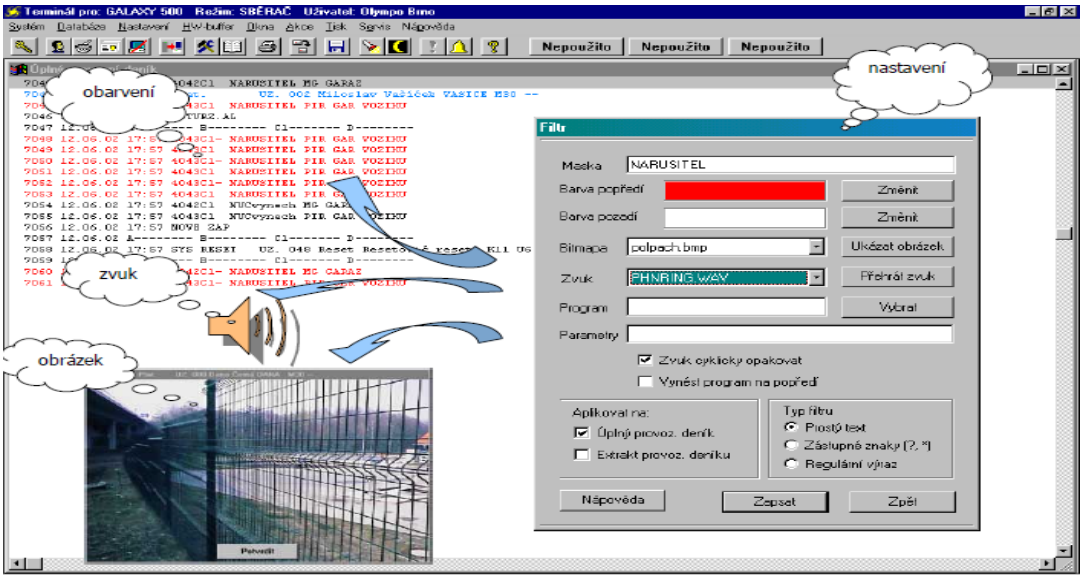
Obr. 5. Hlavní tlačítková lišta programu TEGAL 5.0 [9]

4.1.4 Vzhled programu



Obr. 6. Hlavní okno programu TEGAL 5.0 [9]

PŘÍKLAD – jednoduchý filtr prostého textu aplikovaný na úplný provozní deník



Obr. 7. Aplikace jednoduchého filtru prostého textu v úplném provozním deníku [9]

Pokud program TEGAL přijme událost (Obr. 7) obsahující slovo „NARUSITEL“, výše uvedený filtr tento příchozí řádek vyhodnotí a vykoná vyznačené úkony:

1. řádek obsahující slovo „NARUSITEL“ se v úplném provozním deníku obarví červeně,

2. z reproduktorů připojených k PC se rozezní zvukový soubor PHNRING.WAV a bude se nepřetržitě opakovat, dokud jej obsluha neumlčí. (volba zvuk - cyklicky opakovat),

3. na monitoru se zobrazí obrázek PLOT.BMP tj. např. místo napadení.

4.2 Program SIMS (Safety Informational Monitory Software)

Dalším z informačních a monitorovacích software pro potřebu subjektů zabývajících se ochranou majetku, střežením prostor i mobilní techniky prostřednictvím elektronických zabezpečovacích systémů, kterým se budeme v této části práce zabývat je program SIMS (Safety Informational Monitory Software). Základními vlastnostmi software je jeho spolehlivost, variabilita při připojování nejrůznějších pultů centralizovaných ochran, a v neposlední řadě nadstandardní uživatelský komfort. Nositelem autorských a licenčních práv je firma Vladimír Hrachovina SW SIMS. Program SIMS je napsán pro prostředí OS Windows. Jako databázový prostředek využívá SQL Server. Vyžaduje operační systém Windows 2000(server) a vyšší.

Disponuje ovladači na řadu bezpečnostních zařízení používaných v ČR (namátkou PCO řady SG DR, HaSaM, Jablotron, FBII, RHMS, FEI, Matilda, NAM, Radom, ORZO Security a další). Pro přenos zpráv je možné využívat telefonní, radiové, SMS, GPRS a IP komunikátory. Je schopen všechny PCO, pro které má výrobce vyvinuty ovladače připojovat současně do jednoho systému. Komunikace mezi počítačem a PCO jsou na úrovni služeb, nikoliv aplikace.

Program umožňuje:

- vést přehlednou databázi všech zpráv,
- vést přehlednou databázi objektů, datově nesrovnatelně bohatou, s popisem instalovaného bezpečnostního zařízení a jeho stavem,
- ke každému objektu připojit strukturovaně soubory nebo URL odkazy (mapy, plánky, fotografie, IP kamery a další),
- vytvářet zprávu o činnosti obsluhy (dobu reakce na poplachové hlášení, aktuální čas příjezdu zásahové skupiny a další) do připraveného formuláře (časy jednotlivých úkonů se zapisují automaticky),
- tisk sestav hlášení pro zákazníky (zprávy, akce, činnost hlídací agentury, popis narušených smyček),
- v automatickém nebo manuálním režimu lze odesílat výpisy,
- zablokovat příjem poplašných hlášení od zadaného objektu (v době např. servisních zásahů - tato funkce je u objektu indikována),
- maximální měrou usnadňuje práci operátorům (zprávy informativního charakteru ukládá do souboru zpráv automaticky na rozdíl od poplašných zpráv, u kterých vyžaduje obsluhu),
- odesílat a přijímat zprávy SMS. Odesílání zpráv může být provedeno jak manuálně, tak automaticky s vazbou na událost doručenou z PCO,
- nad záložkou **Objekty** a záložkou **Akce** zobrazovat obrazové i textové soubory, mapové podklady (i z veřejných zdrojů) a také záznamy IP kamer,
- střeženým zákazníkům umožňuje on line kontrolu adres objektů, kontaktních osob a zpráv ze zabezpečovacích ústředen jejich objektů.

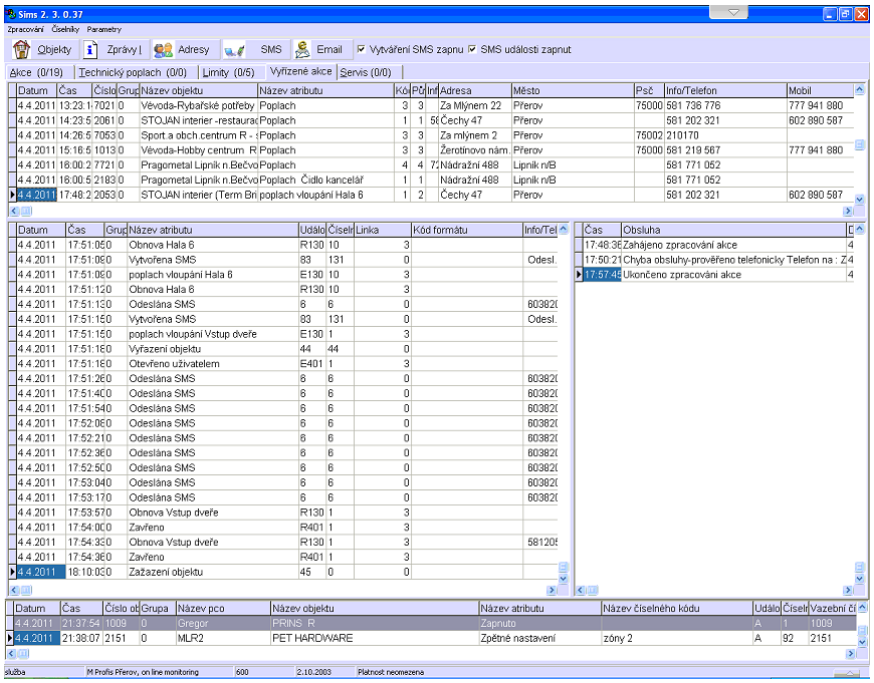
Program je předurčen pro provoz v sítích. Široce pojatá přístupová práva chrání data před možným zneužitím nebo neodborným zásahem.

Výrobce tohoto softwaru uvádí na trh i nadstavby k softwaru SIMS:

Fakturace - program umožňující fakturovat z dat programu SIMS

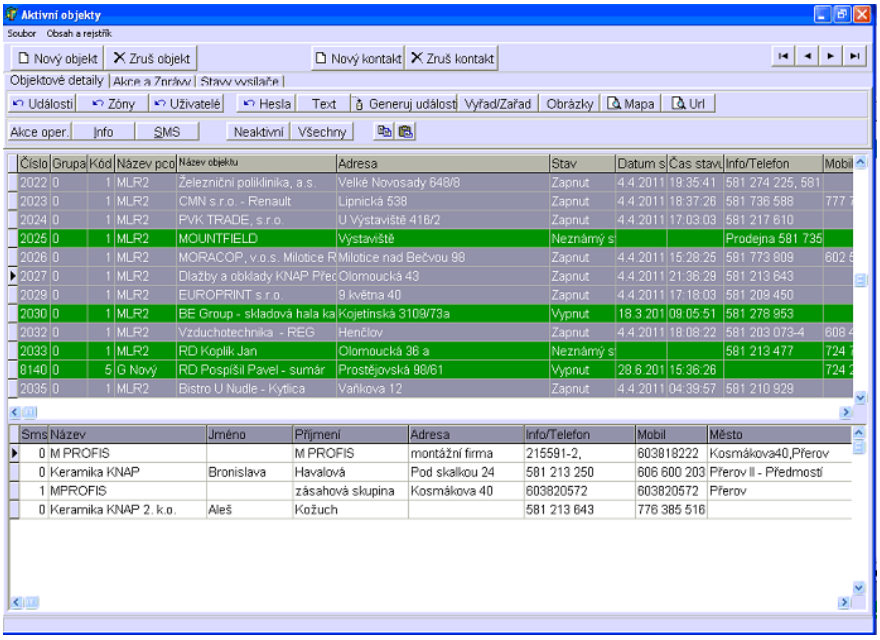
SIMSWEB - program umožňuje přístup k datům prostřednictvím Internetu. Poskytuje zabezpečený provoz a přístupová práva uživatelů umožňují diferencovat úroveň zobrazení dat.

4.2.1 Vzhled programu



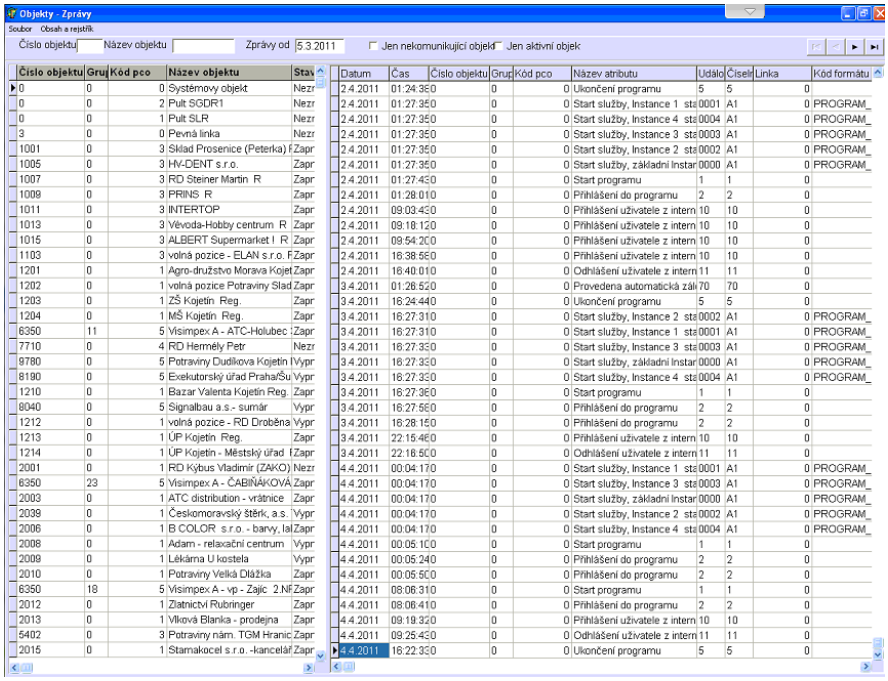
Obr. 8. Základní dialogové okno programu SIMS

V tomto dialogovém okně jsou pro obsluhu PCO znázorňovány veškeré akce, které se dějí ve střežených objektech. Přehled a rozmanitost zasílaných zpráv (hlášení stavů jako: OTEVŘENO, ZAVŘENO, ZASTŘEŽENO, TÍSEŇ apod.) závisí na použitém poplachovém bezpečnostním systému ve střeženém objektu tzn. v závislosti na použité PZS. Nejdůležitější oblast dialogového okna pro obsluhu PCO se nachází ve spodní části, kde v reálném čase přicházejí zprávy ze střežených objektů. Dále se zde nachází informační část monitorovacího software, ve které se zobrazuje narušení příslušných akcí (DOCHÁZKA, NEPOVOLENÉ OTEVŘENÍ apod.), definovaných uživatelem.



