Dohledová poplachová přijímací centra

A Supervisory Alarm Receiving Centre

Bc. František Navrátil

Diplomová práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

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

Jméno a příjmení:	**Bc. František Navrátil**
Osobní číslo:	**A13351**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Dohledová poplachová přijímací centra**
Téma anglicky:	**A Supervisory Alarm Receiving Centre**

Zásady pro vypracování:

1. **Analyzujte legislativní požadavky na poplachové systémy.**
2. **Popište možnosti integrace dílčích poplachových systémů.**
3. **Proveďte analýzu integračních platforem.**
4. **Stanovte modelová řešení návrhů integrovaných poplachových systémů.**
5. **Zhotovte komparační studii modelových návrhů integrovaných poplachových systémů.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **VALOUCH, Jan. Projektování integrovaných systémů. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj (152 s.). ISBN 978-80-7454-296-1.**
2. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I.: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2011. ISBN 978-808-7500-057.**
3. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management III.: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2013. ISBN 978-808-7500-354.**
4. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV.: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2014. ISBN 978-808-7500-576.**
5. **ČSN CLC/TS 50398. Poplachové systémy Kombinované a integrované systémy Všeobecné požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. 20s. Třídící znak 334597.**
6. **ČSN CLC/TS 50131-1 Poplachové systémy Poplachové zabezpečovací a tísňové systémy, Část 1: Systémové požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2007. 40s. Třídící znak 334591.**
7. **ČSN EN 50132-1 Poplachové systémy CCTV sledovací systémy pro použití v bezpečnostních aplikacích, Část 1: Systémové požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. 40s. Třídící znak 334592.**

Vedoucí diplomové práce: **Ing. Rudolf Drga, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **12. ledna 2015**

Termín odevzdání diplomové práce: **15. května 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně 25. 5. 2015

.....
podpis diplomanta

ABSTRAKT

Předmětem diplomové práce je analýza legislativních požadavků kladených na jednotlivé poplachové systémy při jejich vzájemné integraci. Postupně jsou rozebírány způsoby a možnosti integrace jednotlivých systémů a provedena analýza integračních platforem již existujících bezpečnostních systémů. V souladu zákonných a normativních požadavcích jsou stanoveny modelová řešení návrhů integrovaných bezpečnostních systémů a provedena komparační studie obsahující doporučení k typizovaným řešením v závislosti dle rozsahu aplikace.

Klíčová slova:

poplachové aplikace, integrace, integrační platformy, integrované bezpečnostní systémy.

ABSTRACT

The subject of this thesis is an analysis of legislative requirements for individual alarm systems in their mutual integration. Gradually, there are discussed ways and means of integrated various systems and the analysis of integration of platforms in already existing security systems. In accordance with legal and regulatory requirements are specified model design solutions, integrated security systems and a comparative study with recommendations. Typified solution varies depending upon the scope of application.

Keywords:

alarm applications, integration, integration platform, integrated security systems.

Mé poděkování patří vedoucímu diplomové práce panu Ing. Drgovi, Ph.D. za umožnění vypracování absolventské práce a především mému odbornému konzultantovi Ing. Jiřímu Ševčíkovi za cenné rady a věcné připomínky, které mi pomohly tuto práci zkompletovat. Rád bych také touto cestou vyjádřil svou vděčnost své rodině a lidem, kteří mě jakýmkoliv způsobem podporovali během celého studia na VŠ.

„*Musíš se mnoho učit, abys poznal, že málo víš.*“

Michel de Montaigne

OBSAH

ÚVOD

Trend současnosti spočívá ve spojování různých technologií ve vyšší celek. Motivací uceleného řešení je jednoznačně nárůst různých technických vymožeností a potřeba tak sjednotit a zefektivnit uživatelský přístup k nim. Jako příklad lze použít smart technologie disponující velkým potenciálem do budoucnosti vlivem připojení do celosvětové internetovské sítě. Tento směr vývoje, spočívající ve splynutí a sjednocení informačního toku z různých zdrojů do jednoho uživatelského prostředí, byl zaznamenán i v oblasti bezpečnostních poplachových systémech a to zejména v dohledových a přijímacích centrech. Dříve bylo vybavení center striktně normalizováno jednak vlivem omezené nabídky bezpečnostních systémů a také tím, že provoz těchto zařízení bylo pouze v rukou státních bezpečnostních složek. Unifikace se taktéž týkala připojení systémů jen o specifických vlastnostech. Na trhu se dnes již objevuje celá řada výrobců a distributorů nabízející pestrou nabídku systémů a zařízení rozdílných typů i principů, podporující různé komunikační rozhraní či standardy. Základem spojování, taktéž integrace, by vždycky měla být účelně navržená architektura, zaměřená především na podporu konkrétních požadovaných procesů a činností. Integračnímu procesu by však měla předcházet také důkladně provedená analýza s následnou syntézou dostupných prostředků a nástrojů zastřešující samotné ucelené řešení, složené ze vzájemně provázaných prvků. Jednotlivé návrhy by taktéž měli být provedeny v souladu s legislativními požadavky a to hlavně normativních v dané aplikační sféře. S procesem spojování ve vyšší celek úzce souvisí vývoj otevřených platforem a standardů, které splynutí různorodých technologií značně napomáhá. Důvody provedení integrace, ať už v jakémkoliv specializovaném odvětví, jsou jednoznačné. Jde především o zvýšení efektivity, stability, přehlednosti, bezpečnosti a v neposlední řadě o snížení provozních nákladů výsledného procesu, zařízení nebo systému. Tato diplomová práce se ve svých kapitolách bude zabývat jednotlivými okruhy problematiky, předcházející skutečné realizaci integrovaného poplachového bezpečnostního systému. Na dohledová poplachová přijímací centra bude nahlíženo z pohledu výběru a nasazení softwarových integračních platforem dodavatelem služby, který je zároveň systémovým integrátorem.

I. TEORETICKÁ ČÁST

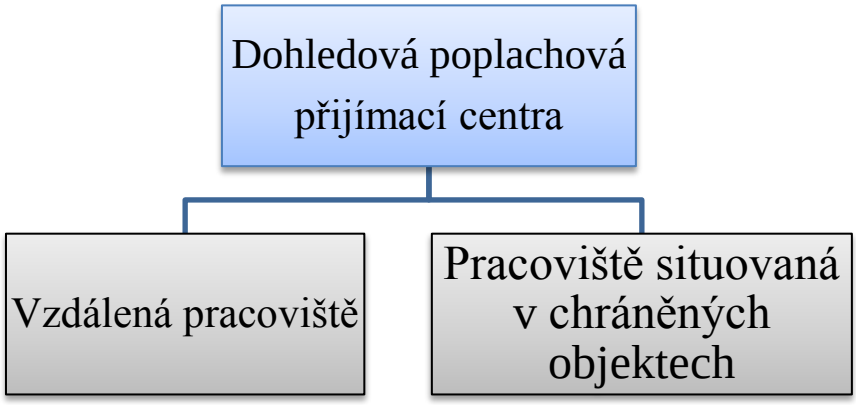
1 LEGISLATIVNÍ POŽADAVKY NA INTEGRACI POPLACHOVÝCH SYSTÉMŮ

Úvodní kapitola upřesňuje význam a typy dohledových a poplachových přijímacích center v rámci ochrany majetku a osob, vyjmenovává jednotlivé poplachové aplikace a systémy, které mohou být připojeny na tento centrální vyhodnocovací a monitorovací prostředek.

Následující části se týkají zákonných, podzákonných a především normativních předpisů, které popisují stanovené požadavky na kombinované a integrované poplachové systémy. Souhrnně jsou popsány i nezbytnosti, které jsou kladeny na integraci jednotlivých bezpečnostních systémů (PZTS, CCTV, ACS a EPS) do jednoho funkčního celku, tedy do integrovaného poplachového systému.

1.1 Dohledová a poplachová přijímací centra

Dohledová a poplachová přijímací centra (dále jen DPPC), můžeme charakterizovat jako nástroj pro příjem, zobrazení, vyhodnocení a reprodukci informací o stavu chráněného objektu nebo jeho části s možností následné adekvátní zpětné reakce. Mezi základní součástí DPPC je hardwarové vybavení, softwarové nástroje a samozřejmě také fyzická obsluha jednající v souladu se stanovenou metodikou efektivního zásahu. V dřívější době byl pojem „pult centrální ochrany“ (původní název dohledového a poplachového přijímacího centra), chápán pouze jako vzdálené pracoviště pro příjem zpráv o narušení, poruše, popřípadě ztráty spojení apod. a k organizaci zásahu. Vlivem rozvíjejícího se podnikání, narůstajícího soukromého majetku a hlavně pro zvýšení efektivity a přehlednosti při střežení a monitorování velkých objektů či komplexů budov se přijímací centra také budují přímo v chráněných objektech i jako součásti vrátnic nebo recepcí. Tento typ řešení dohledu nad objektem, má kromě již zmíněných výhod, přednosti v možnostech přenášet více informací a to z vícera systémů, ať už poplachového nebo nepoplachového rázu aplikace. Přednost realizace DPPC situovaného přímo v chráněném objektu oproti vzdálenému pracovišti spočívá v přenosu dat jen z jednoho objektu oproti stovkám až tisícům objektů, na které je vzdálené pracoviště připojeno. [1]



Obr. 1: Základní členění DPPC

Výhody pracoviště DPPC situovaného přímo v chráněném objektu nebo v komplexu budov jsou:

- lepší přehlednost, efektivita a vizualizace objektu,
- možnost přenášet více informací z různých systémů v objektu,
- aplikace integrovaných a kombinovaných systémů,
- absence přenosových cest zřizované a spravované soukromými firmami,
- a unifikace rozhraní mezi jednotlivými systémy.

Mezi poplachové aplikace, které se podílejí na zvýšení bezpečnosti a snížení bezpečnostních rizik v budovách, a jsou předmětem možného integrování v jeden celek do DPPC přednostně patří:

1. poplachové zabezpečovací a tísňové systémy (PZTS),
2. kamerové dohledové systémy (CCTV),
3. systémy kontroly vstupů (SKV) a
4. elektrická požární signalizace (EPS).

1.2 Všeobecné požadavky na kombinované a integrované poplachové systémy

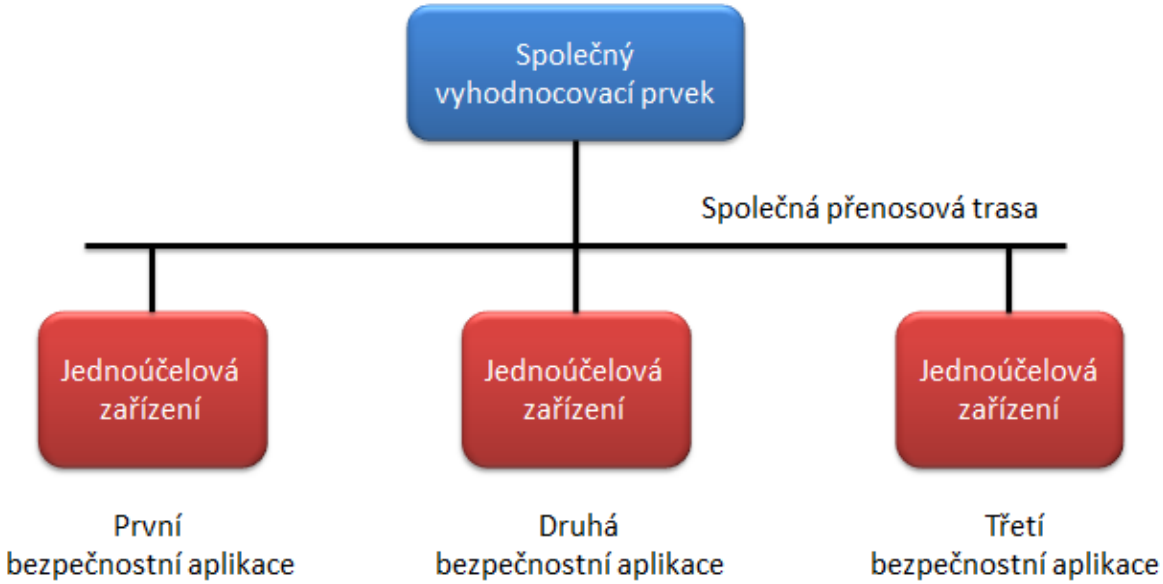
Všeobecné normativní požadavky na integraci poplachových systémů jsou popsány v technickém předpisu: ČSN CLC/TS 50398 Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky. Tento dokument je jediný předpis přímo týkající se integrace a je označován jako základní technická norma v oblasti IPS. V první řadě stanovuje obecnou definici integrovaného poplachového systému: „*Systém mající jedno nebo více společných zařízení, alespoň jedním z nichž je poplachová aplikace.*“ [str.9, 2] Dále udává obecné požadavky s odkazy na použití příslušných norem týkající se každé konkrétní poplachové aplikace. [2]

V rámci tohoto normativního předpisu lze IPS specifikovat celkem do tří různých typů neboli konfigurací. Rozdíl mezi jednotlivými konfiguracemi je v použití jednoúčelových zařízení, přenosových tras, společných zařízení a společného vybavení.

- Typ 1 je normou charakterizován pro použití integrace jen jednoúčelových poplachových i nepoplachových systémů. Jednoúčelové systémy jsou dále připojeny ke společnému doplňkovému zařízení, které zprostředkovává integritu a k jednotlivým systémům je připojen prostřednictvím doplňkové přenosové trasy. Současně platí, že zařízení uváděno v této konfiguraci, nesmí být nepříznivě ovlivňováno dalšími jednoúčelovými systémy ani doplňkovými zařízeními a to v kterémkoliv provozním stavu.
- Typ 2 oproti předchozímu typu je aplikovatelný na integrované systémy, jež pro svoji činnost používají společné přenosové trasy, společná zařízení a vybavení. Dále se Typ 2 dělí na podtypy 2A a 2B podle toho, zda případně vzniklá porucha v kterékoliv jedné aplikaci nemá žádný negativní účinek (Typ 2A), anebo může mít negativní účinek (Typ 2B) na jinou jakoukoliv další poplachovou aplikaci. Pro oba typy však platí, že porucha společného zařízení musí být signalizována v aplikacích, která sdílejí společná zařízení.

Pro orientaci a přehlednost jsou konfigurace Typu 1 a 2 znázorněny na schématech níže.

Obr. 2: Schéma konfigurace typu 1 [2]



Obr. 3: Schéma konfigurace typu 2 [2]

Norma dále klasifikuje dvě třídy tzv. centrálních ovládacích zařízení (normou označováno jako CCF). Jde o doplňkové zařízení, např.: počítač v dozorovém pracovišti, které je pou-

žívané k ovládání popř. řízení nebo signalizaci a je připojené k jednomu nebo k více jednoúčelovým systémům. CCF je obvykle obsluhováno vyškoleným personálem a není součástí běžných ústředen poplachových zabezpečovacích systémů.

Třída 1: centrální ovládací zařízení, uváděné do třídy 1, může být použito pouze k zobrazení informací a to v prostorách, kde na systém dohlíží obsluha IPS. A zároveň ústředny PZTS nebo signalizační panely, které jsou normou vyžadované jako signalizační zařízení, musí být taktéž umístěny ve stejných prostorách jako zařízení CCF. V případě poruchy CCF klasifikované v třídě 1 bude poplach zaregistrován obsluhou vizuálně ze signalizačního panelu PZTS.

Třída 2: centrální ovládací zařízení, spadající do třídy 2, je jediným zařízením k zobrazování informací a tím pádem je to jediný informační display v dozorovém pracovišti, ze kterého se obsluha dozvídá o stavu systému. Jestliže CCF umožnuje kromě zobrazování informací i prostředky pro nastavení vlastností systému, uvádění do střežení/odstřežení apod., musí být navrženo tak, aby bylo plně v souladu s jednotlivými aplikačními normami a je uváděno jako integrovaný systém typu 2.

Průběh provozu CCF ve třídě 2 musí být monitorován a případná porucha musí být signalizována. Monitorování činnosti musí zahrnovat i samotnou monitorovací funkci s detekcí a signalizování výpadku monitorovací sekvence. Normativní předpis počítá s tím, že zařízení CCF obvykle není normalizované zařízení a proto by měl existovat specifický postup pro případ poruchy uvádějící minimálně to, jak se dostat k jednotlivým ústřednám popř. ovládacím prvkům ústředen a jak je ovládat. Samozřejmostí je také signalizace stavu napájení a záložní zdroj pro dobu potřebnou k vykonání nezbytných postupů při poruše hlavního napájení.

Signalizace informací v IPS musí být provedena v pořadí priorit jednoznačným způsobem a to v ohledu na aplikované typy poplachových systémů. Všeobecně norma uvádí pořadí priorit, které je doporučené avšak pro různé realizace nevhodné, popřípadě současná přítomnost více typů zpráv může vést k jiné zobrazené prioritě. Obecně by tedy mělo být použito šest priorit signalizací:

1. priorita zahrnující poplachové signály ze systémů k ochraně života a zdraví při požárním poplachu nebo i při napadení.
2. priorita týkající se taktéž poplachových signálů vztahujících se k ochraně majetku, nebo ochraně proti nedovolenému vniknutí do chráněných prostor.
3. priorita, kde jsou zařazeny další poplachové signály z ostatních systémů.
4. priorita signalizující stavy o poruchách v systémech k ochraně života a majetku.
5. priorita signalizující stavy o poruchách z ostatních poplachových systémů.
6. priorita zahrnující ostatní informace z ostatních nepoplachových systémů. [2]

V návaznosti na výše stanovené priority pak existují požadavky na signalizaci, které uvádějí, že jakákoliv činnost aplikace nesmí zamezovat indikaci poplachu a současně jestli vzniklo více poplachů z více než jedné aplikace, musí být tato událost signalizována. Kromě aktuálně zobrazených informací by měly být k dispozici taktéž doplňkové informace, avšak při vyobrazení doplňkových informací musí být zachována viditelnost aktuálních prioritních informací.

1.3 Poplachové zabezpečovací a tísňové systémy

Poplachový zabezpečovací systém ve své podstatě slouží k detekování přítomnosti nebo vniknutí popřípadě pokusu o vniknutí pachatele do předem definovaného chráněného prostoru nebo objektu. Poplachový zabezpečovací a tísňový systém pak představuje kombinovaný systém, určený jak k detekci poplachu narušení, tak i k signalizaci tísňového poplachu například při vyhlášení tzv. tichého poplachu osobou při přepadení nebo při zdravotních potížích. V praxi se k systému občas připojují i prvky k lokální detekci požárního nebezpečí, popřípadě prvky k detekci zaplavení nebo úniku nebezpečných látek. Takto vytvořený kombinovaný systém však není považován za systém integrovaný. [3]

1.3.1 Požadavky na poplachové zabezpečovací a tísňové systémy

Normativní požadavky na systémy PZTS v ohledu na integraci vycházejí především z normy ČSN EN 50 131-1 ed.2, která je souhrnně stanovuje na systémové úrovni. Z tohoto předpisu lze v návaznosti na IPS vyčíst především následující informace. [4]

1. Veškeré komponenty systému PZTS musí být navzájem kompatibilní, musí být zvoleny v souladu s třídou prostředí a stanoveným stupněm zabezpečení.
2. Komponenty pocházející z jiných bezpečnostních aplikací mohou být integrovány s prvky PZTS avšak pouze za předpokladu, že nedojde k nežádoucímu ovlivňování vlastností komponentů PZTS.
3. Jakékoliv ovládací prvky musí být uspořádány logicky a nezaměnitelně tak, aby byla minimalizována pravděpodobnost nesprávné obsluhy.
4. Norma stanovuje, k jakým indikacím musí dojít v závislosti na stupni zabezpečení a také to, že tyto povinné indikace musí být umístěny společně na ústředně systému PZTS nebo na doplňkovém ovládacím zařízení. Pod pojmem doplňková ovládací zařízení se rozumí klávesnice, biometrický prvek nebo čtečka karet systému SKV, kterým lze ovládat systém PZTS.
5. Indikaci vzniknutou systémem PZTS nelze zrušit, pokud nebude odstraněna příčina, která tuto indikaci způsobila.
6. Doplňkové ovládací zařízení, stejně jako prvky PZTS, musí obsahovat prostředky pro detekci sabotáže a zároveň jejich kryty musí být provedeny robustně tak, aby nemohlo dojít k přístupu k jejím vnitřním prvkům bez zjevného poškození.
7. Propojení mezi jednotlivými komponenty systému musí být navrženo s ohledem na minimalizování možnosti, že dojde ke zpožďování, modifikace nebo ztrátě signálů nebo zpráv a zároveň propojení mezi systémy musí být monitorováno.
8. Při normálním provozu musí být signál nebo zpráva ze zdroje doručena do určeného prvku do 10 sekund.
9. V požadavcích ohledně provozní spolehlivosti je psáno, že v systému musí být aplikovány prostředky, které zajistí, aby případné chyby vzniklé nesprávnou obsluhou, jež by mohly negativně ovlivnit normální činnost PZTS, byly indikovány nebo nejlépe zcela vyloučeny.

Dle norem lze do systému PZTS integrovat i komponenty, pro které neexistují žádné technické normativní předpisy. Stále však musí platit obecné požadavky na kompatibilitu, požadavky na zpracování signálu a funkčnost systému. Celkový stupeň zabezpečení pak odpovídá prvku s nejnižším stupněm zabezpečení, u kterého byl stupeň stano-

ven. V dokumentaci ke komponentům PZTS musí být k dispozici dostatečné informace popisující integraci každého prvku s ostatními prvky systému.

1.4 Kamerové dohledové systémy

Kamerový dohledový systém pro použití v bezpečnostních aplikacích můžeme charakterizovat jako technický prostředek pro ochranu majetku a osob sledování zájmového prostoru v reálném čase. Sledování a následné vyhodnocování záběrů je umožněno s využitím prvků, ze kterých je systém složen: z kamer (kamerových jednotek), datového média, monitorovacího zařízení a přidružených zařízení použitých pro přenos dat a ovládání. Nedílnou součástí systému je i ovládací software aplikovaný pro sledování, nastavování, správu, vyhledávání v záznamech, archivaci a zálohování dat atd. Komplexně lze takovýto bezpečnostní systém chápat jako nástroj pro sledování, verifikaci příčiny vzniklého poplachu, rekonstrukci bezpečnostní situace. Kamerové systémy lze využít i pro účely sledování a vyhodnocování technologických postupů ve výrobním procesu, ke kontrole dodržování bezpečnostní předpisů a nařízení (BOZP), ale i ke kontrole pohybu vozidel s možností zaznamenání SPZ a následného porovnání s údaji uloženými v databázovém systému. Doposud zažité a hojně používané označení CCTV, v překladu z anglického originálu: uzavřený kamerový okruh (closed circuit television), již s rozvojem a aplikací IP kamerových systémů není tak přesné. V rámci IP systémů, založených na protokolu TCP/IP, lze videosignál přenášet po síti do celého světa. Z těchto důvodů je daleko vhodnější souhrnně pro kamerové dohledové systémy používat název video dohledový systém (zkráceně VSS), i když je v normách a mnohých literaturách stále uváděna zkratka CCTV. [5]

V rámci integrovaného bezpečnostního systému se VSS nejčastěji propojují se systémy PZTS pro okamžitý přenos obrazové informace nebo započetí záznamu z místa, kde došlo k napadení. Kamerové systémy se často navazují také na systémy EPS. V případě hlášení požárního poplachu z určitého požárního úseku, dojde k aktivaci kamery, která se v daném prostoru nachází. Výstup kamery je pak např. zvěčněn na monitoru ostrahy, která pak podnikne adekvátní odezvu na vzniklou situaci.

1.4.1 Požadavky vztahující se na kamerové dohledové systémy

Legislativní postuláty kladené na integraci VSS systému jsou prezentovány v normě ČSN EN 50132-1, která stejně jako norma ČSN EN 50 131-1 ed.2 stanovuje systémové požadavky ovšem nikoliv na systémy PZTS, ale na CCTV sledovací systémy pro použití

v bezpečnostních aplikacích. Pro přehlednost jsou požadavky shrnuty do 9 bodů, některé níže uvedené zákonitosti jsou uvedené v normě týkající se pokynů o aplikaci - ČSN EN 50132-7: Část 7.