Obr. 9. Seznam objektů v programu SIMS

Na obrázku je znázorněno dialogové okno z programu SIMS, ve kterém je uveden seznam střežených objektů, u kterých jsou ve spodní části dialogového okna zadány kontaktní osoby a jejich údaje pro případ nutnosti kontaktovat tuto osobu v případě vyhlášení poplachu.



Obr. 10. Sumární výpis veškerých hlášení z objektů

Výše je znázorněno dialogové okno z programu SIMS, ve kterém je uveden detailní výpis zpráv z monitorovaných objektů. V této části programu můžeme zobrazovat všechny výpisy hlášení doručených na PCO včetně historie událostí ve střežených objektech.

4.3 Program AlVis (Alarm Visualization System)

Program **AlVis od slovenského výrobce SPIRIT a.s.** je možné použít pro vizualizaci a řízení všech systémů automatických parkovacích systémů (**APS)** a pro integraci přístupového systému s dalšími systémy inteligentních budov.

AlVis je vhodný všude tam, kde vzhledem k požadavkům obsluhy nebo složitosti sledovaného objektu, vybaveného množstvím různých zařízení, není možné bez počítačové nadstavby dosáhnout přehledného a inteligentního monitorování a řízení objektu. Systém AlVis podporuje připojení více než 70 různých zařízení (systémy přístupu, zabezpečení, požární ochrany atd.), což z něj činí ideální prostředek pro integraci technologií různých výrobců instalovaných v objektech se společnou ostrahou. [10]

Charakteristika

AlVis je univerzální grafické vývojové prostředí určené na tvorbu aplikací monitorovacích a řídících systémů. Je vhodný všude tam, kde vzhledem k požadavkům obsluhy, složitosti sledovaného objektu, množství různých zařízení a prioritních úrovní, není možné bez použití počítačového systému dosáhnout přehledný flexibilní lehce adaptovatelný monitorovací, řídící a výstražný systém.

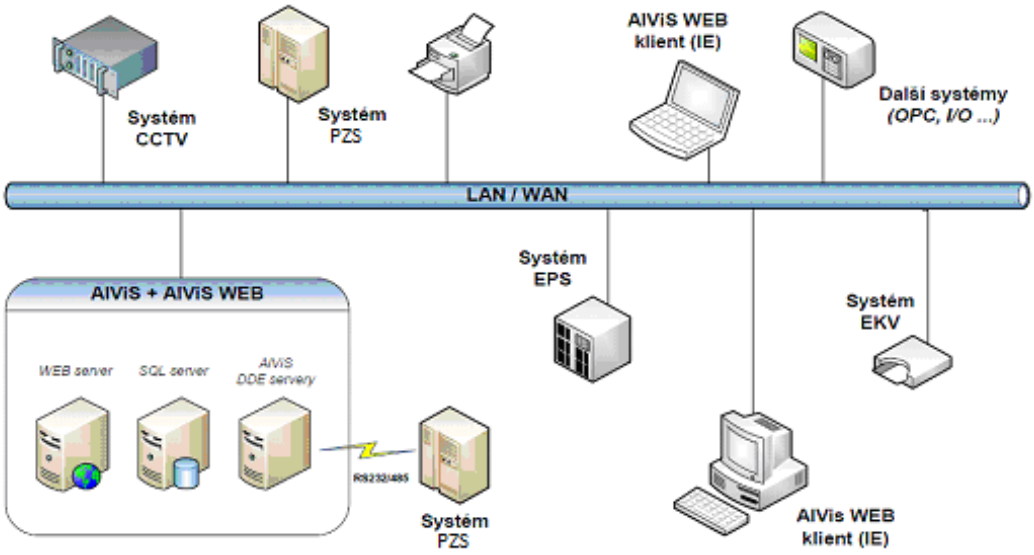
Ekonomické přínosy inteligentního a integrovaného řízení budov prostřednictvím systému AlVis spočívají v úspoře energií při optimalizovaných procesech osvětlení, topení a klimatizace ve vazbě na systémy řízení přístupu a přítomnosti osob. Dalším ekonomickým přínosem je úspora na mzdách za ochranu a správu objektu, když při kvalitně nastaveném systému zvládne požadované úlohy menší počet zaměstnanců.

Bezpečnostní přínos inteligentního a integrovaného řízení budov prostřednictvím systému AlVis spočívá ve zpřehlednění celkové situace a automatickém provázání systémů při řešení havarijních a evakuačních postupů v budově.

Architektura klient / server

AlVis je založený na architektuře klient / server, což umožňuje distribuované rozdělení monitorovacího a výstražného systému na více počítačích, vzájemně propojených pomocí

počítačové sítě (LAN, WAN, INTERNET…) Samotný program AlVis je klientem určeným na vizualizaci stavu monitorovaného prostoru. Pro svoji činnost využívá služby programových serverů, které komunikují s připojenými zařízeními a poskytují potřebné údaje. Neomezené množství programových serverů a klientů může být aktivováno v rámci počítačové sítě a na komunikaci mezi nimi se využívá standardní protokol „DDE“ (v případě síťové komunikace NetDDE). Každý klient může zobrazovat libovolnou podmnožinu údajů poskytovaných dostupnými servery. [10]



Obr. 11. Struktura systému [11]

Otevřenost

AlVis nemá žádné omezení na druh, množství, výrobce, ani způsob připojení monitorovaných zařízení. V současnosti je k dispozici několik desítek komunikačních serverů pro podporované systémy, a tato množina se neustále rozšiřuje.

Podpora práce v sítích LAN / WAN (TCP / IP)

Program podporuje připojování vzdálených zařízení pomocí modulů terminálových serverů (převodníků RS 232/TCP/IP). Tím umožňuje bezpečnostní monitoring vzdálených objektů a lokalit.

Technické předpoklady instalace

Počítač PC Pentium II, 512 MB RAM, 1G HDD s operačním systémem MS Windows 2000 SP4\XP\Vista a MS IE 6.0. Volitelná výbava je zvuková karta, síťová karta, modem. Jedna, anebo více ústředen PZS / EPS připojená na počítač přes sériové linky, nebo speciální vstupní / výstupní kartu.

Jednoduché konfigurování a modifikace systému

Systém AlVis pracuje ve dvou režimech:

1) Režim „vývoj“ je určený pro návrh monitorovacího a výstražného systému. Umožňuje vkládat uživatelem definované grafické plány objektů a rozmístit v plánech mnohostavové symboly hlásičů a zařízení, a to včetně jednoduché manipulace s nimi (zvětšování a zmenšování symbolů přímo v plánech, rotace, zrcadlení a převracení symbolů). Pro plány i symboly jsou podporovány tyto formáty: jpg, gif, bmp, wmf, emf. Další užitečnou pomůckou související s grafickým jádrem je rozšířená funkce tzv. tooltipu[12]. Kromě běžné informace o symbolu je tooltip doplněn o možnost zobrazení poslední protokolové zprávy související s vybraným symbolem. Má zabudované prostředky umožňující úplné přizpůsobení aplikace na požadavky zákazníka a prostředky na ulehčení práce při tvorbě aplikace jako:

- funkce kopírování konfiguračních údajů na různých úrovních (od stavů hlásiče až po vkládání celých plánů objektů)
- funkce skupinových úprav aplikace pomocí inteligentního příkazu „nahradit“ s využitím regulérních výrazů
- funkce konfigurování symbolů podle dopředu připravených šablon

Webové oblasti, webové plány

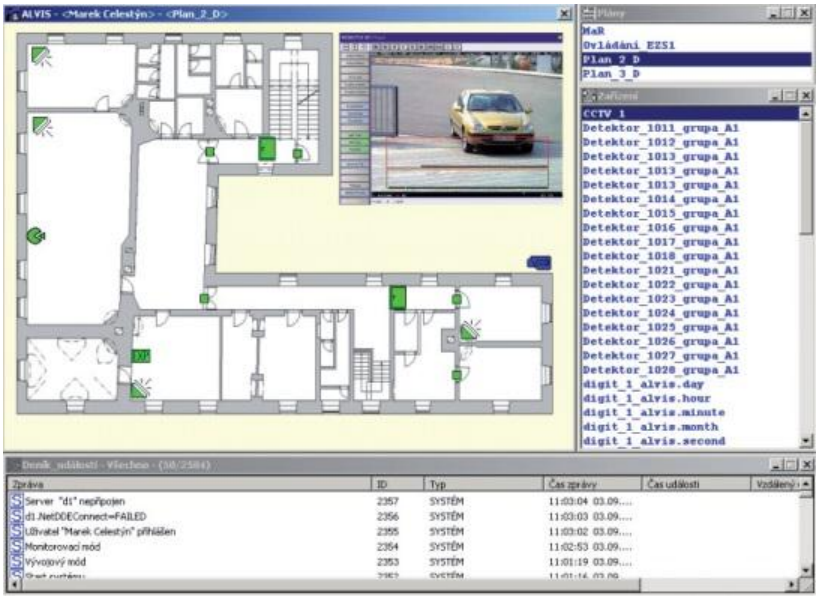
Do aplikace AlVis je možno kromě běžných plánů vložit i libovolný počet oblastí zobrazující HTML, XML soubory, nebo přímo WWW stránky. Kromě přímé definice odkazu na WEB oblasti je možné využít i funkce vnitřního skriptovacího jazyka AlVisu pro práci s WEB oblastmi a vytvářet tak dynamicky spravované WEB odkazy. Tyto vlastnosti řeší zejména propojení AlVisu s kamerovými systémy a umožňují přenos videosignálu pro CCTV systémy podporující prohlížení dat z prostředí WEB prohlížečů. S masivní podporou WEB technologií souvisí i vnitřní funkce Alvisu umožňující generovat reporty o instalaci do přehledné a uživatelsky definovatelné WEBové podoby s využitím formátu XML. Tento formát je také možno použít přímo pro uložení aplikace AlVis.

[12] Tooltip - chápeme jako malé „vyskakovací okno“, které většinou doplňuje informace

2) Režim „monitorování“, který aktivuje vstupně-výstupní linky a zobrazuje změny stavů monitorovaných zařízení. Umožňuje sledovat všechny události na monitoru, aktivně pomocí myši přepínat plány, případně vysláním povelů řídit připojená zařízení.

Přehledné zobrazení monitorovaného prostoru

Monitorovaný prostor je v systému AlVis reprezentovaný plány. Na plánech umístněné symboly reprezentují monitorovaná zařízení. Systém umožňuje definovat libovolné množství plánů (podlaží budov, parkoviště apod.). Plán je obrázek vytvořený grafickým programem nebo scanovacím zařízením.



Obr. 12. Zobrazení monitorovaného prostoru [10]

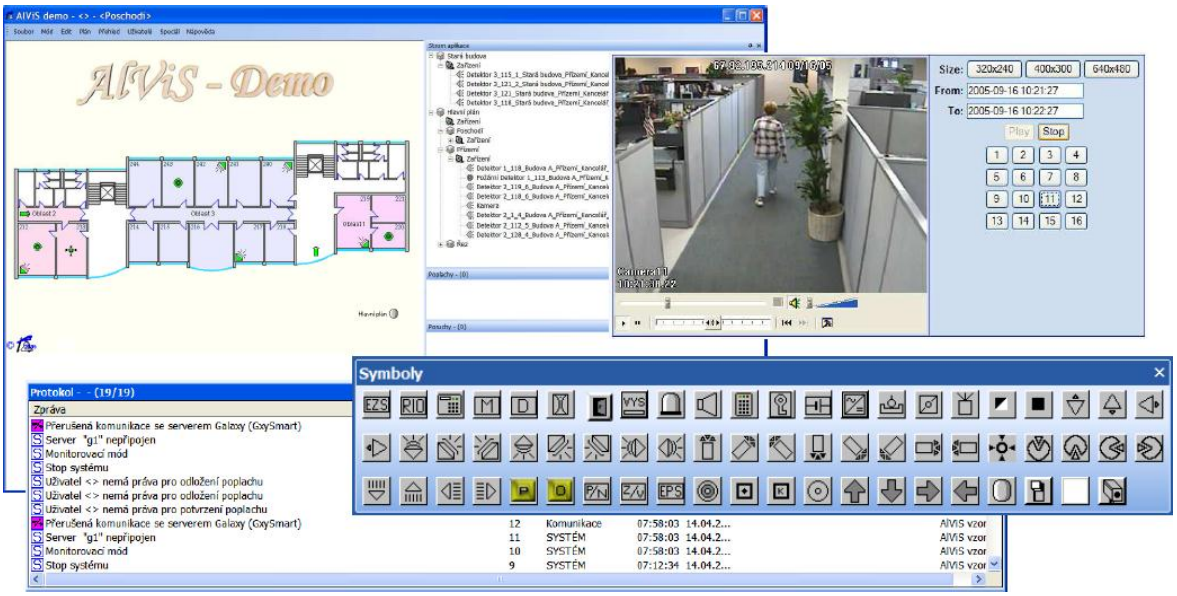
Monitorovaná zařízení

Všechna monitorovaná zařízení (kamery, detektory pohybu, otřesu, požáru, tísňová tlačítka atd.) jsou v systému AlVis reprezentována symboly umístněnými na plánech. Pro každý symbol je možné definovat chybové hlášení (porucha, odstranění poruchy) a stavy v závislosti na skutečně naměřených hodnotách signálů přicházejících od zařízení (odlišené barvou respektive tvarem symbolu). Pro každý stav zařízení je možné definovat následující atributy:

- chování symbolu – zvukový signál resp. blikání symbolu v případě, že nastal daný stav zařízení
- poplach – definování daného stavu jako poplachového, přičemž pro každý poplach je možné určit prioritu poplachu, oprávněnost obsluhy, potvrdit poplach,

automatické zobrazení plánu, na kterém nastal poplach a automatické potvrzování poplachu

- poplachové zprávy – krátkou zprávu zobrazovanou v přehledovém okně poplachů a dva druhy podrobných zpráv zobrazovaných v zvláštním okně s instrukcemi pro obsluhu resp. s podrobnějším popisem stavu, automatické tisknutí plánu a podrobných informací o poplachu
- výstupy – povelové řetězce, které budou automaticky vyslané na požadované zařízení v případě, že nastal daný stav resp. aktivované manuálně obsluhou (kliknutím myší na symbol zařízení). Tato vlastnost umožňuje na základě signálu zařízení řídit ostatní zařízení systému (např. na základě změny stavu detektoru pohybu aktivovat kameru)
- protokol – definování zprávy zapisující se do protokolu na disk počítače spolu s datumem a časem, kdy nastal a s možností on-line výstupu na tiskárnu



Obr. 13. Zobrazení symbolů v plánech [12]

Grafická lokalizace místa, z kterého přichází hlášení o změně stavu poplachu.