1. Vzniklá událost (přepadení, vloupání nebo požár) může aktivovat poplachový vstup systému VSS a spustit tak záznam popř. jinou přednastavenou činnost systému. Aktivační signál může vygenerovat konkrétní komponent např. detektor pohybu, otevření nebo kouře popřípadě jiný systém PZTS, SKV, EPS.
2. Odezva na poplach rovněž může aktivovat prvky systému bezpečnostního managementu (řízení přístupu nebo poplachové přijímací centrum).
3. Systém VSS může být integrován i s nepoplachovými aplikacemi: bankomaty, systémy rozpoznávání SPZ, s prodejními vybaveními pro dohled nad zbožím a elektronickou kontrolu zboží nebo systémy řízení budov.
4. Interface mezi jednotlivými aplikovanými systémy může ovládat společné databáze, řídit přenos dat i vzájemně řídit systémy.
5. V rámci požadavků na propojení nebo integraci jakéhokoliv dalšího zabezpečovacího systému k systému VSS se norma přímo odkazuje na evropskou technickou specifikaci CLC/TS 50398, která se musí aplikovat.
6. Všeobecně normativní předpis stanovuje dva druhy přenosu dat, kdy je fyzická přenosová cesta buď:
   - součástí systému VSS, nebo
   - je cesta poskytnuta třetí stranou jako externí propojení komponentů.
7. Jakékoliv propojení v systému i mezi systémy musí být provedeno tak, aby nedocházelo ke zpoždění, ztrátám a modifikaci přenášených dat.
8. Je vyžadováno sjednocení systémových úrovní přístupu všech systémů připojených k VSS z důvodu neautorizovaného přístupu.
9. V dokumentaci o prvcích systému by měli být poskytnuty dostatečné informace k zajištění integrace komponentů do systému VSS včetně se specifikací datového rozhraní. [6,7]

Aktivační impulzy vzniklé vlivem mimořádné události mají být odbavovány v tom pořadí, v jakém došly do společného vyhodnocovacího zařízení s výjimkou situace, kdy je příslušný vstup upřednostněn před ostatními prostřednictvím přiřazené priority signalizace. Obecný sled priorit je uveden v předpisu ČSN CLC/TS 50398, a v této práci je již zmíněn v kapitole 1.2 .

1.5 Systémy kontroly vstupu

Systémy kontroly vstupu je jeden z typů poplachových systémů, který se v bezpečnostních aplikacích nasazuje tam, kde je potřeba zajistit evidenci a řízení přístupu do chráněného prostoru nebo objektu. Účelem tohoto systému je řídit přístup a to z hlediska přidělených práv, jež stanovují kdo, kdy a kam má povoleno vkročit s cílem minimalizování rizika vstupu nepovolených osob a tím i navýšení úrovně bezpečnosti. SKV se především skládá z technických zařízení potřebným k samotnému řízení a dále z konstrukčních a organizačních opatření. [8]

Z hlediska integrovaných systémů se elektronický systém kontroly vstupu nejčastěji provazuje s poplachovými zabezpečovacími a tísňovými systémy, například pro ovládání a signalizaci stavu zóny systému PZTS se použije identifikační prvek přiložením k terminálu SKV, nebo se do systému SKV integrují VSS pro zaznamenání obrazových dat např. pro identifikaci a verifikaci uživatele systému.

1.5.1 Požadavky kladené na systémy kontroly vstupu

Obecné požadavky, vztahující se na systémy kontroly vstupu, prošly v nedávné době značných změn. Onou změnou je vydání zcela nové normy ČSN EN 60839-11, která má nahradit dosavadní předpis ČSN EN 50133-1 a tím zásadně změnit definici standartu pro SKV. Došlo ke zcela jiné definici úrovně zabezpečení, než bylo uváděno v původní normě. Místo klasifikace tříd identifikace (třída 0 až 3) a tříd přístupu (třída A nebo B) jsou definovány stupně zabezpečení 1 až 4 stejně jako u systémů PZTS a VSS. Tímto krokem se při integraci podstatně sjednotí a zjednoduší volba prvků v ohledu na zvolenou úroveň zabezpečení. [9]

Vzhledem k tomu, že výše jmenované normativní předpisy platí současně až do poloviny roku 2016, kdy platnost normy ČSN EN 50133-1 vyprší, jsou následující souhrnné legislativní požadavky na integraci SKV s ostatními poplachovými systémy uvedeny

v návaznosti na obě normy i spolu s normou uvádějící pokyny pro aplikace (ČSN EN 50133-7).

1. V elektronickém systému kontroly vstupu mohou být aplikovány kromě povinných funkcí uváděné normou i další funkce, avšak pouze za předpokladu, že nebudou mít negativní vliv na povinné funkce.
2. Výpadek nebo obnovení komunikace mezi zařízeními nesmí mít za následek uvolnění portálů (vstupů) a zároveň ověřování komunikace musí být realizováno jako součást finální instalace.
3. Zařízení (zařazené do stupně zabezpečení 2 až 4) musejí umožnovat autonomní provoz po přerušení komunikace s ovládacím zařízením.
4. Propojení mezi komponenty systému musí být navrženo a provedeno tak, aby byly minimalizovány možnosti modifikace, zpoždění nebo ztráta dat při přenosu.
5. Je-li použita veřejná datová sít (internet) ke komunikaci mezi komponenty, požaduje se u stupňů 3 a 4 šifrování komunikačních signálů.
6. Během jakékoliv poruchy komunikace s ovládacím panelem nesmí dojít k uvolnění místa přístupu a zároveň porucha komunikace nesmí mít vliv na proces rozhodování o přístupu.
7. Po úplné ztrátě napájení a následném obnovení je požadováno restart celého systému SKV. [10,11,12]

1.6 Elektrická požární signalizace

Elektrická požární signalizace je systém, který představuje významný prvek v oblasti požární ochrany osob a majetku. Je součástí souboru požárně bezpečnostních zařízení a jeho účelem je zajištění včasné detekce požáru, nejlépe již v raném stádiu a jeho lokalizace v chráněném objektu s následným předáním poplachové informace o vzniklém nebezpečném stavu. Systém je složen ze třech základních komponentů: ústředny EPS, hlásiči požáru, signalizací a popřípadě doplňkovými zařízeními, která jsou systémem ovládána. [13]

V praxi se EPS nejčastěji integruje s dalšími požárně bezpečnostními zařízeními, jako jsou například stabilní hasicí zařízení (SHZ), zařízení pro usměrnění pohybu kouře při požáru nebo zařízeními pro únik osob apod. V oblasti integrovaných systémů se systémy EPS propojují se systémy kontroly vstupu, kdy při vyhlášení požárního poplachu ústředna sys-

tému EPS vyšle signál k uvolnění přístupových portálů systému SKV. V současné době se ve stále větší míře uplatňují systémy videodetekce požáru, zkráceně VFD (Video Fire Detection), který pro detekci požáru využívá obrazový kamerový záznam s použitím počítačových systémů pro analýzu obrazových dat. Použitím tohoto systému VFD se jedná už o integraci se systémem VSS.

1.6.1 Legislativní požadavky na elektrickou požární signalizaci

Legislativa týkající se požární bezpečnosti, potažmo systému EPS a jeho integrace je poměrně rozsáhlá. Obecnější formu legislativních požadavků tvoří zákony a vyhlášky, které s návrhem a integrací EPS přímo nesouvisí, ale navazují na již mnohem konkrétnější, normativní předpisy. Jako základní legislativní úpravu je uváděn Zákon č. 133/1985 Sb. o požární ochraně, ve znění pozdějších předpisů. Tento základní předpis vytváří a upravuje podmínky pro ochranu zdraví, života a majetku před požáry nebo jinými živelnými pohromami popřípadě mimořádnými událostmi. Stanovuje povinnosti státních orgánů, jednotek požární ochrany a právnických a fyzických osob. Mimo jiné stanovuje takzvané kategorie požárního nebezpečí a kritéria pro členění do kategorií z důvodu rozdílných nároků při nasazování požárně bezpečnostních zařízení (zkráceně PBZ), mezi které patří i systém EPS. [14]

V návaznosti na tento zákon dále existuje Vyhláška č.23/2008 Sb. o technických podmínkách požární ochrany staveb, jež stanovuje požadavky na vybavení stavby požárně bezpečnostním zařízením. Požárně bezpečnostní zařízení musí být použito v souladu s českými technickými normami. V případě, kdy objekt není vybaven příslušným PBZ a tato skutečnost může mít za následek ohrožení života, zdraví nebo majetku, musí se stavba dovybavit PBZ a to i v případě, kdy to technická norma jen doporučuje. Mimo jiné jsou uváděny typy staveb s odkazy na normy a postupy, kterými je nutné se řídit pro splnění požární ochrany stavby. [15]

Svým obsahem a požadavky, které se již přímo dotýkají integrace EPS s jinými systémy, platí Vyhláška č. 246/2001 Sb. o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru neboli vyhláška o požární prevenci. Tato vyhláška především stanovuje jednak podmínky požární bezpečnosti u fyzických a právnických osob a požadavky na druhy aplikovatelných PBZ a jejich množství, jež jsou určeny k požární ochraně objektu. Vyhláška o požární prevenci předepisuje i normy, kterými je třeba se řídit při projektování EPS:

- ČSN EN 73 0802 – Požární bezpečnost staveb – nevýrobní objekty,
- ČSN EN 73 0804 – Požární bezpečnost staveb – výrobní objekty,
- ČSN EN 73 0875 – Požární bezpečnost staveb – stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení a
- ČSN EN 34 2710 – Elektrická požární signalizace – projektování, montáž, užívání, provoz, kontrola, servis a údržba. [16]

Hlavní zákonný požadavek na PBZ je, že jeho vybavení a množství musí vyplývat z dokumentu požárně bezpečnostního řešení stavby nebo z dokumentace, která je součástí projektové dokumentace schválené stavebním úřadem. Není-li projektování u vyhrazených PBZ vymezeno normativními požadavky, postupuje se podle předpisů výrobců nebo dovozců. Dále jsou ve vyhlášce uváděny druhy PBZ, které lze v praxi spolu integrovat:

a) zařízení pro požární signalizaci, kterou se rozumí např.: EPS, zařízení pro dálkový přenos, ruční požárně poplachové zařízení a autonomní požární signalizaci,
b) zařízení pro potlačení požáru nebo výbuchu např. SHZ nebo automatické samočinné hasící systémy,
c) zařízení pro usměrnění pohybu kouře při požáru např.: klapky, ventilace, kouřotěsné dveře, zařízení pro přirozené odvětrání kouře,
d) zařízení pro únik osob jako jsou evakuační výtahy, nouzové osvětlení, funkční vybavení dveří, nouzové sdělovací zařízení apod.
e) zařízení pro zásobování požární vodou což jsou vodovody, hydranty, plnící stojany atd.
f) zařízení pro omezení šíření požáru, mezi které si můžeme představit požární klapky, dveře, uzávěry otvorů, vodní clony, požární přepážky a ucpávky, dále i
g) náhradní zdroje a prostředky k zajištění provozuschopnosti PBZ (zásoba hasebních látek a vody atd.) a
h) zařízení zamezující iniciaci požáru nebo výbuchu.

V požadavcích na projektování požárně bezpečnostních zařízení se uvádí, že se musí postupovat dle normativních předpisů a v případě, že při aplikování dvou nebo více

PBZ dojde k vzájemnému ovlivňování, musí být v projektu uvedeno způsob a pořadí uvádění jednotlivých systémů do činnosti a tím tak stanoveny priority a jejich funkce při vzniku mimořádné události.