V případě, že monitorované zařízení změní stav a nastane poplach, AlVis může automaticky zobrazit plán, na kterém je umístněný symbol daného zařízení. Symbol změní svou barvu, respektive tvar podle stavu, který nastal, zároveň může blikat a vydávat zvukový signál. V přehledovém okně poplachů se zobrazí poplachová zpráva, na obrazovce se objeví okno s instrukcemi pro obsluhu a s podrobnějším popisem stavu zařízení. Do protokolu událostí se zapíše protokolová zpráva spolu s datem a časem. [10]

Prioritní zpracování událostí v reálném čase

Poplachové stavy jsou vyhodnocovány podle priority a času vzniku. Systém AlVis vyhodnocuje poplach s nejvyšší prioritou v reálném čase. V případě, že nastane víc poplachů se stejnou prioritou, systém je vyhodnocuje podle času, kdy nastaly. Po potvrzení poplachu obsluhou se zobrazí poplach s další nejvyšší prioritou atd. až do potvrzení všech poplachů v systému. Všechny aktuální poplachy jsou zároveň zobrazeny (podle priority a času vzniku) v přehledovém okně poplachů. [12]

Protokolování událostí v systému

Všechny události, které nastaly v monitorovacím a výstražném systému AlVis, jsou protokolované zápisem v protokole událostí. Protokol událostí je soubor nepřetržitě zaznamenávaný na disk počítače a na tiskárnu. Zapisuje se popis a druh události, klíčová slova, datum a čas událostí, datum a čas zprávy. Prohlížení, filtrování a tisk protokolů, kterých může být víc, umožňují přehledové okna protokolu. [12]

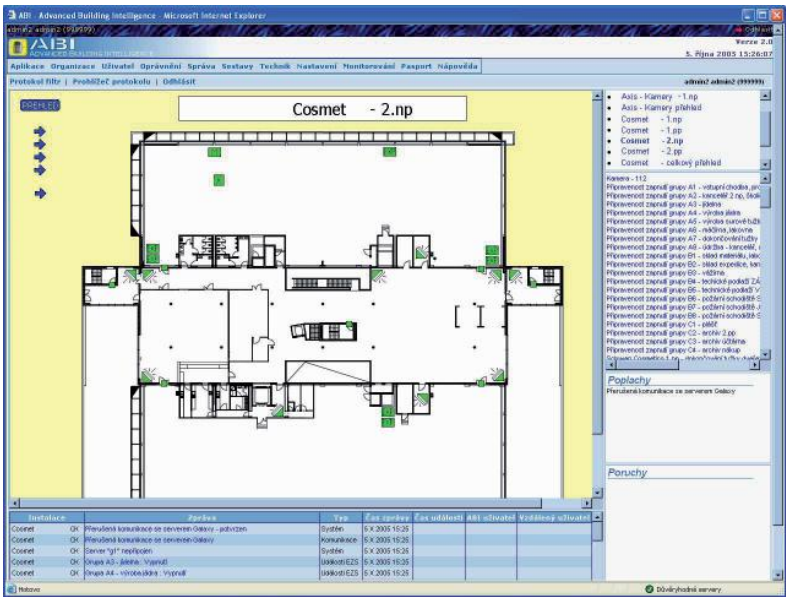
Bezpečnostní parametry systému AlVis

Všechny významné zásahy do programu AlVis jsou chráněny proti neoprávněné manipulaci. Systém hesel a přístupových práv umožňuje flexibilní nastavení oprávnění na vykonávání různých funkcí nezávisle pro jednotlivé pracovníky obsluhy (strážní služby). Ve vývojovém režimu (chráněném superheslem) je možné definovat seznam operátorů, počet a druh informačních oken na obrazovce, parametry zobrazovaných oken (např. zda může obsluha změnit velikost oken a jejich umístnění na obrazovce). Po přepnutí do režimu monitorování je možné vykonávat jen ty operace, na které má momentálně přihlášený operátor oprávnění. Komunikace mezi programovými moduly v počítačové síti je chráněná kryptovacím mechanismem tak, aby nemohla být zneužitá. [10]

AlVis WEB

Jde o sofistikované řešení umožňující plnohodnotnou práci s aplikací nebo i více aplikacemi AlVis libovolnému počtu operátorů za použití standardního prohlížeče WEB stránek (např. Microsoft Internet Explorer, Netscape Communicator, Mozilla, Opera a další) Při realizaci platformy AlVis WEB je využito standardní aplikace AlVisu 3.1 doplněné o server založený na platformě Windows s instalovanou SQL databází, WEB serverem Apache a sadou skriptů tvořících vlastní aplikaci AlVis WEB. Tímto řešením se otvírá možnost vytvoření velkého množství monitorovacích stanic bez licenčních poplatků za každou licenci

programu AlVis. AlVis WEB přebírá nastavení z existujících reálných stanic s běžnou instalací AlVisu a to včetně uživatelských oprávnění a možnosti ovládání připojených technologií.



Obr. 14. Použití ve WEBovém prohlížeči EXPLORER [10]

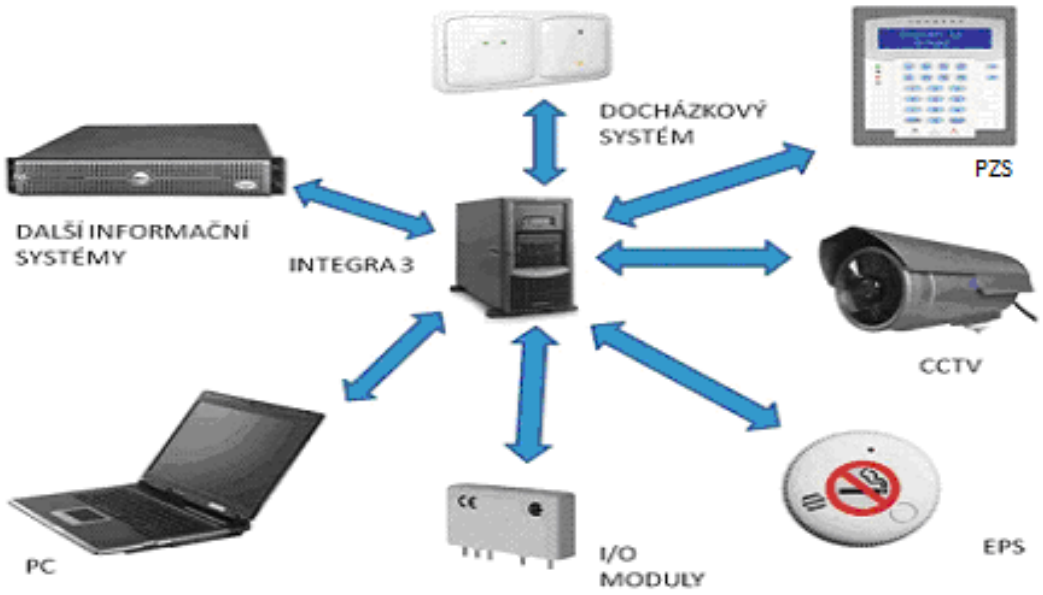
4.4 Program INTEGRA 3

Systém INTEGRA 3 je nástrojem pro správu a řízení bezpečnosti budov, podniků a rozsáhlých areálů. Program **INTEGRA 3 od českého výrobce Integoo spol. s r.o.** lze použít například k vizualizaci systémů **APS 400**.

INTEGRA 3 komunikuje pomocí softwarových ovladačů s bezpečnostními ústřednami PZS, protipožárními systémy EPS, systémy evidence a kontroly vstupu a s kamerovými systémy CCTV. Rozsah podporovaných zařízení zahrnuje vstupně-výstupní moduly, systémy detekce v obraze a díky využití standardních protokolů spolupracuje i se zařízeními typu MaR[13] nebo se systémy třetích stran. Program nabízí možnost umístit prvky reprezentující čtecí moduly přístupového systému na grafický podklad s plánem budovy. Vzniklé provozní události systému jsou online zobrazovány v uživatelském rozhraní, které umožňuje kontrolu systému a snadnou lokalizaci případných poplachových a chybových stavů. Program je mocným integračním nástrojem, který díky svému skriptovacímu jazyku umožňuje práci s daty nejrůznějších technologií a předávání výsledků logických spojení

[13] Zařízení typu MaR – zařízení typu „Měření a Regulace“ např. měření a regulace teploty

dalším subsystémům. Propojení s webovým serverem umožňuje zobrazit grafické a textové informace přímo ve webových prohlížečích v klientské síti.



Obr. 15. Struktura systému [13]

Hlavní úlohou systému je poskytování informací a podporování rozhodování bezpečnostního personálu a zároveň umožnění vzdáleného ovládání technologií (např. zaměření kamery do určitého místa nebo zapnutí střežené oblasti).

Těchto cílů dosahuje Integra 3 tím, že:

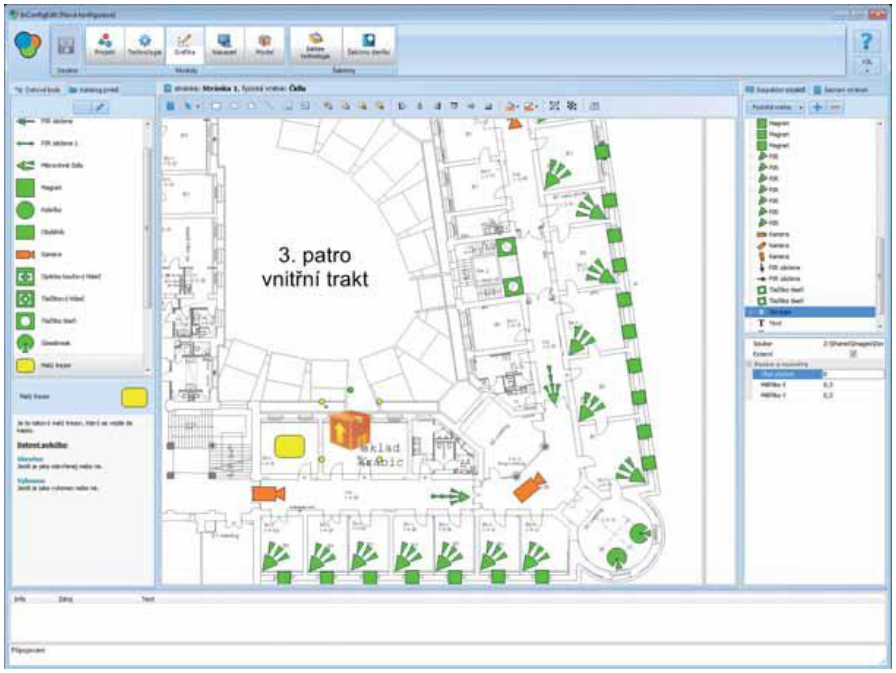
- společně vyhodnocuje údaje z různých bezpečnostních systémů
- prezentuje je způsobem, který je pro personál přehledný a snadno srozumitelný
- umožňuje personálu zadávat pokyny, aniž by bylo třeba učit se ovládat různé technologie
- automatizuje některé rutinní činnosti.

Systém Integra funguje tak, že:

- **Zpracovává data z nejrůznějších bezpečnostních zařízení**, například kamerového systému (CCTV), poplachového zabezpečovacího systému (PZS), protipožárního systému (EPS), vstupních systémů (EKV), veškerých zařízení vybavených I/O moduly (například výtahy či vrata) a dalších zdrojů. To zahrnuje data o tom, zda je zařízení zapnuté a zda je plně funkční, ale především hlášení poplachů a obraz z kamer.

- **Vytváří z nich smysluplné informace** a zobrazuje tyto informace tak, aby byly snadno srozumitelné pro každého uživatele. Na obrazovce se ukazuje třeba plánek areálu s vyznačením, kde vznikl poplach, a obraz z nejbližší kamery. Nebo například plánek téhož areálu s vyznačením, které zóny jsou momentálně v režimu „zastřeženo“. Uživatel tak nemusí přemýšlet o jednotlivých zařízeních. Prostě se dozví, jaká událost nastala, kde dostane instrukci, jak má postupovat.
- **Automaticky sestavuje deníky událostí.** Dispečeři a strážní jsou tak ušetřeni jakékoliv administrativy a vedení organizace naprosto spolehlivě ví, co se stalo, v kolik hodin bylo zastřeženo, zda nastaly poplachové situace a jak na ně kdo reagoval.
- **Umožňuje vzdálené ovládání bezpečnostních technologií**. Pracovníci ochranky a dispečeři mohou například přepnout část areálu do režimu „zastřeženo“, ve kterém jsou veškeré vzruchy vyhodnocovány jinak než během pracovní doby. Mohou si také kliknout na místo na mapce areálu a podívat se bezprostředně na obraz z kamery.
- **Poskytuje podklady potřebné pro vyšetřování událostí**, aniž by bylo zapotřebí procházet elektronické archivy. Systém automaticky „indexuje“ určité události (například neautorizovaný vstup nebo průjezd vozu s konkrétní poznávací značkou), takže při zpětném hledání stačí pár kliknutí myší.
- **Podporuje řízení údržby bezpečnostních zařízení.** Integra 3 udržuje databázi informací o každém jednotlivém bezpečnostním zařízení, včetně historie. Může tak s předstihem upozornit na termín povinné kontroly, naplánovat opravu nebo třeba poskytnout souhrnnou informaci o nákladech zařízení během celého životního cyklu.

Způsob upozornění na mimořádné události (poplachy, poruchy) a jejich zpracování je ze všech integrovaných systémů prováděno jednotným způsobem. Operátor dostává nejen informaci o výskytu události, ale také textové i grafické pokyny, jak situaci řešit. Díky tomu jsou operátoři více samostatní a zvyšuje se jistota, že zareagují předepsaným způsobem.



Obr. 16. Vzhled uživatelského rozhraní programu INTEGRA 3 [14]

Některé klíčové výhody je možné shrnout takto:

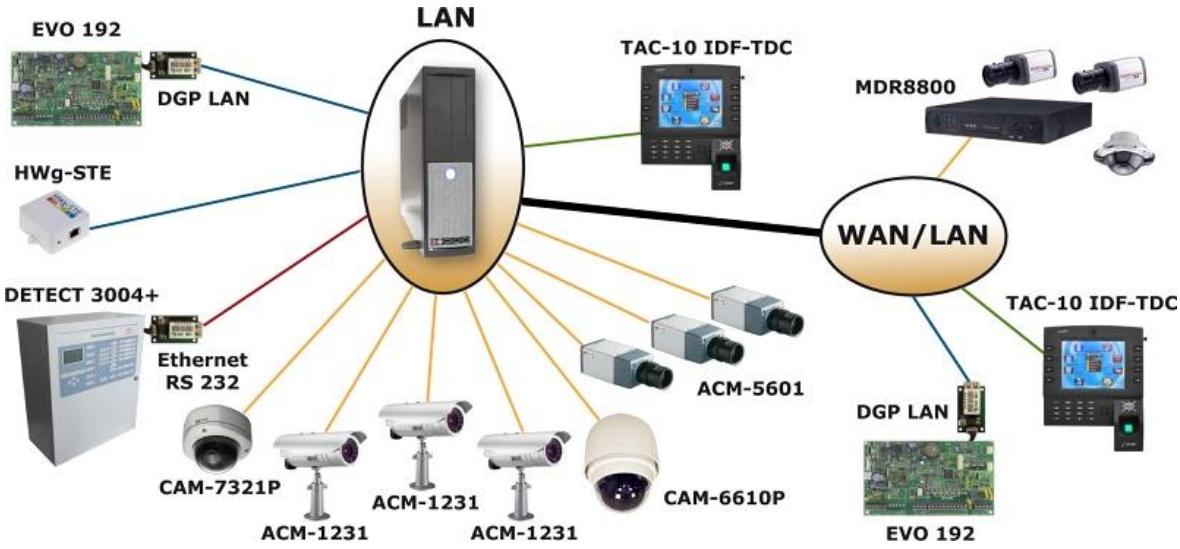
- okamžitá reakce na narušení bezpečnosti
- jistota, že všechna zařízení jsou momentálně plně funkční
- rychlé zapracování operátorů

Integra 3 nenabízí výběr z omezeného počtu nastavení, jak to známe třeba u účetních systémů. Každý správce systému rozhoduje, jak v rámci budovy či areálu definovat zóny, které z nich střežit, která zařízení zapojit, jak definovat jednotlivé režimy, komu umožnit přístup, co sledovat atd.. Dokonce i vzhled ikonek na uživatelských obrazovkách je možné měnit.

Informační systém Integra 3 bychom mohli přirovnat k integrační platformě. Umožňuje hladkou spolupráci různých zabezpečovacích zařízení od různých výrobců. Zároveň však poskytuje jednotné rozhraní, kde každý uživatel najde přehledně zobrazené právě ty informace, které potřebuje ke své práci, ať už se jedná o zaměstnance ostrahy a dispečery, manažery, správce IT, vyšetřovatele a auditory či kohokoliv dalšího.

4.5 Program VAR-NET INTEGRAL

Česká firma VARIANT plus, spol. s r.o., která byla založena v roce 1992, je mimo jiné zaměřena na velkoobchodní činnost v oblasti bezpečnostních a dalších elektronických systémů pro komerční budovy i objekty určené k bydlení. Jednou z jejich činností je i vývoj software, mezi který patří program s názvem **VAR-NET INTEGRAL.** Tento program umožňuje integrovat různé bezpečnostní systémy. VAR-NET INTEGRAL je systém pro sledování, správu a vyhodnocování elektronických systémů budov a rozlehlých objektů. Umožňuje i společnou správu a ovládání více vzdálených objektů klienta z jednoho místa přes webové rozhraní. Je navržen jako ucelené řešení, složené ze vzájemně nezávislých modulů. Moduly jsou schopny pracovat samostatně, jsou však provázány a jejich kombinace poskytuje dodatečnou funkcionalitu. Použití modulů dává uživateli možnost zvolit jen ty funkce, které bude používat, a tím efektivně využít vynaložené prostředky. Toto řešení je určeno pro menší a střední objekty (až 6 typů bezpečnostních technologií, tj. PZS, CCTV, EPS, docházka a přístup pro až 400 osob s přístupovými právy, z toho až 200 s registrovanou docházkou). Do softwaru VAR-NET INTEGRAL jsou zařazeny zabezpečovací ústředny (DIGIPLEX EVO, dle údajů od výrobce bude v budoucnu rozšířen i o ústředny IMPERIAL), kamerové systémy (IP kamery ACTi, DVR Micro Digital), elektronická požární signalizace (JOB detectomat) a docházkové a přístupové terminály VAR-NET. Jak uvádí výrobce v případě potřeby je schopen zajistit i integraci jiných technologií od jiných výrobců (např. ústředny GALAXY, kamery AXIS, EPS SIEMENS atd.), zejména tam, kde má již uživatel některé systémy nainstalovány.



Obr. 17. Možnosti využití programu VAR-NET INTEGRAL [15]

Základní funkce programu

Modulární software se dá funkčně rozdělit do okruhů navzájem provázaných centrální správou osob a detekčních bodů:

Bezpečnost

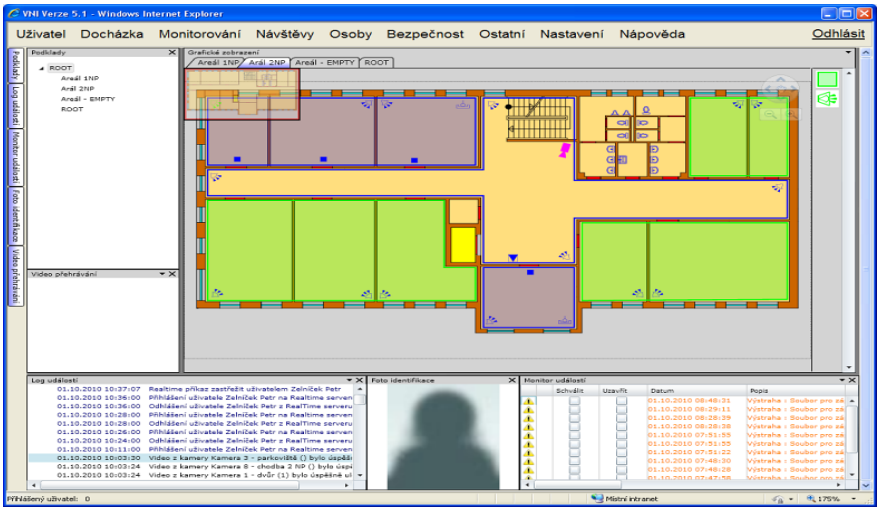
Jednou ze základních funkcí systému je zajistit vzdálený dohled a ovládání bezpečnostních prvků. Vizualizací a sjednocením ovládání se dosahuje přehlednosti a jednoduchosti, zvlášť při integraci více prvků. Požární senzory a ústředny, kontrola vstupu, kamerové a bezpečnostní systémy, to vše je řízeno a logováno dle zadaných pravidel. Samozřejmostí je komplexní záznam o činnosti operátorů systému, stejně jako možnost automatizovaných vazeb mezi připojenými technologiemi.

Management lidí a prostředků

Nejkomplexnější oblastí, kterou VAR-NET INTEGRAL obsahuje, je management lidí. Jako všechny systémy, ve kterých do hry vstupuje lidský faktor, i tento systém je obsáhlý, s mnoha možnostmi nastavení a změn.

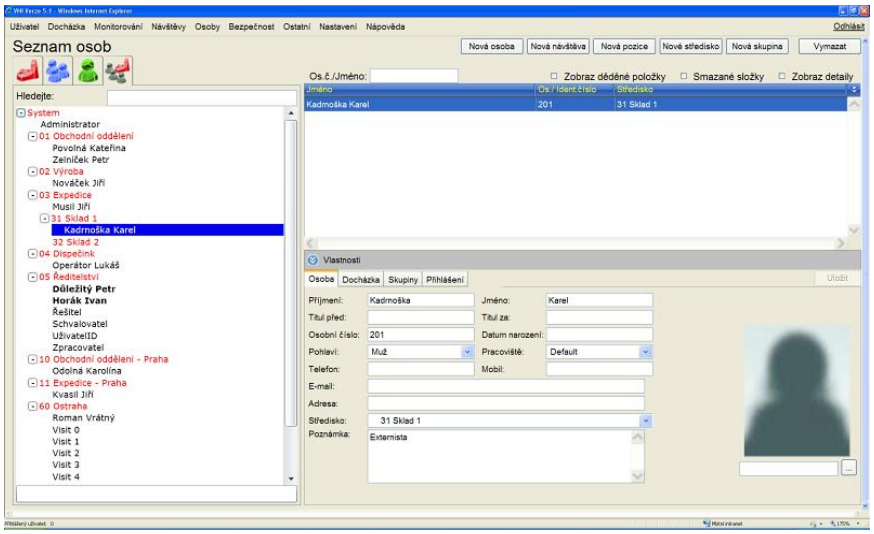
Správa a vyhodnocení

Správa osob a organizační struktury je společná pro všechny moduly. Centralizace a přiřazení práv pozicím, nikoli konkrétním osobám, umožňují správcům systému snadnou orientaci, rychlé provedení změny a vysokou úroveň bezpečnosti. Požadavkům na flexibilitu odpovídá možnost připojení z jakéhokoliv počítače s prohlížečem bez nutnosti instalovat klientské programy či dokonce pořízení specializovaného hardwaru. Architektura systému je maximálně pružná, umožňující pohodlnou konfiguraci a užívání, vždy s důrazem na pohodlí uživatele a ekonomičnost.



Obr. 18. Komunikační okruh PZS/CCTV/EVS/EPS/ENVIR [15]

VAR-NET INTEGRAL je server - klient systém. Tato architektura splňuje důležité zadání úspory prostředků. K ovládání je možno použít jakékoliv PC připojené k internetu. Vzhledem k podpoře TCP/IP protokolu není instalace software VAR-NET INTEGRAL limitována lokální sítí. Tato vlastnost nabízí jedinečnou možnost centralizace databází či obsluhy, a tím i možnost dalšího zefektivnění investic.



Obr. 19. Ukázka doplnění přístupových osob [15]

4.6 Program PersonLocator

Tento software **od české firmy 7 Marsyas Development a.s.** slouží k monitorování pohybu osob a předmětů s pomocí RFID[14] čipů. Je to systém kontroly vstupu a oprávněnosti pobytu s 3D grafickou nástavbou.