1.6.2 Technické a normativní požadavky na integraci

Jak již bylo uvedeno, podmínky pro návrh EPS a vypracování požárně bezpečnostního řešení (PBŘ) stanovuje technická norma ČSN EN 73 0875. V této normě se uvádí, že v PBŘ musí být uveden důvod a způsob vybavení objektu jednotlivými PBZ i s popisem vzájemných vazeb mezi systémy. Zároveň musí být uveden průběh a způsob, jak budou PBZ uváděny do provozu. V požadavcích na EPS je uváděno, že ústředny musí být zajištěny proti neoprávněné manipulaci nepovolanými osobami a pokud je systém EPS vybaven zařízením dálkového přenosu (zkráceně ZDP) nemusí být zřízena trvalá obsluha. Jeli však naopak systém elektrické požární signalizace vybaven ZDP, je nutné systém dovybavit obslužným polem požární ochrany (OPPO) spolu s klíčovým trezorem požární ochrany (KTOP). Pokud je však střežený objekt vysoký více než 45m, popřípadě se jedná o zdravotnické zařízení s více než čtyřmi nadzemními patry, musí být EPS dovybaven ZDP. [17]

Ohledně integrace systému EPS s dalšími systémy je v normě stanoveno, že samotné ovládání EPS musí být provedeno napřímo. Je tedy vyloučeno, aby se EPS ovládala jiným softwarově řízeným systémem. Uplatnění jiného řešení ovládání je možné pouze na základě odborné studie spolehlivosti s jednoznačným průkazem, že i v případě požáru bude systém plnit svou funkci a použité ovládání přes jiný systém, než je systém EPS, bude bezpečné. Tento způsob řešení je aplikován většinou jen ve výjimečných případech, jako jsou řídicí systémy tunelů. V souvislosti s integrací je dále v normě ČSN EN 73 0875 uveden požadavek na vybavení EPS grafickou nadstavbou, která již může být součástí softwarové integrace s jinými bezpečnostními systémy. Grafická SW nadstavba musí být použita v případech, kdy:

a) chráněná plocha, kde je detekováno požární nebezpečí je větší než 10 000 m^2, nebo

b) systém je aplikován na 100 střežených objektů v jedno podlaží, a nebo

c) EPS chrání stavby zvláštního významu.

V oblasti problematiky návrhu EPS norma ČSN EN 34 2710 určuje požadavky na EPS a jeho integraci s dalšími systémy následovně:

1) systém musí být navržen a provozován tak, aby primárně splňoval svůj hlavní účel, tedy ochrana života, zdraví a majetku před požárem,
2) funkčnost EPS při požáru nesmí být ovlivněna ostatními technickými zařízeními a
3) ústředna EPS musí vždy umožňovat provoz ve dvou režimech (den a noc),
4) komponenty a zařízení, které jsou připojeny do systému EPS, musí splňovat požadavky norem řady ČSN EN 54-xx současně však musí být naplněny kritéria:
    - spolehlivosti,
    - funkční účelnosti,
    - náklady v ohledu k hodnotám, které jsou chráněny a
    - hospodárnosti provozu komponentu,
5) v rámci kompatibility integrovaného komponentu může být použit jen prvek, který je certifikován v souladu s ČSN EN 54-13 a
6) vliv jedné vzniklé poruchy na komunikační cestě systému EPS nesmí ovlivnit:
    - komunikaci a vyhodnocení signálu od více jak 32 prvků,
    - vyslání signálu k vyhlášení poplachu,
    - přenos signálu z a do vstupně výstupních zařízení,
    - iniciace provozu ovládaného popřípadě doplňujícího zařízení.[18]

V normativních úpravách, kromě požadavku na vybavení EPS grafickou nadstavbou (uvedeno v ČSN EN 73 0875), se již nezmiňuje o definici, pravidlech ani stanovení podmínek pro jejich nasazení. Současný trend však ukazuje, že integrace ve formě grafických nadstaveb je poměrně hojná, avšak podmínky jejich nasazování nejsou nijak normativně ošetřeny. Podobně je to u typu integrace, kdy systém EPS je provázán se systémem VSS za účelem požární videodetekce. VFD je v normě (jmenovitě ČSN EN 34 2710) popsána jen obecně, tudíž nejsou zde uváděny žádné specifické technické údaje pro výběr komponentu, jeho instalaci, provoz či údržbu. Tento legislativní nedostatek by bylo dobré napravit, protože tento typ detekce požáru nabývá v praxi svého významu. Vhodným doplňkem normativních předpisů by byl požadavek, aby systém VSS určený pro videodetekci požáru musel

splňovat postulát norem pro standartní hlásiče pro detekci kouře (ČSN EN 54-7), popřípadě hlásiče pro detekci plamene (ČSN EN 54-10).

Z hlediska integrace se jako jediný normativ dá považovat ČSN EN 54-13, která se zabývá systémovými požadavky a je zpracována v souvislosti na integraci komponentů PBZ. Udává nároky na vzájemnou propojitelnost prvků systému a kompatibilitu jednotlivých komponentů EPS. Stanovuje také požadavky na integritu EPS (posloupnost operací po detekci požáru) v případě, že je systém připojen k jiným komponentům. [19]

Dílčí závěr kapitoly

Na základě komplexně provedeného rozboru legislativních požadavků, které jsou kladeny na dílčí poplachové zabezpečovací systémy v ohledu na jejich integraci je zřejmé, že na systémy EPS jsou kladeny zcela jiné požadavky, než na ostatní systémy. Tato skutečnost je zakotvena již v Zákonu č. 133/1985 Sb. o požární ochraně a dalších prováděcích vyhláškách, které sice tvoří jen obecnější formu legislativních požadavků, ale přímo se odkazují na jednotlivé normy. V oblasti požadavků při integraci systémů PZTS, VSS a SKV je nejhlavnějším předpisem norma ČSN CLC/TS 50398, na kterou se následně odkazují i ostatní aplikační normy dílčích systémů, ve kterých jsou postuláty v návaznosti na integraci zmíněny jen obecně. Celkově jsou všechny požadavky aplikačních norem na integrovaný poplachový systém uvedeny v přehledu následovně:

- všechna společná zařízení musí splňovat požadavky aplikačních norem systémů, které byly zahrnuty do IPS,
- na systémovou integritu musí být použity ty nejpřísnější požadavky ze všech aplikovaných norem,
- veškeré použité komponenty musí být navzájem kompatibilní a zvoleny v souladu s třídou prostředí a stanoveným stupněm zabezpečení,
- doplňkové ovládací zařízení, musí obsahovat prostředky pro detekci sabotáže,
- propojení mezi komponenty systému musí být navrženo s ohledem na minimalizování zpožďování, modifikací nebo ztrátu signálů a propojení mezi systémy musí být monitorováno,
- komponenty mohou být integrovány pouze za předpokladu, že nedojde k ovlivňování vlastností jiných komponentů a povinných funkcí systému,

- je vyžadováno sjednocení systémových úrovní přístupu všech připojených systémů,
- v dokumentaci by měly být poskytnuty dostatečné informace k zajištění integrace komponentů do systému včetně se specifikací datového rozhraní,
- výpadek nebo obnovení komunikace mezi zařízeními nesmí mít za následek nesprávnou nebo nepožadovanou funkci systému,
- je-li použita veřejná datová síť (internet) ke komunikaci mezi komponenty, je vhodné aplikovat šifrování komunikačních signálů a
- po ztrátě napájení a následném obnovení je požadováno restart celého systému.

Z analýzy legislativních požadavků na systém EPS a jeho integrace vyplývá, že tento systém lze integrovat s dalšími požárně bezpečnostními zařízeními více způsoby. V případě integrace s dalšími poplachovými bezpečnostními systémy v návaznosti na legislativu se jeví nejschůdnější integrace použitím grafické SW nadstavby. Výčet obecných požadavků na integraci EPS je uveden níže:

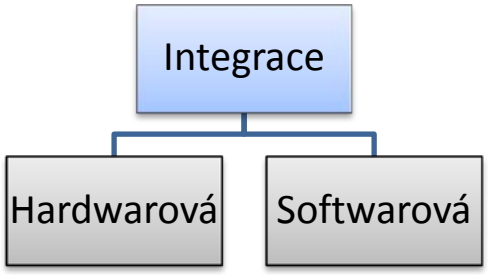
- funkčnost EPS při požáru nesmí být ovlivněna ostatními technickými zařízeními,
- ovládání EPS musí být provedeno napřímo což vylučuje ovládání jiným softwarově řízeným systémem,
- grafická SW nadstavba musí být použita v objektech s plochou více než 10 000 m^2, na 100 střežených objektů v jedno podlaží a ve stavbách zvláštního významu,
- komponenty a zařízení, které jsou připojeny přímo do systému EPS, musí splňovat požadavky norem řady ČSN EN 54-xx.

2 INTEGRACE POPLACHOVÝCH SYSTÉMŮ

Oproti předchozí kapitole, která se věnovala komplexním legislativním požadavkům, se nyní druhá teoretická část bude věnovat již technickým způsobům a prostředkům, jak je možné provést integraci poplachových bezpečnostních systémů.

2.1 Technické způsoby provedení integrace

Obecně lze možnosti propojení jednotlivých poplachových systémů do jednoho celku rozdělit na dvě základní skupiny, přičemž je možné, že se tyto uvedené způsoby integrací mohou vzájemně prolínat a kombinovat.



Obr. 4: Základní rozdělení způsobů integrace [20]

2.1.1 Hardwarová integrace poplachových systémů

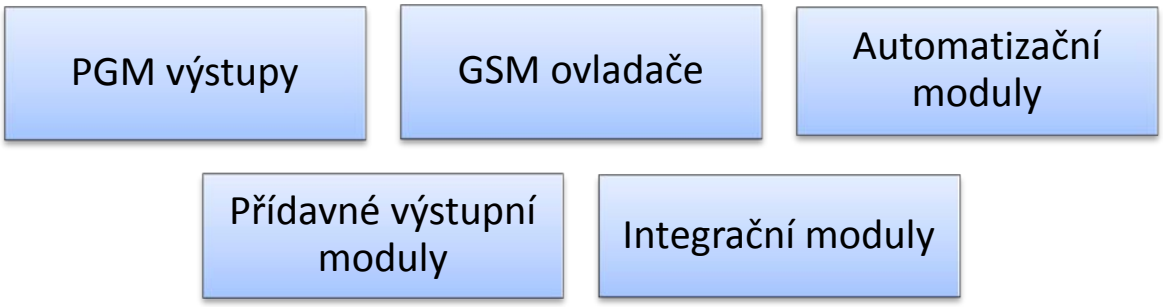
Hardwarová integrace poplachových aplikací spočívá ve vzájemném propojení jednotlivých systémů prostřednictvím jejich vstupů a výstupů a zároveň i na technických vlastnostech systému PZTS, který vedle jeho obvyklých základních funkcí umožnuje i funkce specifické k rozšíření ovládání dalších poplachových systémů. Jako příklad můžeme uvést systém SKV za účelem kontroly vstupu nebo aplikaci VSS například pro změnu snímané scény. K jednotlivým způsobům integrace, jež jsou uvedeny níže, lze zařadit i automatizační systémy v budovách, které kromě jejich hlavní funkce, což je ovládání nepoplachových aplikací (klimatizace, vytápění, žaluzie, ozvučení apod.), umožnují i provázání s prvky poplachových aplikací. Hardwarová integrace se dělí na:

1) integraci IN/OUT (vstup/výstup),
2) integraci, kde ústřední prvek je PZTS,
3) integraci, kde je naopak ústřední prvek komponent systému VSS nebo SKV a

4) integraci, jež zabezpečuje automatizační systém v budově. [20]

2.1.1.1 Integrace typu IN/OUT

Nejnižší stupeň integrace představuje integrace typu IN/OUT, u které se využívá vstupů a výstupů ústředen zabezpečovacích systémů, řídících jednotek nebo přímo komponentů. Mezi systémy jsou přenášené pouze stavové informace, na základě kterých pak dochází k změnám stavu výstupů dle konkrétní konfigurace systému. Tento typ integrace není vhodný pro nasazení do rozsáhlejších aplikací z důvodu technologické náročnosti spočívající v nárůstu počtu kabeláže a limitů v počtu vstupů a výstupů u jednotlivých komponentů. Z pohledu celkové decentralizované správy, ovládání a problematické celkové vizualizace je tento typ integrace vhodnější spíše do menších objektů. Výhodou je však propojení systémů bez ohledu na výrobce, jelikož nejsou používány žádné komunikační protokoly při komunikaci mezi systémy. Označovaný způsob integrace IN/OUT je v praxi realizovatelný celkem pěti způsoby propojení komponentů, viz. výčet na obrázku níže, kdy obecný popis jednotlivých způsobů je nastíněn dále. [20]



Obr. 5: Přehled způsobů integrace IN/OUT [20]

Integrace s pomocí programovatelných výstupů

Jako základní typ integrace IN/OUT považujeme provázání komponentů systému s využitím programovatelných výstupů (zkráceně PGM). Tyto PGM výstupy jsou nejčastěji součástí ústředny PZTS nebo jako doplňující kartové moduly, poskytující dvě stavové informace, anebo se mohou použít k spínání napájecího napětí a to na základě naprogramované aktivační události (zapnutí, vypnutí střežení, narušení apod.). Technicky jsou PGM výstupy realizovány tranzistory s otevřeným kolektorem, tranzistory s uzavřeným emitorem, reléovým výstupem bez potenciálu nebo s napětím o určité velikosti.

Integrace s GSM ovladači

GSM ovladače slouží k realizování bezdrátové integrace prostřednictví přenosu datových zpráv přes GSM síť. Ovládání se provádí na základě iniciační události a to zasláním SMS zprávy nebo prozvonění zařízením. Na trhu jsou GSM ovladače často uváděny jako GSM brány nebo GSM komunikátory a často jsou konstrukčně realizovány jako autonomní zařízení provádějící s pomocí svých reléových výstupů konkrétní přednastavenou činnost.

Integrace s využitím automatizačních modulů

Integrace tohoto typu je realizována univerzálním automatizačním modulem disponující dvoustavovými vstupy pro detektory, čidla, řídicí jednotky apod. a reléovými výstupy pro jakákoliv ovládaná zařízení tímto způsobem. Programování těchto modulů bývá realizováno počítačem připojeného přes Ethernet nebo Internet. Automatizační moduly jsou instalovány většinou přímo v ovládaném zařízení.

Integrace s využitím přídavných výstupních modulů ústředen

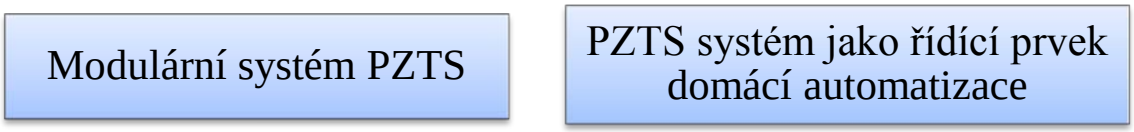
Přídavný výstupní modul je součástí instalace zabezpečovací ústředny a svými pevně nastavenými a tudíž neměnnými výstupy kopíruje vnitřní stavy ústředny, jež se mění vlivem aktivační události. Použitím těchto modulů je možné rozšířit ústřednu o další výstupy v případech, kdy nám nepostačují výstupy, které jsou pevnou součástí základní řídící desky.

Integrace aplikováním integračních modulů

Pro potřebu integrovat různé poplachové i nepoplachové systémy mezi sebou a pro komunikaci s nadstavbovým integračním systémem slouží integrační moduly. Integrační moduly slouží k převodu specifických dat ústředen do jednotného komunikačního standardu za účelem integrace dat pro centralizovanou správu a ovládání různých typů zařízení.

2.1.1.2 PZTS jako integrační prvek

Vlastní integraci jednotlivých prvků může zabezpečovat systém PZTS jako takový a to generováním řídících signálů, kterými by ovládal systémy domácí automatizace, a v druhém případě lze integraci pojat způsobem modulové architektury, kdy každý modul má svoji specifickou funkci a akumulaci dat pro vizualizace a centrální správu zajišťuje PZTS systém. [20]



Obr. 6: Aplikace, kde PZTS je integračním prvkem [20]

Modulární systém PZTS

Integrovaný systém je založen na jednotlivých modulech, představující konkrétní poplachové (SKV, EPS) a nepoplachové (regulace, měření) aplikace. PZTS systém je určený jako integrační prvek připojený ke všem modulům, které řídí a ovládá. Sám dále poskytuje data pro nadstavbový vizualizační SW pro efektivní správu. Nevýhodou tohoto typu integrace je, že v případě poruchy centrálního systému PZTS dojde k narušení funkcí většiny připojených technologií. Ovládání subsystémů PZTS systémem probíhá s pomocí výstupních modulů nebo systémových expandérů.

PZTS jako řídící prvek domácí automatizace

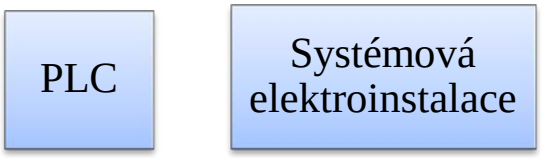
Je-li požadována pouze integrace PZTS systému s dalšími nepoplachovými systémy, jež jsou ovládány domácím automatizačním systémem, přichází na řadu typ integrace, při které systém PZTS generuje řídící signály pro automatizační systémy. Signály může generovat buď přímo ústředna PZTS nebo zdrojem signálu může být konkrétní detektor. Řídící signály, generované např. zabezpečovacím systémem, se transformují prostřednictvím rozhraní na komunikační standard X-10, jež využívá většina automatizačních systémů. Standard X-10 je specifický v tom, že pro přenos signálů mezi komponenty využívá silového vedení v budovách.

2.1.1.3 VSS nebo SKV jako integrační prvek

Komponent zajišťující integraci může být kromě systému PZTS i systém VSS nebo SKV. Tyto systémy mohou taktéž přijímat a i odesílat data a tím ovládat ostatní systémy prostřednictvím svých programovatelných výstupů. V případě systémů VSS se vstupy a výstupy podílející se na integraci nacházejí přímo na kameře nebo na záznamovém zařízení. U systému SKV se tyto řídící prvky převážně nacházejí na řídících dveřních jednotkách. Vstupy jsou technicky realizované zapojením NO a NC. Výstupy jsou reléové s napětím nebo bez něj v závislosti na konfiguraci. [20]

2.1.1.4 Integrace pomocí automatizačního systému

Automatizační systém je v budovách primárně určen pro ovládání nepoplachových technologií, jako je osvětlení, větrání a vytápění. K řízení těchto technologií je používán programovatelný průmyslový počítač (PLC), na který lze připojit i zabezpečovací prvky různých systémů. Dalším způsobem je využití automatizačního systému založeného na technologii systémové elektroinstalace, jež je koncipována na platformě sběrnice rozvedené po celém objektu. [20]



Obr. 7: Oblasti integrace automatizačního systému [20]

PLC jako integrační prvek

Ve velikostně malých objektech lze provést integraci různých technologií za pomocí PLC systému. Jde o zcela autonomní řídicí systém, který je primárně nasazován do objektů za předpokladu řízení a ovládání různých technologií, elektrických spotřebičů a zařízení, avšak jeho dvoustavové vstupy a výstupy lze použít i k připojení komponentů poplachových systémů.

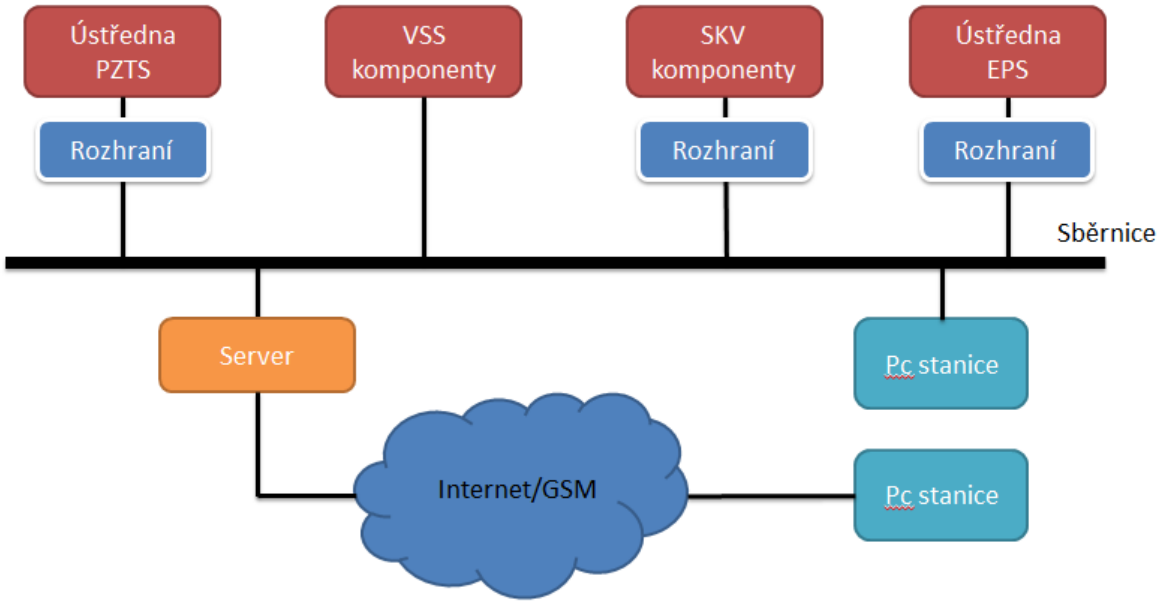
Integrace s pomocí systémové elektroinstalace

Systémová elektroinstalace, také uváděná jako inteligentní instalace využívá síťové centrální sběrnicové infrastruktury objektu ke komunikaci s prvky prostřednictvím tzv. datových telegramů. Podstatnou předností je, že samotná sběrnice může být realizována kroucenou dvojlinkou, silovým vedením nebo rádiovým přenosem. Princip systémové elektroinstalace je ovládání zařízení s pomocí akčních členů a snímačů jak nepoplachového, tak i poplachového rázu. Na trhu jsou známy především sběrnice KNX, EIB a LON.

2.1.2 Softwarová integrace poplachových systémů

Princip softwarové integrace spočívá v použití nadstavbových SW produktů, jenž zajišťují komplexní správu, řízení i vizualizaci aplikovaných bezpečnostních technologií. Nadstavbové řídící produkty jsou nainstalované na externí počítačové technice, která je většinou

server nebo klientská stanice PC, popřípadě i zcela autonomní řídící centrála. Jednotlivé systémy jsou prostřednictvím komunikační sběrnice připojeny k hardwarovým prvkům obsahující právě zmíněný nadstavbový integrační SW. Jako datové rozhraní se zpravidla používá Ethernet, ať už v rozsahu LAN nebo WAN, popřípadě sériové rozhraní RS 232 a port USB a to zejména u méně rozsáhlých aplikací. Softwarová integrace oproti hardwarovému řešení nabízí přístup k jednotlivým funkcím, vzdálenou správu a řízení technologií prostřednictvím vzdáleného počítače nebo i prostřednictvím mobilního zařízení s přístupem k internetové síti. [20]



Obr. 8: Znázornění schématu SW integrace [20]

Jednotlivé bezpečnostní aplikace jsou k serveru, kde je nainstalovaný nadstavbový integrační SW, připojeny prostřednictvím datové sběrnice a rozhraní, které umožňuje napojení ústředen PZTS, EPS popř. komponenty SKV na sběrnici. Komponenty VSS jsou ke sběrnici připojeny bez rozhraní, protože technologie IP kamerových systémů umožnuje komunikaci se síťovými prvky přímo. Klientské Pc stanice se k serveru může připojit jak lokálně přes LAN, tak i vzdáleně prostřednictvím internetu nebo sítě GSM. Alternativně se s klientskou stanicí lze k jednotlivým ústřednám napojit přímo přes sériové rozhraní s absencí serveru. Softwarovou integraci můžeme rozdělit na čtyři podkategorie.

1) Software ústředen poplachových zabezpečovacích systémů,
2) softwarová integrace pro uživatelskou správu,

3) integrační vizualizační software a
4) integrační software systémů budov.