PersonLocator je inteligentní sytém pro monitorování pohybu osob nebo věcí pomocí osobních aktivních RFID přívěšků ve všech prostorách střeženého objektu a jejího okolí. Aktuální polohu osob nebo věcí lze on-line zjistit v běžném webovém prohlížeči, a to formou přehledných tabulek, nebo lze polohu pozorovat v 3D grafickém modelu budovy v podobě zástupných ikon s jejich jmény. To vše zcela nezávisle na jejich chování. Pohyb objektů mezi jednotlivými oblastmi lze také zpětně vyčíst v jakémkoliv období v historii. Přesnost monitorování závisí na hustotě pokrytí snímači v objektu. PersonLocator poskytuje informace k jednotlivým osobám, kolik hodin strávili za zvolené období aktivně v dané oblasti objektu, u svého pracovního stroje, kolik na prodejně, kolik v kanceláři, kolik v zázemí, ve skladu, mimo objekt atd.. Lokality se uživatelsky definují. Informace obdržíte přehledně v tabulkách. Protože se jedná o moderní webovou aplikaci, je klientský přístup velmi jednoduchý.

Přístupový systém a kontrola pohybu

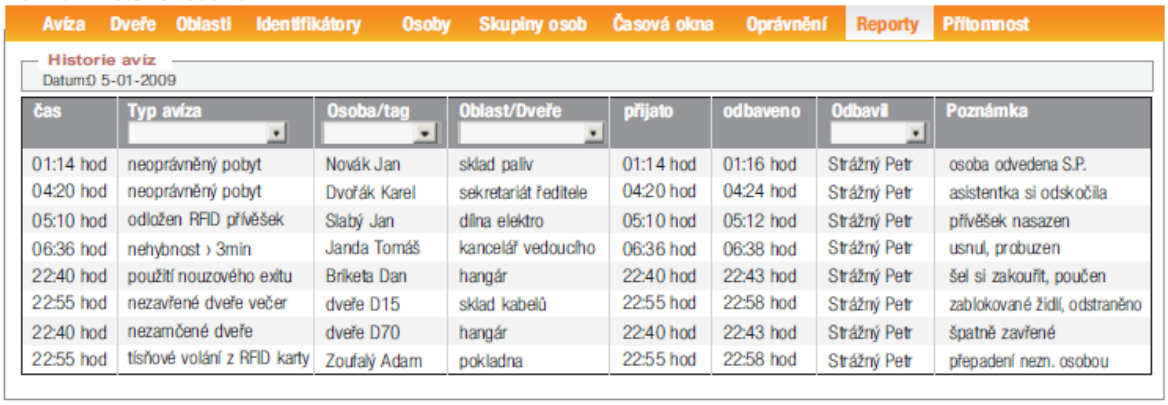
Systém umí pomocí RFID identifikátorů provozovat také přístupový systém přímým ovládáním klasických nebo samozamykacích elektrických zámků (ABLOY, BEFO, BERA). Přístupová práva se definují komfortním způsobem. Od klasických přístupových systémů se PersonLocator liší tím, že nedefinuje pouze to, zda systém oprávněné osobě otevře dveře, ale definuje i to, zda se vůbec může daná osoba v oblasti pohybovat, přičemž je lhostejné, jak se neoprávněná osoba do oblasti dostala. Když systém vyhodnotí osobu v dané oblasti jako neoprávněnou, pošle na stanoviště stálé bezpečnostní služby bezpečnostní hlášení. Ochranka má k dispozici informace o stavu dveří, např. zda jsou dveře dlouho otevřeny, nezavřeny, nezamčeny nebo vyraženy. Dveře se po odchodu z místnosti automaticky zamykají na dva západy.

[14] RFID čip – slouží k bezkontaktní komunikaci na krátkou vzdálenost, identifikace na rádiové frekvenci

Bezpečnostní hlášení stálé bezpečnostní službě

Systém umí zcela automaticky posílat na vytipované PC pracovišti stálé služby bezpečnostní hlášení typu:

- neoprávněná osoba v oblasti, konkrétní osoba v oblasti,
- totální nehybnost osoby,
- odložení osobního RFID přívěšku,
- osoba v oblasti déle než určený časový limit,
- nezavřené dveře večer,
- zavřené, ale nezamčené dveře atd..



Obr. 20. Prohlížení historie všech hlášení [16]

Agenda Přítomnost osob v oblastech osob

Agenda **Přítomnost osob v oblastech objektu** slouží k přehledu, kolik osob se nalézá on-line v jednotlivých oblastech (místnostech) objektu a informace je rozdělena na osoby oprávněné k tomuto pobytu a na osoby neoprávněné. V případě, že jsou v oblasti pouze neoprávněné osoby (bez doprovodu osob oprávněných), zasílá agenda **Avíza** varovné hlášení ostraze o této skutečnosti, přičemž v hlášení je informace, kdo se neoprávněně v dané oblasti nachází. V případě, že klikneme v níže uvedeném seznamu na jednu z oblastí, odkaz nás přenese do agendy **Seznam osob** ve vybrané oblasti, kde jsou již uvedena konkrétní jména osob.

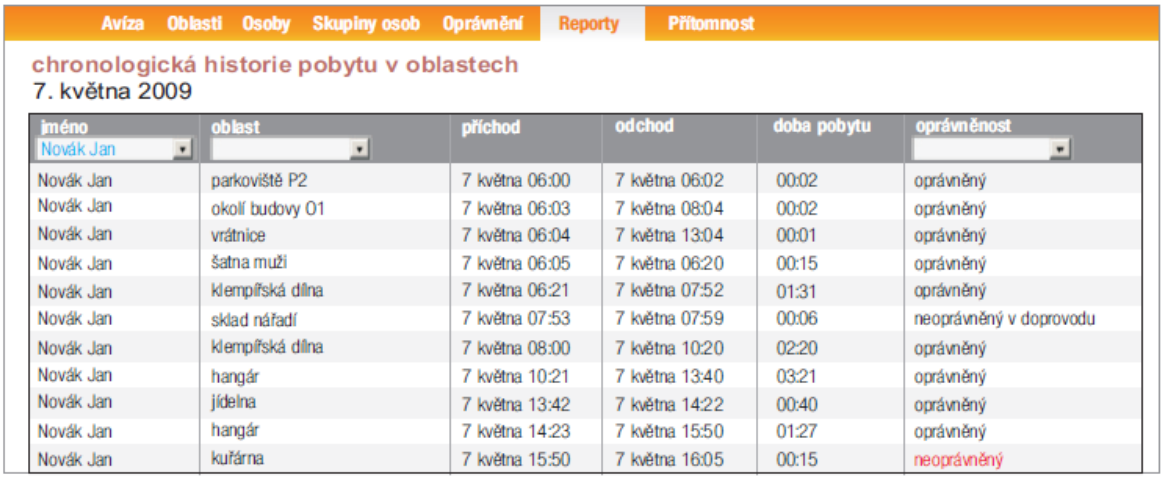
Kontrola oprávněnosti pobytu osob v oblasti

Díky tomu, že systém PersonLocator umí nejenom opravňovat ke vstupu u dveří autorizovanou osobu, ale hlavně umí automaticky on-line kontrolovat, zda osoba, která se nachází již uvnitř oblasti, je zde oprávněně, či nikoli a to bez ohledu na to, jak se tam dostala. Navíc systém bere v úvahu, zda osoba, která se nachází v oblasti, kde nemá příslušná oprávnění, je zde v doprovodu oprávněné osoby. V případě, že je v doprovodu takovéto osoby, tak je vše v pořádku. Když ovšem oprávněná osoba z oblasti odejde a nechá neoprávněnou osobu samotnou, systém vyhlásí po nastaveném čase bezpečnostní hlášení ochrance. Veškerou historii vyřešených bezpečnostních hlášení a komentářů může správce vyčíst z agendy **Reporty/Historie avíz**. Ve sloupci ”Typ avíza” si správce vybere jednu kategorii, například: “neoprávněná osoba v oblasti bez doprovodu". Do historie bezpečnostních hlášení se zapisuje čas přijetí hlášení, typ hlášení, lokalita, inkriminovaná osoba, zodpovědná osoba, která bezpečnostní hlášení vyřešila a její komentář. Filtrovat jde např. podle jména inkriminované osoby nebo oblasti, která nás zajímá.

Zpětné informace o pobytu osob v objektu

Z reportů můžeme vyčíst veškerou historii pohybů osob v objektu. Tyto reporty si můžeme kdykoli prohlížet nebo exportovat do např. MS Excelu, a v něm poté upravovat do hlášení nebo grafů atd.. K dispozici má uživatel tyto automaticky generované reporty:

- chronologický rozpis pohybů osob v jednotlivých oblastech objektu,
- kumulovaný souhrn pobytu osob v jednotlivých oblastech objektu,
- historie bezpečnostních hlášení,
- historie otevření dveří atd..



Obr. 21. Chronologická historie pobytu osob v jednotlivých oblastech objektu [16]

Můžeme s nadsázkou konstatovat, že o softwaru PersonLocator bychom mohli uvažovat jako o opravdovém revolučním systému měření loajality a produktivity zaměstnanců nebo kontroly pohybu věcí.

Dílčí závěr

Předcházející kapitola o monitorovacím software analyzuje jednotlivé vybrané monitorovací programy z hlediska jejich možností nasazení, činností, využití, způsobu grafického zobrazení a dalších vlastností. Tato jednotlivá kritéria budou předmětem hodnocení v následující kapitole, kde si jednotlivé programy zařadíme z hlediska různých možností využití.

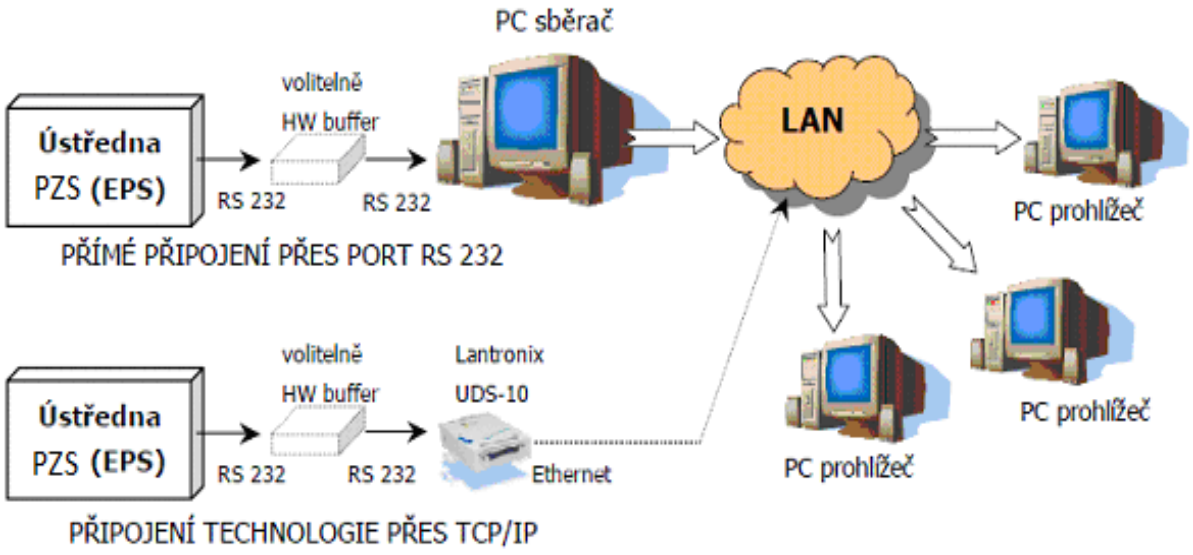
5 NÁVRH MOŽNOSTÍ VYUŽITÍ MONITOROVACÍCH SOFTWARŮ V ZABEZPEČOVACÍCH SYSTÉMECH

Tato kapitola se zabývá vyhodnocením a zařazením jednotlivých popisovaných monitorovacích softwarů dle vybraných vlastností a možností použití, ať už v poplachových či nepoplachových aplikacích.

5.1 Poplachové zabezpečovací systémy

Z hlediska poplachových zabezpečovacích systémů popisované monitorovací softwary TEGAL, SIMS, AlVis, INTEGRA 3 a VAR-NET INTEGRAL splňují požadavky kladené na moderní zobrazování. Uvedené programy jsou výrobci právě deklarovány hlavně jako aplikace k použití v poplachových zabezpečovacích systémech a je to jejich hlavní účel.

Programy TEGAL, AlVis a VAR-NET INTEGRAL podporují monitorování PZS připojených přes port RS – 232 a technologii TCP/IP (Obr. 22), čímž umožňují bezpečnostní monitorování vzdálených lokalit a objektů.



Obr. 22. Způsob připojení PZS (EPS) [8]

Pokud bychom chtěli rozdělit monitorovací systémy podle vhodnosti použití z hlediska PZS použitých například v rodinných domech, státních úřadech, obchodních domech, kancelářských objektech, výrobních objektech, školských zařízeních, musíme brát v úvahu rozsáhlost sledovaných objektů, množství umístěných prvků PZS v objektu a podle toho odvíjející se množství přicházejících zpráv na PCO s monitorovacím softwarem, který má

právě za povinnost tyto informace analyzovat a vyhodnocovat. V této části hodnocení hraje významnou roli kritérium schopnosti monitorovacího programu toto množství dat analyzovat a následně vyhodnotit.