Každá z těchto podkategorií je specifická poskytovanými funkcemi integračního nadstavbového software. Počet a úroveň použitých funkcí SW se odráží v použité technice s ohledem na potřeby instalačních a montážních firem a hlavně v požadavcích zákazníka a posléze uživatele integrovaného bezpečnostního systému.

2.1.2.1 Software ústředen poplachových zabezpečovacích systémů

Typ tohoto základního doplňkového programového nástroje je primárně určen pro nastavení a naprogramování ústředen poplachových zabezpečovacích systémů. Propojení počítače s řídící jednotkou ústředny je realizováno dálkově nebo místně a to prostřednictvím modemu, telefonní linky, sériovým rozhraním nebo po síti. Kromě programování a nastavení slouží i pro sledování stavu systému, vyhodnocování a archivaci vzniklých událostí zapsaných v paměti. Aplikací těchto SW produktů jde o integraci v rámci vyhodnocení a archivaci dat a událostí ústředen, které mohou být spojeny s dalšími systémy. Ovládací programy na této úrovni jsou určeny pro realizaci a zavedení systému do provozu, popřípadě pro potřebu pozdějších servisních zásahů vyškolenými montážními techniky. [20]

2.1.2.2 Softwarová integrace pro uživatelskou správu

SW nástroje pro uživatelskou správu umožnují kromě sledování stavu systému, vyhodnocování a archivaci událostí také uživatelské nastavení řídících jednotek připojených k systému. V praxi se tento typ programů nejčastěji uplatňuje v systému PZTS s nástavbou pro kontrolu vstupu. Mezi rozšířené funkce pro uživatelskou správu v ohledu na integraci se systémem SKV patří zejména:

- možnost nastavení uživatelských kódů a profilů,
- popisování podsystémů a přístupových terminálů,
- filtrování událostí s parametry: uživatel, čas, dveře, událost atd.,
- vytváření a správa časových rozvrhů pro přístup a také
- přidělování a evidenci přístupových karet, čipů apod.

Součástí těchto produktů zpravidla nejsou prvky pro vytváření mapových podkladů a plánů chráněných objektů. Proto jsou softwary pro uživatelskou správu vhodné jen pro aplikace menšího charakteru, kde s přehledností a orientací v systému a v samotném objektu by nebyl žádný problém. [20]

2.1.2.3 Integrační vizualizační software

V rozsáhlých bezpečnostních aplikacích se již nasazují vizualizační softwary, které na rozdíl od předešlých programů pro uživatelskou správu poskytují funkci pro vizualizaci (vyobrazení) celého integrovaného systému a to v reálném čase. Záměr použití těchto SW prostředků je jasné – zvýšení přehlednosti nad systémem a zefektivnění řešení konkrétní bezpečnostní situace. Na základě vložených půdorysných plánů objektů a mapových podkladů v kterých je graficky vyznačena poloha komponentů bezpečnostního integrovaného systému (veškeré komponenty PZTS, SKV, VSS, EPS), má obsluha možnost sledovat stav celého systému. Kromě monitoringu může pracovník ostrahy i ovládat vybrané funkce systému a vzdáleně je řídit. Mezi typické funkce patří ovládání kamer, dveří, střežení podsystémů nebo aktivování PGM výstupů k ovládání dalších zařízení. Souhrnně integrační vizualizační SW oproti předešlým nástrojů poskytuje navíc prostředky pro:

- vkládání plánů a map objektů,
- umísťovat do nich značky a komponenty zabezpečovacích systémů,
- tvořit popisy subsystémů, přístupových bodů v plánech,
- ovládat PGM výstupy a stavy podsystémů přímo z mapových podkladů. [20]

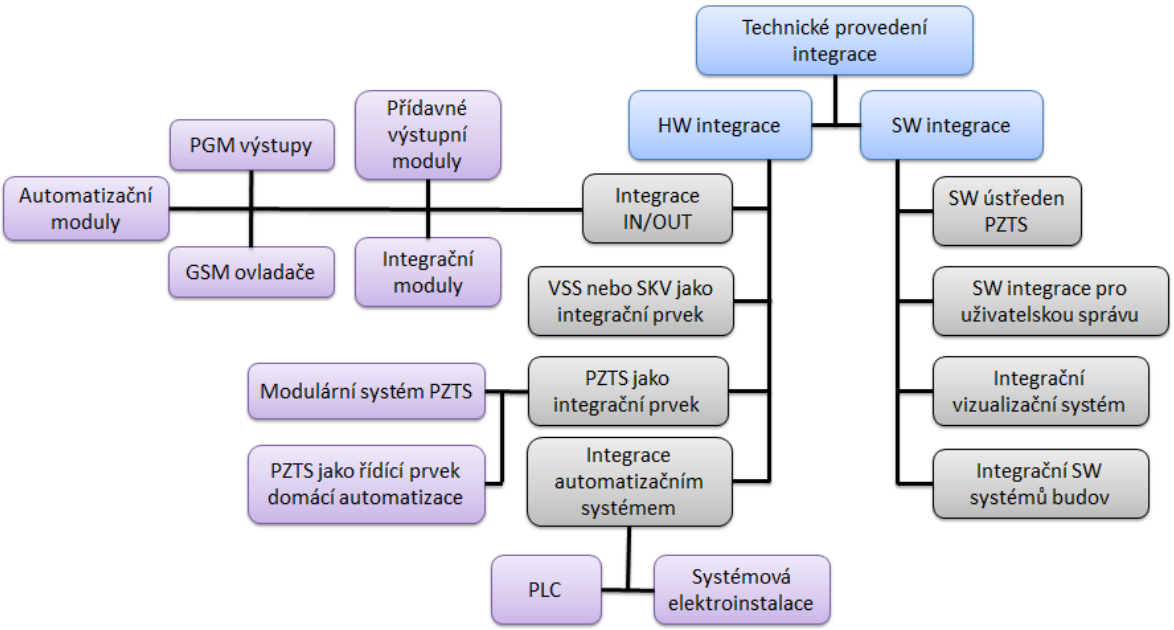
2.1.2.4 Integrační software systémů budov

Nadstavbový integrační SW systémů budov je realizovaný vzájemným propojením veškerých bezpečnostních technologií i ostatních nepoplachových technologií obsažených v budově. Integrace je založena SW nástroji nainstalovaném na serveru, který je ovládaný prostřednictvím webového prohlížeče na klientském PC. Jde tedy o architekturu typu klient-server. Technicky je propojení mezi jednotlivými aplikacemi a serverem provedeno pomocí integračních modulů. Jako integrační moduly považujeme jednotlivá rozhraní neboli komunikátory (interface) mezi interní sběrnicí jednoho konkrétního systému a standardizovaným rozhraním serveru, nejčastěji LAN. Typ této SW integrace poskytuje uživateli nastavení automatických vazeb mezi jednotlivými poplachovými i nepoplachovými

systémy, lokální i vzdálenou správu, ovládání a dokonce i správu docházky s návazností stravovací a mzdový systém. Samozřejmostí je také vizualizace a správa uživatelů. [20]

Dílčí závěr kapitoly

Z teoretické části týkající se technických způsobů, jak lze integrovat jednotlivé systémy vyplývá, že v mnoha ohledech je pro jednoduchost a efektivitu řízení komplexní bezpečnosti a to zvláště v aplikacích velkého rozsahu, vhodné aplikovat integraci s pomocí nadstavbových SW produktů. Mějme ovšem na paměti, že použití integračních programů je jen doplňkové a jeho výpadek činnosti nesmí negativně ovlivňovat chod jednotlivých poplachových systémů, jež jsou k němu připojeny. Z těchto důvodů je nejvhodnější některé důležité mezisystémové vazby zabezpečit již na hardwarové úrovni – HW integrací. Pro komplexní přehled o možných způsobech provedení integrace je vhodné provést grafickou vizualizaci, zahrnující veškeré varianty.



Obr. 9: Grafická vizualizace způsobů provedení integrace

3 KOMUNIKAČNÍ ROZHRANÍ

Kapitola úzce související s problematikou integrace popisuje typy obecných komunikačních standardů, jež se používají ke komunikaci mezi dvěma a více zařízeními nebo k přenosu dat do SW nástrojů zajišťující centrální sběr informací o IPS. Kromě popisovaných technologií existuje spousta dalších, velmi specifických protokolů, které byly vyvíjeny na účelem propojení konkrétních systémů. Z pohledu používaných fyzických rozhraní, bez ohledu na komunikační protokol, se ke komunikaci používají:

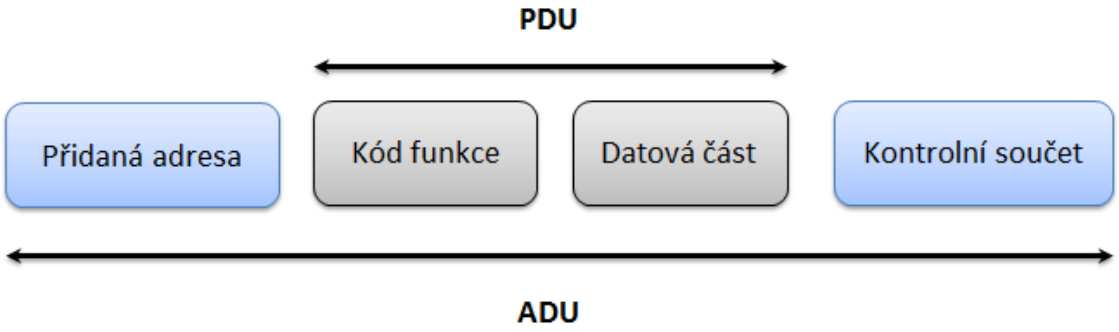
a) sériové rozhraní USB,
b) asynchronní sériový přenos RS-232 a RS-485,
c) a Ethernet s využitím protokolu TCP/IP. [20]

3.1.1 Komunikační standardy

Hlavní přednosti všech otevřených komunikačních standardů je, že servery ani klienti nemusí být pouze od jednoho výrobce, což skýtá mnoho výhod zvláště při integraci různorodých zařízeních od různých výrobců nejen zebezpečovací techniky, ale především automatizačních technologií. Následující přehled uvádí nejběžnější používané standardy.

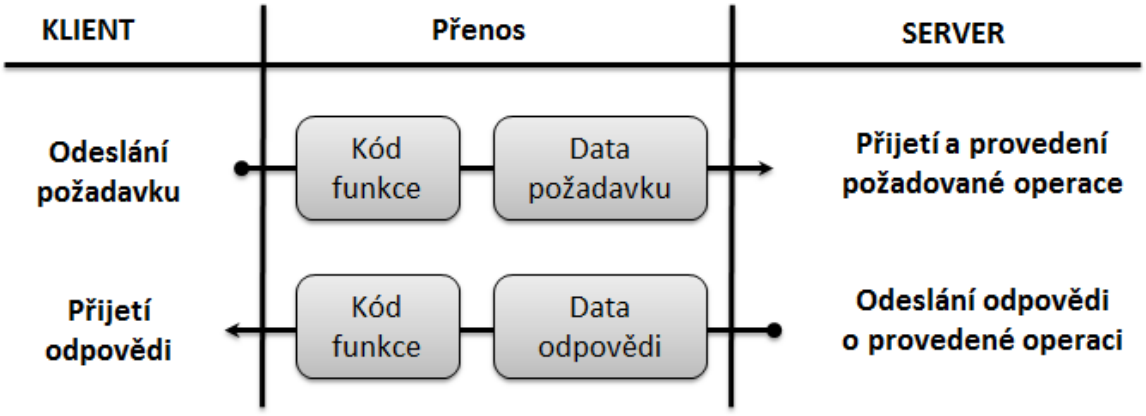
3.1.1.1 Protokol MODBUS

Komunikační protokol Modbus je otevřeným protokolem umožňující vzájemnou komunikaci různých typů zařízení od programovatelných logických automatů (PLC), PC, čidel, detektorů, měřících přístrojů, ústředen poplachových zabezpečovacích systémů až po dotykové displeje apod. Podporuje celou řadu komunikačních médií, jako jsou sériové linky RS-232 a RS-485, optické i rádiové sítě a především síť Ethernet s využitím protokolu TCP/IP. Je založen na principu klient/server, kdy předávání datových zpráv probíhá mezi řídícím prvkem tzv. master zařízením (serverem), jež posílá konkrétní dotazy jednotlivým ovládaným zařízením typu slave (klient) a ti mu odpovídají. Komunikace je tedy realizována metodou požadavek-odpověď a specifikace dané funkce je definována v samotném kódu funkce, která je součástí vlastního požadavku směřovanému ke klientu.



Obr. 10: Struktura standardu Modbus [21]

Standart Modbus definuje strukturu přenášené zprávy na úrovni PDU (Protocol Data Unit) protokolu, což znamená, že Modbus je zcela nezávislý na použitém typu komunikačního média. Součástí PDU je kód funkce a vlastní datová část. V kódu funkce je uveden druh operace, přičemž první polovina (1-127) celkového rozsahu funkce je určena pro druh operace, která se má provést a druhá polovina rozsahu (128-255) je vyhrazena pro oznámení negativní odpovědi. V datové části PDU jsou uvedeny data k provedení činnosti dané kódem funkce, např.: adresa prvku, počet vstupů, číselná hodnota apod. popřípadě i žádná hodnota, pokud to k provedení určité činnosti není zapotřebí. Jeli však Modbus protokol použit v síti typu LAN nebo WAN, je PDU rozšířen o další části: adresu a kontrolní součet tvořící zprávu na aplikační úrovni, tedy ADU (Application Data Unit).



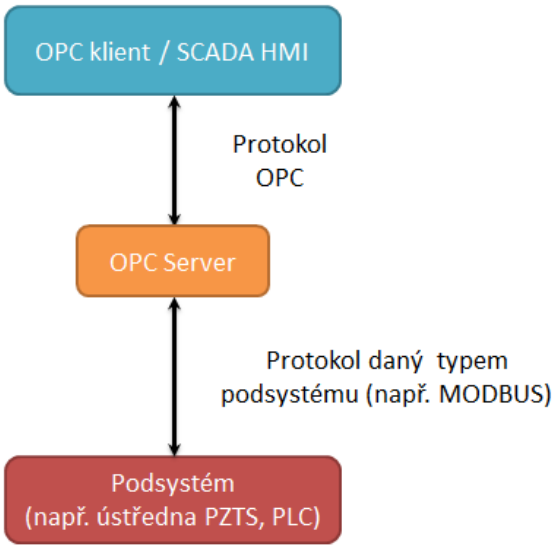
Obr. 11: Komunikace s použitím protokolu Modbus [21]

Komunikace probíhá tak, že po odeslání požadavku klientem a zpracování a provedení operace serverem, odpoví sever zprávou obsahující v poli kódu funkce číselné ozna-

čení provedené operace pro indikaci úspěšného úkonu a v datové odpovědi pak případně pošle požadovaná data klientem. Pokud však došlo při vykonávání operace k chybě, v poli kódu funkce je uvedeno číslo požadované funkce avšak s nastaveným nejvyšším bitem, jež signalizuje neúspěch a v datové části je poslán důvod neúspěšné operace, vyjádřen chybovým kódem. [21]

3.1.1.2 OPC standard

OPC standard (Open Proces Control), určený pro bezpečnou a spolehlivou výměnu dat v průmyslové automatizaci, je vyvíjen americkou mezinárodní organizací OPC Foundation se kterou spolupracují různé společnosti zabývající se monitoringem, řízení a vizualizací v oblasti technologických procesů v čele firmami Honeywell a Siemens věnující se i průmyslu komerční bezpečnosti. OPC standart je charakterizován jako sada specifikací průmyslového standardu, jež definuje komunikační rozhraní pro ovládání technologických procesů. S využitím architektury klient/server upravuje datovou komunikaci mezi řídícím zařízením (master) a klientským zařízením, aplikací typu SCADA/HMI (Supervisory Control And data Acquisition/Human-machine Interface), nástrojem pro správu a monitoring. [22]



Obr. 12: Princip komunikace při standardu OPC [23]

OPC server neboli master zařízení je přímo připojen k automatizačnímu zařízení (např. ústředně PZTS) a s pomocí SW ovladače a protokolem daného typu pro konkrétní podsystém, např. Modbus si s ním vyměňuje data. Na OPC sever se následně připojují OPC klienti (součást řídící nebo vizualizační aplikace), kteří si dle konkrétních specifikací přebírají

data ze serveru. Dle požadavků obsluhy, jež jsou určeny koncovým automatizačním zařízením, pak OPC klient zpětně předává příkazy serveru. Součástí dané implementace je i technologie DCOM od firmy Microsoft, díky níž komunikace může probíhat i s pomocí sítě LAN a relační databázový server pro centralizaci a uchovávání dat. Nastavení komunikace probíhá nejprve konfigurací OPC serveru. V serveru se provede nastavení tzv. vstupně-výstupních bodů a tím se nadefinují serverem požadované informace a následně se provede napojení na data uložené v paměti ovládaného zařízení i s nastavením periody pravidelného přenosu dat. V druhém kroku se konfiguruje OPC klient tím, že se vyhledá a připojí požadovaný OPC server s pomocí DCOM technologie a následně se v klientu nastaví vyhodnocování veličin, které jsou v serveru nakonfigurovány a které bude server poskytovat klientu a tím SW aplikaci za účelem řízení, vyhodnocování a vizualizaci. [23]

3.1.1.3 Technologie DDE

DDE (Dynamic Data Exchange) je protokol pro dynamické výměny dat. Byl vyvíjen firmou Microsoft pro vzájemnou komunikaci aplikací na bázi operačního systému MS Windows (MS Exel, Word apod.). Kromě předávání dat v rámci jednoho počítače taktéž umožňuje komunikaci v rámci počítačové síti. Protokol DDE je koncipován na bázi server/klient a pro vzájemnou výměnu dat používá sdílenou paměť. Dnes je již poněkud zastaralým standardem, více se v praxi používá novější, rychlejší a již jmenovaný protokol OPC, který může plnit stejnou funkci.

O realizaci komunikace se stará klient, který inicializuje DDE konverzaci a dále i řídí probíhající výměnu dat. Server potvrdí otevření spojení a následně je pouze pasivním členem konverzace, který odpovídá na žádosti a poskytuje informace klientovi. Ukončení DDE konverzace může provést jak klient, tak server. Typy komunikačních linek jsou celkem tři v závislosti na skutečnostech, při kterých proběhne přenos dat:

- Cold link – přenos proběhne pouze na základě požadavku od klienta,
- Hot link – automatický přenos probíhá v tu chvíli, kdy dojde ke změně dat na serveru a
- Warm link - při modifikaci dat server nejprve pošle informaci klientovi o změně dat a až po potvrzení přenosu klientem dochází k odeslání.

Při započetí DDE konverzace klientem zašle serveru název požadované služby (aplikace) a téma (subjekt, např. datový soubor). Tyto dva typy prvků konverzace nelze během přenosu

měnit. Následně se odesílá prvek, který identifikuje přeposílaná data (položka databáze, buňka tabulky) během konverzace. [24]

3.1.1.4 Ascii protokol

Komunikace prostřednictvím tohoto protokolu probíhá způsobem příkazů a odpovědí. Hostitelský počítač (server) posílá příkazy danému ovládanému zařízení ve formě Ascii znaků. Řízené zařízení pak odpovídá ve stejném formátu dat. Aby bylo možné realizovat komunikaci v Ascii kódu, je třeba nadefinovat příkazový konfigurační soubor, ve kterém jsou ke konkrétním Ascii znakům přiřazeny příkazy pro řízení, ovládání, zápis a čtení dat ze zařízení. Definice konfiguračního souboru je závislá na konkrétním výrobci.

Tab. 1: Skladba Ascii sekvence příkazu [25]

#	AA	00	[Data]	[CS]	(CR)
Oddělovač	Adresa zařízení	Příkaz	Data	Kontrolní součet	Návrat vozíku

Každý příkaz Ascii sekvence je série Ascii znaků, která vždy začíná předponou neboli oddělovačem, který kromě znaku # **o** hodnotě Ascii 0x23 hex (v hexadecimální soustavě) může být vyjádřen znaky %, $, @ anebo znakem ~. Každá sekvence končí znakem návratu vozíku (CR), také zakončovacím znakem, vyjádřeném 0D hex. Mezi počátečním a zakončovacím znakem se nachází adresa zařízení, se kterým je potřeba komunikovat. Adresa je vyjádřena dvoumístným polem AA, jež může nabývat hodnot 00 až FF hex. Následující pole obsahuje konkrétní příkaz, který má zařízení provést. Seznam příkazů a jejich Ascii vyjádření závisí na každém výrobci dané technologie a bývá uveden v příkazovém seznamu manuálu k danému zařízení. V poli data jsou uvedené hodnoty potřebné pro vykonání příkazu, popřípadě požadovaná data serverem. Volitelnou položkou je kontrolní součet [CS] uvedený bezprostředně před zakončovacím znakem. Účelem použití kontrolního součtu je rozpoznání komunikační chyby, která by nastala při přenosu. Je-li kontrolní součet neplatný, zařízení příkaz ignoruje a požadovaný úkon se provede až po přijetí příkazu s platným kontrolním součtem. [25]

3.1.1.5 Formát XML

Formát xml je zkratkou eXtensible Markup Language a v překladu znamená rozšířitelný značkovací jazyk. Byl vyvinut za účelem výměny dat mezi aplikacemi a pro publikování

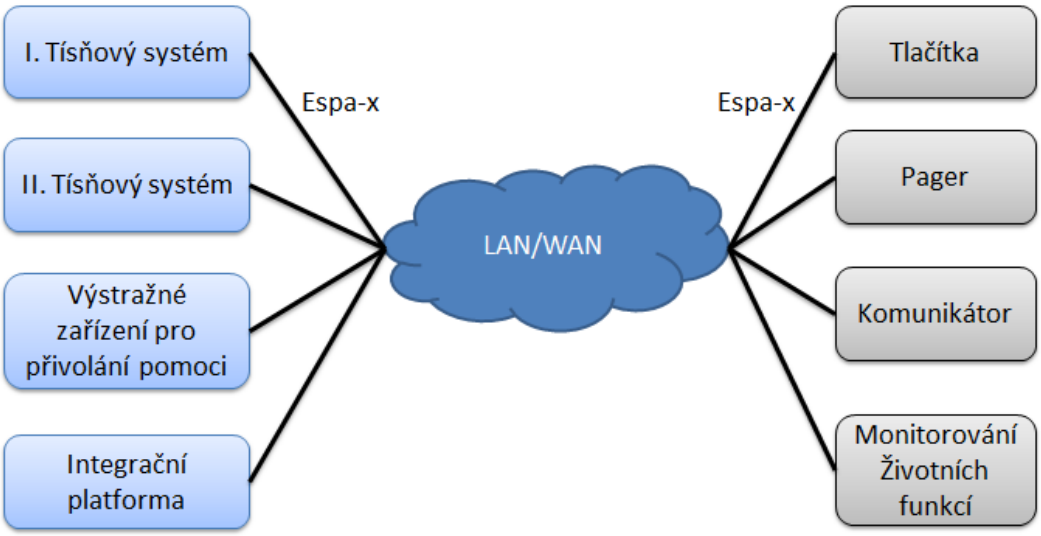
dokumentů. XML formát není jazyk, který je určen pro zobrazení dokumentů, jako je jazyk HTML, ale představuje formát dokumentů obsahující popis dat a jejich strukturalizaci. Jinými slovy předepisuje, jak zapsat data společně s jejich významem. Není tak úzce svázán s nějakou konkrétní platformou nebo proprietární (datově uzavřenou) technologií, která by vyžadovala speciální program pro zpracování komunikace. XML vynalezla konsorcia W3C a specifikace formátu XML je zdarma přístupná na jejím webu. Každý výrobce tak může bez problémů implementovat podporu tohoto formátu. Velkou výhodou použití tohoto standardu je to, že dokumenty obsahující instrukce a data psaná v XML mohou být přenášeny na jakoukoliv softwarovou platformu nebo zařízení bez ztráty informace. Svou jednoduchostí, rozšiřitelností a otevřeností se stal univerzálním komunikačním formátem. [26]

```
<?xml version="1.0" encoding="UTF-8" ?>
<system>
 <pzts>
    <podsystem="3" zona="2">zastřežit</prikaz>
    <podsystem="3" zona="3">zastřežit</prikaz>
 </pzts>
 <skv>
    <dvere="1" zona="2">blokovat</prikaz>
    <dvere="2" zona="2">blokovat</prikaz>
    <dvere="1" zona="3">blokovat</prikaz>
 </skv>
</system>
```