Tab. 1. Vhodnost použití

PZS (EPS) v objektech	*Software*					
	TEGAL	*SIMS*	*AlVis*	*INTEGRA 3*	*VAR - NET*	*Person Locator*
Rodinný dům	1	1	1	1	1	5
Státní úřad	1	3	1	1	3	5
Obchodní dům	1	1	1	1	1	5
Kancelářský objekt	1	1	1	1	1	5
Výrobní objekt	1	1	1	1	1	5
Školské zařízení	1	1	1	1	1	5

V předchozí tabulce (Tab. 1) jsou seřazeny softwary podle toho, zda jsou vhodné pro použití v různých vytipovaných objektech. V této tabulce jsou hodnoty rozděleny do číselné škály v rozmezí 1 až 5, kdy číselná hodnota rovnající se 1 – nejvhodnější, 2 – vhodné, 3 – méně vhodné, 4 – nevhodné a 5 - nepoužitelné pro použití při monitoringu PZS v daném objektu.

5.2 Kamerové systémy CCTV

Mezi další kritérium hodnocení patří schopnost jednotlivých monitorovacích softwarů zobrazování střežených míst kamerovým systémem CCTV.

Vzhledem k tomu, že výše jsme již sledované monitorovací softwary rozdělili podle využití v poplachových zabezpečovacích systémech, budeme v této kapitole hodnotit softwary TEGAL, SIMS, AlVis, INTEGRA 3 a VAR-NET INTEGRAL.

Obr. 23. Kamery používané v CCTV [17]

V této části hodnocení je uvedena schopnost monitorovacích programů integrovat zobrazení z kamerových systémů CCTV do svého programu.

Tab. 2. Tabulka softwarů s rozdělením podle podpory monitorování CCTV

	Software					
	TEGAL	*SIMS*	*AlVis*	*INTEGRA 3*	*VAR - NET*	*Person Locator*
Podpora CCTV	ANO	ANO	ANO	ANO	ANO	NE

Opět musíme konstatovat, že vývojáři těchto programů už v dnešní době považují za standart, aby jejich dodávaný software byl schopen zpracovávat a zobrazovat snímky pořízené kamerovým systémem CCTV ze střežených míst.

5.3 Docházkové systémy

Dalším sledovaným kritériem je možnost.zobrazení a vedení přístupového, docházkového systému ACCESS v těchto softwarech. Opět programy rozdělíme na ty, co jsou přístupové

a docházkové systémy schopny monitorovat, případně na ty, co jsou přímo vyvíjeny pro tento účel.

Obr. 24. Docházkový terminál [18]

Zde musím konstatovat, že program SIMS je sice schopen ve svých zaznamenaných hlášeních dosáhnout záznamu, kdy byl učiněn vstup do objektu, ale není zaměřen na vedení docházky v plném rozsahu např. vedení jmenného seznamu zaměstnanců a jejich pohybů přes systém ACCESS.

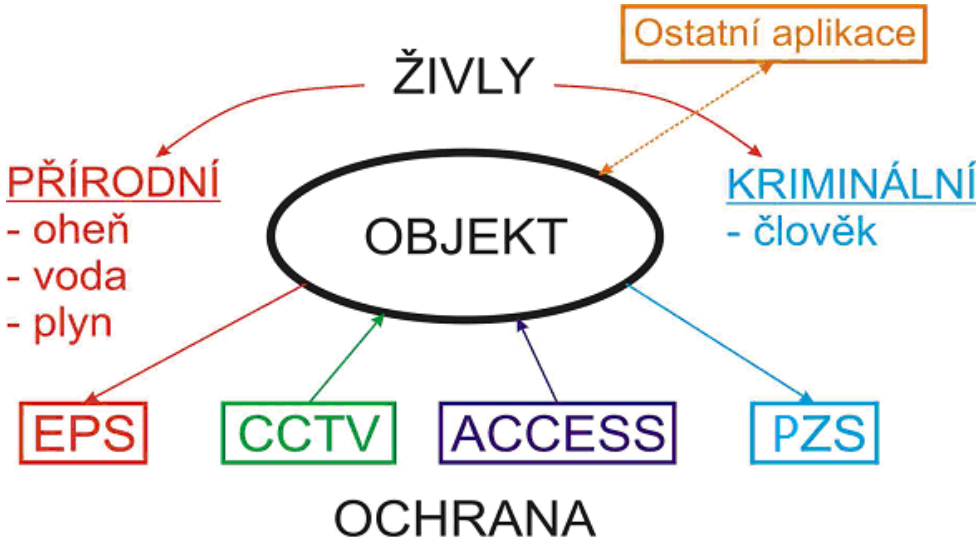
Tab. 3. Podpora přístupových a docházkových systémů

	Software					
	TEGAL	*SIMS*	*AlVis*	*INTEGRA 3*	*VAR - NET*	*Person Locator*
ACS systém	ANO	NE	ANO	ANO	ANO	ANO

V této kategorii hodnocení je na prvním místě software PersonLocator. Tento software je naopak primárně určen ke sledování pohybu osob, takže je využíván v docházkových systémech. Výrobce tohoto softwaru se zaměřuje konkrétně na tuto činnost. Zbylé hodnocené softwary umožňují integraci s docházkovými systémy ACCESS a následně dokáží zpracovávat údaje o docházce dodávané tímto docházkovým systémem.

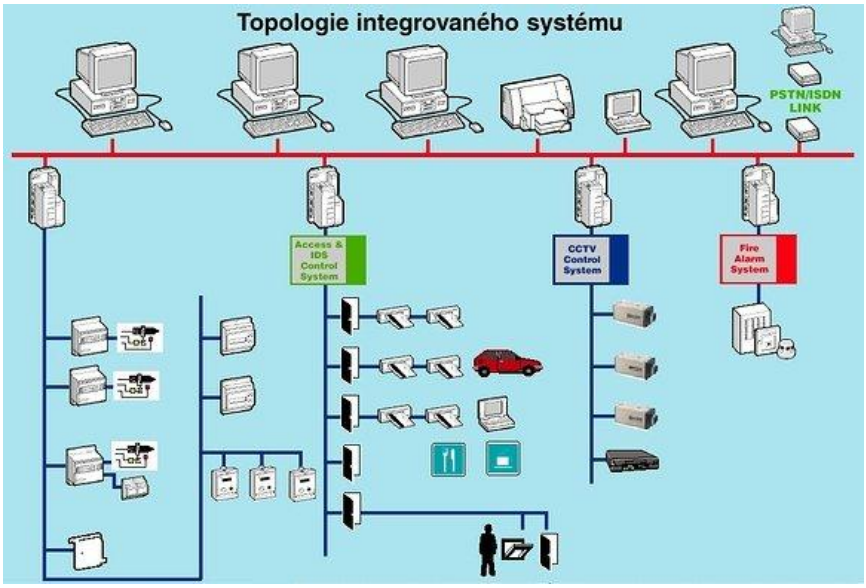
5.4 Integrace

Kapitola s názvem „Integrace“ se zabývá schopností monitorovacích softwarů spolupracovat s různými poplachovými či nepoplachovými systémy.



Obr. 25. Příklad aplikací určených k integraci a ochraně objektu

Pod pojmem spolupráce těchto programů si můžeme představit schopnost zobrazovat a zaznamenávat různé stavy poplachových nebo nepoplachových zařízení jako jsou např. nepoplachové aplikace – ovládání výtahů, spouštění klimatizace, zapínání osvětlení, zatahování žaluzií, docházkový systém a poplachové – poplachový zabezpečovací a tísňový systém.



Obr. 26. Topologie integrovaného systému [19]

5.4.1 Integrace v poplachových aplikacích

Mezi poplachové aplikace řadíme poplachový zabezpečovací a tísňový systém. Všechny popisované softwary, kromě programu PersonLocator, jsou přímo vyvíjeny primárně pro použití v těchto systémech. Jejich úkolem je vytvářet uživatelské prostředí pro obsluhu tím, že obsluze dokáže jednoduše, přehledně a co nejrychleji zprostředkovávat zprávy z těchto systémů. Jednotlivé monitorovací programy využívají k tomuto účelu různých zobrazovacích metod, ale v zásadě zobrazují všechny podstatné věci a záleží jen na uživateli, pro které grafické znázornění spočívající v umění jednotlivých programů si pro tuto činnost vybere.

5.4.2 Integrace v nepoplachových aplikacích

Pojmem nepoplachové aplikace rozumíme např. ovládání výtahů, spouštění klimatizace, zapínání osvětlení, zatahování žaluzií, docházkový systém apod..

Obr. 27. Schéma integrace [20]

Popisované monitorovací softwary tady můžeme rozdělit na dvě kategorie. Na ty, které podporují integraci v těchto aplikacích, a ty, které tuto integraci neumožňují. Mezi softwary umožňující integraci s nepoplachovými systémy jednoznačně patří INTEGRA 3 a AlVis. Tyto monitorovací softwary jsou ideálními kandidáty pro uživatele, který má záměr řídit a sledovat systémy budov tzv. inteligentní budovy.

Tab. 4. Porovnání z hlediska využití jednotlivých programů

Software	*Vlastnosti a oblast použití*				
	PZS	*Kamerový systém*	*Docházkový systém*	*Integrace v poplachových aplikacích*	*Integrace v nepoplachových aplikacích*
TEGAL	+	+	+	+	-
SIMS	+	+	-	+	-
AlVis	+	+	+	+	+
INTEGRA 3	+	+	+	+	+
VAR-NET	+	+	+	+	-
Person Locator	-	-	+	-	-

V závěru této kapitoly je uvedena srovnávací tabulka (Tab. 4), ve které jsou znázorněny jednotlivé monitorovací programy v souvislosti s možností využití v určených oblastech. V této tabulce jsou jednotlivé programy označeny v jednotlivých kategoriích znamínky + nebo –, a to v závislosti na tom, zda uvedenou vlastnost nebo oblast použití tento monitorovací software podporuje či nikoliv. Podle znázorněné tabulky č. 4 se můžeme mylně domnívat, že program AlVis a INTEGRA 3 jsou nejlepší, vzhledem k tomu, že podporují všechny vyjmenované vlastnosti a oblasti použití. Toto tvrzení není zcela pravdivé, protože například v docházkových systémech může tyto softwary předčit program

PersonLocator. Tato tabulka ukazuje jen možnosti jednotlivých softwarů nikoliv jejich kvalitu v dané vlastnosti nebo oblasti použití.

Dílčí závěr

Všechna hodnocení vyplývají z technických parametrů a výrobcem či dodavatelem deklarovaných systémových možností jednotlivých produktů. V některých srovnatelných případech je vycházeno z osobního expertního odhadu. Hodnocení úrovně příslušného monitorovacího softwaru bude vždy závislé na hodnocení uživatelů pracujících s těmito monitorovacími programy a na jejich spokojenosti.

6 VÝVOJOVÉ TRENDY V OBLASTI POUŽITÍ MONITOROVACÍCH SOFTWARŮ

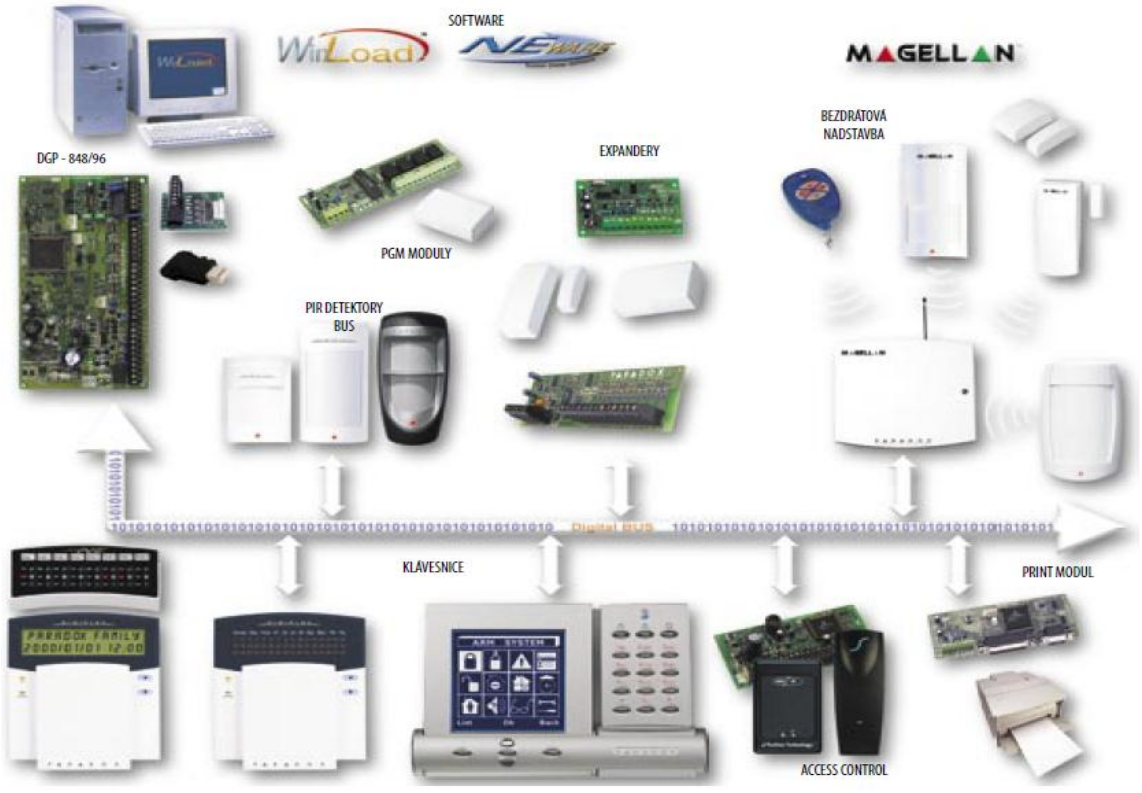
Význam ochrany majetku narůstá v dnešní době do extrémních výšek. K významu ochrany majetku přispívají nejrůznější faktory. Jedním z nich je nepochybně statisticky doložené zvyšování hodnoty nemovitého majetku, na kterou má vliv jak rostoucí objem, tak i cena investic. Dalším z neméně významných faktorů je zvyšující se frekvence nejrůznějších hrozeb, rizik a také nároků na provoz a zabezpečení. Nejdůležitějším je však cenový poměr mezi investicí do zabezpečení a celkovou cenou majetku. Chráněný majetek má několikanásobnou hodnotu oproti investici do jeho zabezpečení. Jedná se především o rodinné domy, bytové či nebytové prostory, podnikové budovy nebo areálové komplexy**.**

Trend růstu složitosti a různorodosti bezpečnostních zařízení je patrně nezvratný. Zabezpečení ve formě kamerového systému, ochrany proti neoprávněnému vniknutí a u větších komplexů ve formě zónového přístupu, kontroly zaměstnanců, protipožární ochrany či zabezpečení a automatizace vrátnic je vysoce účinné, navíc s vysokou variabilitou i cenově přijatelným řešením, jak ochránit svůj majetek. V objektech, provozech a kancelářích každé větší organizace dnes najdeme kamery, protipožární zařízení, systém řízení vstupů, čidla na oknech a dveřích a další slaboproudé systémy. Ve velkých administrativních budovách jsou takových zařízení desetitisíce. Stále složitější infrastruktura vyžaduje pracnější správu a údržbu. Různorodost zařízení představuje náročný problém i pro bezpečnostní personál a manažery – je stále obtížnější rychle pochopit, co se děje a správně reagovat. Odpovědi na otázky jako např. „ Co znamená aktivace čidla v sekci B16? Kde se ta sekce vůbec nachází? Jaké další informace ze stejné zóny mohu získat?“, už vyžadují technicky zdatného uživatele, zvláště v situaci, kdy je nutné zasáhnout velmi rychle. Logickým řešením tohoto dilematu je **integrace**. Spojení různorodých bezpečnostních zařízení do kompaktního celku umožňuje nejen zjednodušit zprávu, ale také usnadnit práci ochranky, řadu činností automatizovat a snížit náklady na ostrahu při současném zvýšení bezpečnosti - **centralizovaný dohled snižuje provozní náklady a zároveň zvyšuje bezpečnost.**

V současné době se produkty od kanadské firmy PARADOX Security Systems (DIGIPLEX, MAGELLAN, IMPERIAL) nebo české firmy Jablotron Alarms a.s. (OASIS) považují za nejmodernější v oblasti monitorovaných objektů.

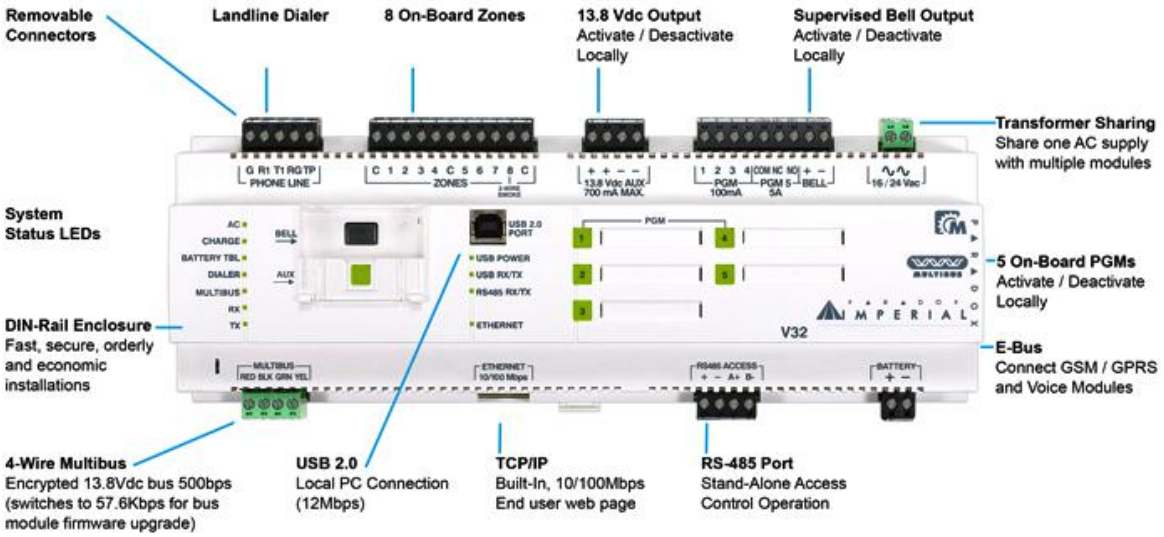
Zabezpečovací systémy PARADOX Digiplex patří mezi nejpoužívanější poplachové zabezpečovací systémy pro střední a velké objekty v České republice. Tyto systémy již byly nainstalovány na několika stovkách bank, vojenských a vládních objektech a dalších budovách vyžadujících vysokou úroveň zabezpečení. V souladu s českými a mezinárodními standardy jsou ústředny a detektory PARADOX určeny pro třídu 2 (nízká a střední rizika) a pro třídu 3. (střední a vysoká rizika).

Plně modulární technologie, zajišťuje maximální přizpůsobení konkrétním požadavkům aplikace a možnost inovace. Plná integrace zabezpečovacího a přístupového systému, umožňuje mnoho dalších funkcí, jako je ovládání zabezpečení přístupovými kartami, monitorování dveří zabezpečovacím systémem, řízení výstupů na základě libovolné události nebo událostí (např. pro řízení osvětlení, klimatizace, topení atd.) a ukládání všech událostí do historie systému pro pozdější vyhledávání. Bezdrátová nástavba MAGELLAN umožňuje připojení bezdrátových detektorů nebo bezdrátové ovládání systému. Systém lze také dálkově ovládat pomocí telefonu s tónovou volbou, kterým se mohou nastavovat a odstavovat jednotlivé skupiny nebo ovládat výstupy (např. garážová vrata). Podpora komfortní obsluhy systému také ovládat a monitorovat pomocí speciálních programů z PC.



Obr. 28. Zabezpečovací systém PARADOX [21]

Dalším přírůstkem od výrobce PARADOX nové koncepce zabezpečení je ucelený systém domácí automatizace, řízení přístupu, zabezpečení s názvem IMPERIAL. Systém využívá nejnovější komunikační technologie v kombinaci s uživatelsky jednoduchým nastavením, údržbou a provozem.

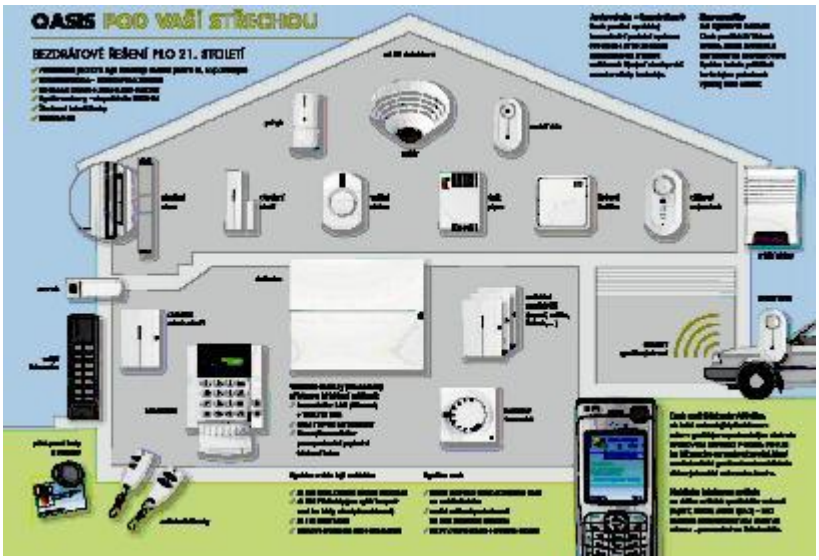


Obr. 29. Ovládací ústředna pro ovládání a programování systému IMPERIAL [22]

Systém IMPERIAL využívá program **BabyWare**, který je určený pro technika i uživatele zabezpečovacího systému. Umožňuje bezpečné a komfortní programování, servis a obsluhu zabezpečovacího systému.

Systém Oasis od českého výrobce Jablotron Alarms a.s. je profesionálním poplachovým zabezpečovacím systémem, který se dokáže přizpůsobit přesně požadavkům zákazníka. Jablotron Alarms a.s. je jedničkou na trhu především v produkci a vývoji bezdrátových zabezpečovacích systémů. Jeho výhoda je zřejmá, je to rychlá a levná instalace, možnost přemístění bezdrátových prvků, je to prakticky jediná možnost ve stávajících objektech, kde je použití kabelů vyloučené (estetické důvody, bourání, sekání). Bezdrátový systém lze jednoduše rozšířit a vzhledem k velkému dosahu lze zabezpečit i budovy vzdálené až několik set metrů. Systém Oasis umožňuje své ovládání dálkově mobilním telefonem nebo přes internet. Umožňuje takové funkce, jako odesílání upozornění jako zavření oken či dveří při odchodu z domu nebo firmy. Služby jako zapínání osvětlení, ventilátorů při průchodu kolem detektoru pohybu. Okenní detektor střeží plášť objektu, ale při větráni může také tento detektor vypnout okruh topení. Se zajištěním zabezpečovacího systému se mohou vypnout některé spotřebiče. O všem, co se domácnosti nebo firmě děje, má uživatel neustále

přehled prostřednictvím svého mobilu či internetu. Všechna tato hlášení událostí ze zabezpečeného prostoru můžou samozřejmě odcházet také na bezpečnostní agenturu, která v případě vloupání nebo třeba požáru zajistí okamžitý profesionální zásah přímo na místě.



Obr. 30. Schéma využití zabezpečovacího systému OASIS [23]

Požadavkem kladeným na dnešní monitorovací systémy je i spolehlivost těchto systémů. To znamená, že i na příslušný monitorovací program jsou kladeny nároky spočívající ve spolehlivosti a funkčnosti monitorování, například během výpadku centrální dohledové aplikace z důvodu výpadku elektřiny, nebo havárie PC, na kterém běží centrální monitorovací aplikace. Tuto funkčnost si zajišťují příslušné hlídací firmy individuálně a to např. pro případ výpadku energie záložními zdroji UPS15 a pro případ havárie PC s monitorovacím programem je tento program spuštěn na více nezávislých PC v centrále hlídací služby. Zároveň je v zájmu hlídacích agentur provádět pravidelné zálohování přijímaných dat a tím předcházet ztrátě dat. Tato činnost zvyšuje samotnou spolehlivost. Výpadek energie nebo havárie PC v monitorovacím centru nemá přímý vliv na poplachové zabezpečovací systémy ve střeženém objektu. Tyto systémy běží i nadále, jen by se mohlo stát, že při nevybavenosti dohledového centra záložními zdroji, případně nespuštění monitorovacího programu na více sobě nezávislých PC, by ostraha zůstala tzv. „slepá“. To znamená, že pracovníci ostrahy by nevěděli o stavech střežených objektů. Pro případ výpadku PZS a jeho jakékoliv části (např. požární hlásiče, rádiový přijímač, detektor) je

[15] UPS – záložní zdroj energie - zajišťuje souvislou dodávku elektřiny pro zařízení

dnešním trendem schopnost těchto monitorovacích systémů ihned hlásit případnou poruchu této části PZS monitorovacímu softwaru, aby tuto situaci dokázala ostraha pružně řešit.

V současné době je mimo jiné kladen velký důraz na pracovníky obsluhující PCO, kteří pracují se spuštěnými monitorovacími programy. Se stále se zvyšující integrací různých systémů ve střežených objektech dochází přímou úměrou ke zvyšování složitosti a množství příchozích hlášení, stavů a nutnosti hledat nejvhodnější řešení. Z toho plyne, že na obslužný personál těchto monitorovacích center jsou kladeny velké nároky a požadavky na schopnosti vzniklé situace řešit.

Velkým faktorem ovlivňujícím vývojové trendy v oblasti použití monitorovacích softwarů je bezesporu trend vývoje nových technologií a následná snaha tyto nové technologie použit v samotných poplachových zabezpečovacích systémech. Budoucnost je čím dál tím více směřována k integraci poplachových a nepoplachových aplikací. Vývoj hardwarové a softwarové integrace bude především záviset na společnostech, které se zabývají realizací projektů s využitím integrace. Pokud dodavatelé budou mít snahu využívat více typů zařízení a kompletovat projekty cestou softwarové integrace, donutí výrobce věnovat více času na vývoj univerzálnějších komunikačních prostředků. Výsledkem by byla snaha o co možná nejdokonalejší software schopný automaticky rozpoznat a integrovat co nejvíce typů zařízení nabízených na trhu. V dnešní době mezi technologie, které se začínají dostávat do popředí, patří např. technologie bezdrátového přenosu, a to nejen mezi samotnou poplachovou ústřednou a PCO, ale i mezi jednotlivými prvky poplachového zabezpečovacího systému. Mezi další takové technologie můžeme zařadit technologii dotykových displejů a obrazovek, která již taky nachází uplatnění v tomto oboru. Dále rozvoj samotných poplachových zabezpečovacích systémů o technologie biometrického rozeznávání osob, rozeznávání státních poznávacích značek aut, digitální analýza obrazu, dálkové ovládání tónovou volbou (hlasové) atd. Všechny tyto technologie směřují ke zdokonalování všech systémů a tím k dokonalejšímu zabezpečení střežených budov. V konečném výsledku tyto technologie použité v bezpečnostních systémech slouží hlavně ke snížení škod způsobených ať už člověkem nebo přírodou.

ZÁVĚR

Pokud se podíváme na všechny popisované monitorovací softwary, tak v současné době jsou tyto programy uživatelsky velmi příjemné na obsluhu. Při výběru softwaru uživatelem jsou na vlastnosti jako jednoduchost obsluhy, přehlednost, seznam monitorovaných míst, paměť událostí apod. kladeny velké nároky, a proto jsou u vývojářů monitorovacích softwarů řazeny na první místo. Mezi další takové požadavky patří možnost integrace více různých systémů ve střeženém objektu a jejich sledování. Obsluha těchto systémů by neměla mít nějak zvlášť velký problém s identifikací jednotlivých hlášení a následnou rychlou reakcí k přijetí příslušného opatření na případný poplach. V současné době je stále více rozšířen pojem „Inteligentní budova“ a její možnost řízení a sledování. Z realizací těchto budov plynou další požadavky k využití monitorovacího systému ve více oblastech, než jen v poplachových zabezpečovacích systémech. Tento požadavek možnosti integrace více různých systémů ve střeženém objektu a jejich sledování nesplňují všechny sledované monitorovací programy. Programy AlVis a INTEGRA 3 jsou ideálními kandidáty k využití, jak v rozsáhlých komplexech, tak v inteligentních budovách Naopak program PersonLocator vzhledem k tomu, že je primárně určen ke sledování pohybu osob a věcí, tak nelze od něj očekávat schopnost plnit funkce jako např. střežení, spuštění klimatizace, regulace osvětlení apod., ve střežených objektech. Programy SIMS, VAR-NET a TEGAL jsou využívány především pro monitoring poplachových aplikací (PZS, EPS). Schopnost monitorovat a řídit nepoplachové aplikace v objektech u těchto softwarů je omezená nebo zcela chybí.

U všech popisovaných monitorovacích bezpečnostních softwarů je využíváno v zásadě jednotného stylu zobrazení, který spočívá v jednom dialogovém okně rozděleném na více částí. Počet částí, styl zobrazení těchto částí v dialogovém okně, obsah těchto oken se liší. U každého monitorovacího programu je kladen důraz na jiné aktuální zobrazení pro pracovníky dohledového centra. Samozřejmostí těchto softwarů je možnost si uživatelem toto zobrazení přizpůsobit k obrazu svému. Avšak pro všechny monitorovací programy platí jedna zásada - **každá funkce jakékoliv aplikace nesmí bránit signalizaci poplachu!!!**

Bezpečnost objektů je a zcela jistě bude stále důležitým oborem, který se neustále vyvíjí a zdokonaluje. Díky rychlému vývoji technologií a novým možnostem techniky se otevírají další a další příležitosti pro zdokonalování systémů. Zvyšuje se tlak ze strany uživatele na stále vyšší účinnost těchto systémů a také požadavky na stále vyšší komfort pro uživatele. Na společnosti zabývající se vývojem a instalací bezpečnostních technologií jsou kladeny vyšší nároky týkající se znalosti nových trendů, znalosti nových oborů, které se postupně k zabezpečovací technice postupem doby připojují a jsou nedílnou součástí bezpečného objektu. Vývoj software i hardware umožňuje firmám pružně reagovat na aktuální požadavky vyplývající z nových situací, které uživatel vytváří. Větší budovy nebo komplexy budov se zcela jistě díky stále složitějším technologiím neobejdou **bez podpory přehledného grafického prostředí** a bez vzájemného propojení těchto technologií mezi sebou nelze účinně provozovat „život“ těchto budov.

ZÁVĚR V ANGLIČTINĚ

If we look at all the described monitoring software, and currently these programs are very user friendly to use. When selecting software, the user is on the property as simplicity, clarity, a list of monitored sites, event memory, etc. placed great demands and, therefore, the monitoring software developers ranked the first place. Among other such requirements include the possibility of integrating multiple systems in guarding and monitoring. Operation of these systems would not be terribly big problem with the identification of individual reports and quick reaction to the adoption of appropriate measures for any alarm. Currently, the increasingly widespread notion of "intelligent buildings" and the possibility of management and monitoring. The implementation of these buildings derive additional requirements for use of the monitoring system in more areas than just the security alarm systems. This requirement is the possibility of integrating multiple systems in guarding and monitoring do not all follow the monitoring programs. Programs Alvis and INTEGRA 3 are ideal candidates for use in both large complexes and buildings in intelligent contrast PersonLocator program since it is primarily intended to monitor the movement of persons and things, so not to expect the ability to perform functions such as surveillance, run air-conditioning, lighting control, etc., in guarded buildings. SIMS, VAR-NET and Tegal are used primarily for alarm monitoring applications (OPT, EPS). The ability to monitor and control applications in buildings unwarning these software is limited or missing.

The ability to monitor and control applications in buildings these software is limited or missing. For all described security monitoring software is used in essentially a single-style display, which consists of a single dialog box, divided into several parts. The number of parts, these parts of the visual style of the dialog box, the contents of these windows are different. For each of the monitoring program, emphasis is placed on display for other current staff supervision center. Of course the software is free to customize this view by his own image. However, for all monitoring programs apply one principle - **every function of any application may prevent the alarm function!!!**

Security objects, and certainly will become an important field that is constantly evolving and improving. With rapid technological developments and new possibilities technology opens more and more opportunities for improving systems. Increasing pressure from users on increasing the efficiency of these systems and also demands an ever greater comfort. Companies engaged in the development and installation of safety technologies are subject to higher demands on the knowledge of new trends, new fields of knowledge, which is gradually to a security technology over time and are connected integral part of the secure facility. Development of software and hardware, enables companies to flexibly respond to current requirements arising from new situations, the user creates..

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] KŘEČEK, Stanislav a kolektiv; *Příručka zabezpečovací techniky*. Blatná: Blatenská tiskárna, s.r.o., 2006. 158 s. ISBN 80 – 902938 – 2 – 4. s. 5

[4] JUDr. UHLÁŘ, Jan; *Technická ochrana objektů II. díl*. 2. vyd. Praha: Policejní akademie České republiky, 2009. 232 s. ISBN 978 – 80 – 7251 – 313 – 0. s. 143

Internetové zdroje:

[2] *Monitorovací SW NET-G* [online]. 2011 [cit. 2011-05-14]. Dostupné z WWW: <http://www.nam.cz/texts.asp?category=15&sub=4>.

[3] *The Fire Alarm Telegraph* [online]. 2011 [cit. 2011-05-14]. Dostupné z WWW: <http://www.firehallmuseum.org/fire_alarm_telegraph/firealrm.htm>.

[5] *Muzeum* [online]. 2011 [cit. 2011-03-11]. Dostupné z WWW: <http://www.i-servis.cz/znalec/muzeum.htm>.

[6] *Zásady provozování kamerového systému z hlediska zákona o ochraně osobních údajů* [online]. 2011 [cit. 2011-05-14]. Dostupné z WWW: <http://www.jopos.cz/cctv/zasady.php>.

[7] *Základní i nformace o kamerových systémech* [online]. 2011 [cit. 2011-01-18]. Dostupné z WWW: <http://www.orisplus.cz/kamerove-systemy-zakladni-udaje>.

[8] *TEGAL - grafický monitorovací a terminálový program s vyhodnocením docházky* [online]. 2011 [cit. 2011-02-02]. Dostupné z WWW: <http://www.adiglobal.cz/iiWWW/docs.nsf/all/457B949CCA91B33CC12574110000D529/$FILE/KL_Tegal_v5_cz_oc.pdf>.

[9] *TEGAL 5.0 - Uživatelský manuál* [online]. 2011 [cit. 2011-02-02]. Dostupné z WWW: <http://www.adiglobal.cz/iiWWW/docs.nsf/all/4EEED42C8A770CC9C12574110000D5A7/$FILE/UM_Tegal_5_cz_oc.pdf>.

[10] *ADI-OLYMPO - programová řešení pro řízení a monitoring* [online]. 2011 [cit. 2011-03-04]. Dostupné z WWW: <http://www.adiglobal.cz/iiWWW/cz/Produkty110.nsf/wp/katalogy/$file/kl_alvis_www.pdf>.

[11] *Alvis WEB 3.2* [online]. 2011 [cit. 2011-03-10]. Dostupné z WWW: <http://www.adiglobal.cz/iiWWW/cz/Produkty110.nsf/wp/katalogy/$file/kl_alvis32_web.pdf>.

[12] *Alvis 3.2* [online]. 2011 [cit. 2011-03-21]. Dostupné z WWW: <http://www.adiglobal.cz/iiWWW/cz/Produkty110.nsf/wp/katalogy/$file/kl_alvis32_4s.pdf>.

[13] *Integra 3 – jednotné řízení všech bezpečnostních technologií v organizaci* [online]. 2011 [cit. 2011-05-14]. Dostupné z WWW: <http://businessworld.cz/it-strategie/integra-3-jednotne-rizeni-vsech-bezpecnostnich-technologii-v-organizaci-7019>.

[14] *Nová generace systému pro správu podnikové bezpečnosti* [online]. 2011 [cit. 2011-04-04]. Dostupné z WWW: <http://www.integoo.cz/sites/default/files/letak_integoo_integra_web.pdf>.

[15] *VAR-NET INTEGRAL* [online]. 2011 [cit. 2011-04-04]. Dostupné z WWW: <http://www.variant.cz/sekce231-var-net-integral.html>.

[16] *PersonLocator* [online]. 2011 [cit. 2011-04-14]. Dostupné z WWW: <http://www.7md.cz/docs/person-locator-wireless/Datasheet_Person_Locator.pdf>.

[17] *Kamerové systémy* [online]. 2011 [cit. 2011-04-11]. Dostupné z WWW: <http://www.delta-plzen.cz/elektricke-zabezpecovaci-systemy/kamerove-systemy/>.

[18] *Docházkový systém* [online]. 2011 [cit. 2011-05-14]. Dostupné z WWW: <http://www.amsyscz.cz/Produktyaslužby/Docházkovýsystém/tabid/74/language/cs-CZ/Default.aspx>.

[19] *Inteligentní budova* [online]. 2011 [cit. 2011-04-25]. Dostupné z WWW: <http://www.tzb-info.cz/1143-inteligentni-budova-i>.

[20] *AMX – inteligentní dům* [online]. 2011 [cit. 2011-04-25]. Dostupné z WWW: <http://www.digitalnidomacnost.cz/amx-inteligentni-dum/>.

[21] *PARADOX zabezpečovací systémy* [online]. 2011 [cit. 2011-05-14]. Dostupné z WWW: <http://www.besys.cz/dokumentace/paradox.pdf>.

[22] *IMPERIAL* [online]. 2011 [cit. 2011-05-1]. Dostupné z WWW: <http://www.eurosat.cz/3875-imperial.html>.

[23] *Bezdrátový zabezpečovací systém Jablotron OASIS* [online]. 2011 [cit. 2011-05-14]. Dostupné z WWW: <http://www.acesys.cz/jablotron-oasis.html>.

SEZNAM POUŽITÝCH VÝRAZŮ A ZKRATEK

ACS	Přístupový systém
APS	Automatický parkovací systém
CCTV	Uzavřený kamerový systém
ČR	Česká republika
ČSN	Česká státní norma
DVR	Digitální videorekordér
EKV	Elektrická kontrola vstupu
EN	Evropská norma
EPS	Elektrická požární signalizace
GPRS	Technologie bezdrátového přenosu dat
HDD	Pevný disk
IP	Internetový protokol
IT	Informační technologi
LAN	Local Area Network – lokální počítačová síť
LZPS	Listina základních práv a svobod
PCO	Pult centralizované ochrany objektů
PZS	Poplachový zabezpečovací systém
SMS	Služba krátkých textových zpráv
TCP/IP	Protokolová architektura definovaná sadou protokolů pro komunikaci v počítačové síti
UPS	záložní zdroj energie - zajišťuje souvislou dodávku elektřiny pro zařízení, která nesmějí být neočekávaně vypnuta
VHS	Systém domácího videa

SEZNAM OBRÁZKŮ

SEZNAM TABULEK