Obr. 13: Příklad deklarace XML dokumentu

3.1.1.6 Rozhraní Espa-x

Protokol Espa-x (Enhanced Signaling Protocol for Alarm Processes – XML-based) vychází ze standardního sériového datového rozhraní Espa, které bylo určeno zejména pro tísňovou signalizaci zdravotním sestrám a pečovatelům prostřednictvím mobilního rádiového pageru. Vlivem měnících se požadavků na mobilní tísňovou signalizaci a zavedením TCP/IP standartu pro VoIP (voice over IP) byl modifikován i Espa protokol na Espa-x, který je již založen na architektuře klient/server a standardu XML pro použití v LAN a WAN sítích. Integrační platforma s tímto implementovaným komunikačním protokolem umožňuje propojení různých bezpečnostních a komunikačních systémů s tísňovými systémy včasného varování určené především pro zdravotnické zařízení, domy s pečovatelskou službou a podobně. [27]



Obr. 14: Komunikace s pomocí protokolu Espa-x [27]

3.1.1.7 Protokol SNMP

Transakčně orientovaný protokol SNMP (Simple Network Management Protocol) je založený na modelu architektury klient/server a pro vlastní komunikaci používá protokol UDP neboli User Datagram Protokol, jež je vhodný pro servery, které obsluhují mnoho klientů směřující na ně dotazy. Použití protokolu je jednoduché a široce rozšiřitelné. Používá se především pro nastavování hodnot na určitém zařízení připojeném k datové síti a získávání hodnot z těchto zařízeních. Komunikace probíhá mezi správcem (snmp klient) představovaný například jednoduchým snmp prohlížečem a agentem (snmp server) na straně decentralizovaného zařízení. Režimy přenosu zpráv jsou dva, kdy při prvním správce zasílá cílené dotazy agentovi a zpětně přijímá od něho odpovědi, přičemž správců může být i více. Druhý režim spočívá v asynchronním způsobu komunikace, při které agent zasílá zprávy a hodnoty správci nebo správcům v nepravidelných intervalech. Asynchronní režim přenosu je zvlášť výhodný při vzniku nepředvídatelných situacích například při vzniku poruchy nebo sabotáže subsystému, kdy agent ihned informuje správce.

Tab. 2: Skladba SNMP datového paketu [28]

verze SNMP	community string	PDU typ	ID dotazu	error status	error ID	OID	hodnota

Existuje několik verzí protokolu SNMP. První dvě verze SNMPv1 a SNMPv2c používají pro autentizaci tzv. community string představující heslo ve formě textu, třetí verze SNMPv3 je zabezpečena zašifrovaným jménem a heslem. PDU typ je typ SNMP dotazu, uvádějící jestli jde o dotaz nebo odpověď. ID dotaz číselně identifikuje vznesený dotaz, ID error zase číslo poruchy, pokud není error status nastaven na: no error. OID uvádí adresu zařízení a hodnota obsahuje data pro nastavení. Nevýhodou tohoto standardu je, že použití UDP protokolu nezaručuje doručení datového paketu. Od verze 2 je však implementována kontrola o doručení zprávy. [28]

3.1.1.8 Html jazyk

Html je programovacím značkovacím jazykem používaný pro tvorbu webových stránek, které mohou sloužit jako uživatelsky klientské rozhraní, jehož prostřednictvím je možné vzdáleně ovládat integrovaný systém. Zkratka html vychází z názvu Hyper Text Markup Language a jednotlivé stránky html nebo záložky jsou propojeny hypertextovými odkazy. Html je hlavním nástrojem pro předávání relativně objemných dat, např. obrazové informace a vzdálenou správu a konfiguraci systémů v síťovém prostředí. [29]

3.1.1.9 Fórum Onvif

Onvif (Open Network Video Interface Forum) představuje otevřené průmyslové fórum pro vývoj a rozvoj globálního komunikačního standartu pro zařízení přenášející data prostřednictvím IP technologie. Specifikace Onvif definuje společný protokol pro výměnu dat a informací mezi síťovými prvky jako jsou síťové videorekordéry, servery, kamery a video management systémy (zkráceně VMS). Kromě výměny dat umožnuje taktéž automatické vyhledávání daného zařízení v lokální síti, video streaming a poskytování inteligentních metadat o kamerových záznamech pro další zpracování. Souhrnně tedy fórum Onvif zajišťuje interoperabilitu mezi síťovými produkty a to bez ohledu na výrobce. V dnešní době komunikační standard podporuje více než 500 výrobců síťových zařízení. Technologie je založena na protokolech SOAP a RTP a jako komprimační formáty používá motion JPEG, MPEG-4 a H.264. Verze standardu Onvif se dělí na takzvané profily, jež snadno umožňují uživatelům identifikovat specifické vlastnosti interoperability a zajistit kompatibilitu zařízení.

a) Profil S je určený pro IP video systémy a podporuje video a audio streaming, PTZ ovládání, řízení výstupního relé kamery a video konfiguraci.

b) Profil C byl vyvíjen pro systémy kontroly vstupu založených na IP technologii poskytující informace o konfiguraci, událostech, alarmech stejně jako řízení přístupu.
c) Profil G slouží pro ukládání a načítání konfigurací, kontrolu nahrávání v zařízení a taktéž slouží pro příjem zvuku a metadat z kamerového bodu.
d) Profil Q představuje mechanismus pro nastavení pokročilého zabezpečení, konfiguraci a datové integrity. [30]

Dílčí závěr kapitoly

V kapitole byly stručně popsány typy rozhraní a uvedeny nejčastěji užívané univerzální komunikační standardy uplatňované při komunikaci mezi integrační platformou a jednotlivými systémy integrovaného poplachového systému. Ohledně této problematiky existuje mnohem více komunikačních rozhraní a protokolů, vyvíjených speciálně pro provázání konkrétních systémů, kterých je v praxi vhodné přednostně používat pro danou aplikaci. Vhodným příkladem může posloužit specifický komunikační protokol GXYSMART, vyvíjený za účelem přenosu dat mezi konkrétním integračním systémem C4 a bezpečnostními systémy od společnosti Honeywell.

II. PRAKTICKÁ ČÁST

4 ANALÝZA INTEGRAČNÍCH PLATFOREM

Oddíl věnující se integračním platformám nejprve charakterizuje tyto integrační nástroje pro centralizovanou správu. Následně se kapitola již věnuje odborným analýzám a rozboru vlastností použitých technologií několik konkrétních integračních platforem, které jsou momentálně dostupné na trhu. Na základě provedených analýz je pak provedená komparační studie integračních platforem.

4.1 Integrační platforma

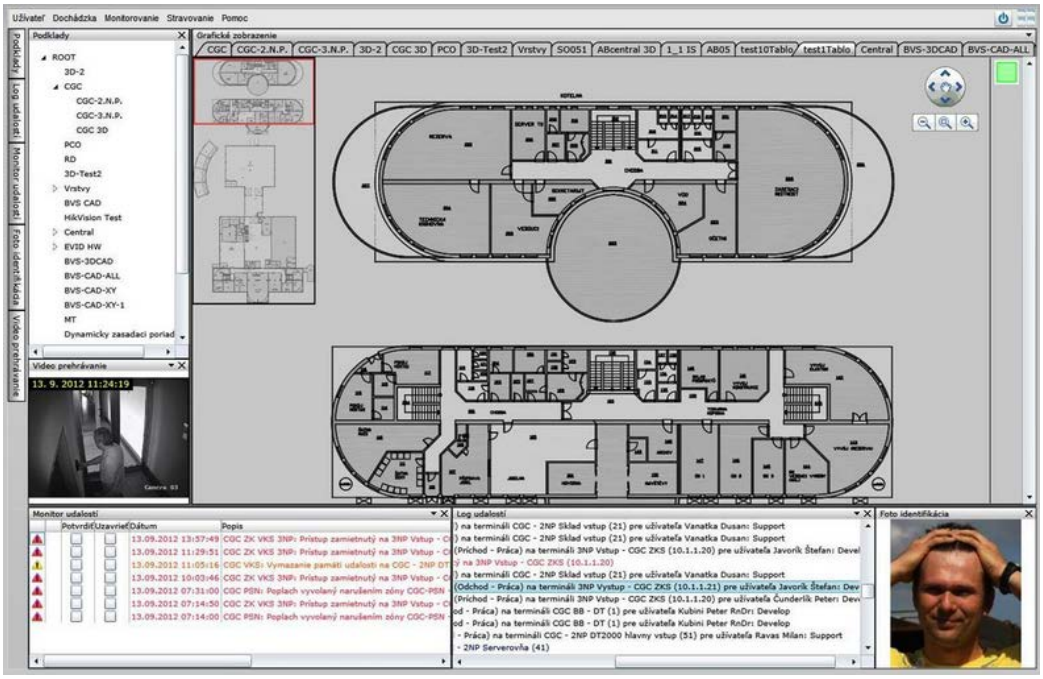
Integrační platforma slouží k vlastní softwarové integraci různorodých bezpečnostních technologií do jednoho celku za účelem centrální správy zařízeních podílející se na objektové bezpečnosti chráněného prostoru. Princip systému je založen na propojování na sobě zcela nezávislých zařízení a technologií od různých výrobců, spravování jejich činností z jednoho dozorového místa, v jednom přívětivém a přehledném uživatelském prostředí. Důležitým aspektem těchto SW řešení je, jak už bylo uvedeno i v legislativních nárocích, že jednotlivá zařízení nejsou vzájemně ovlivňována. Použitím tohoto sofistikovaného řešení uživatel získává nejen větší efektivitu v řízení komplexní bezpečnosti ale i výrazné snížení nákladů na zaškolení obsluhy tohoto systému vlivem jednotného ovládání všech technologií. Aplikováním integrační platformy získáme efektivní nástroje pro:

- centrální správu všech bezpečnostních zařízení v objektu,
- monitoring a řízení jednotlivých systémů v objektech,
- grafickou vizualizaci bezpečnostních zařízení,
- zautomatizování bezpečnostních postupů a procesů,
- komplexní analýzy a vyhodnocení bezpečnostních rizik a informací a
- centrální management identit. [31]

V závislosti na požadavcích uživatelů, rozsah vlastností systému a kombinacích různých výrobců bezpečnostních technologií jsou k dispozici následující integrační platformy: Alvis, SBI, C4, Integra, VAR-NET Integral, Latis SQL a AxxonSoft jejichž analýzy budou předmětem dalších podkapitol.

4.1.1 Platforma SBI

Software Secure Building Inteligence, uváděný na trhu pod zkratkou SBI je systém určený pro komplexní obsluhu veškerých elektronických bezpečnostních systémů v objektu. Je vyvíjen slovenskou společností CGC a.s., jejíž hlavní vizí je přinášet na trh nové integrované řešení pro efektivnější monitorování, ovládání a správu technologií od různých výrobců. Kromě veškerých poplachových aplikací umožnuje propojení s docházkovými a parkovacími systémy, stravovacími systémy, systémy pro měření a regulaci (zkráceně MaR) a environmentální systémy. [32]



Obr. 15: Ukázka SW SBI [32]

Jde o modulární systém, uživatel si tedy při realizaci systému v objektu zvolí jednotlivé moduly z hlediska využitelnosti. V použití modulárního systému spočívá i velká flexibilita, je tedy možné systém dovybavit, popř. rozšířit či přizpůsobit a tím navýšit funkcionalitu systému a to vše bez ztráty dat. Základní princip činnosti systému spočívá v použití databázového prostředí MS SQL2008 (MS SQL Express), ve kterém se shromažďují veškeré informace a data z jednotlivých aplikací a zároveň personální údaje. Architektura SBI je postavena na systému klient/server (databázový server) s podporou TCP/IP protokolu s možností lokálního přístupu, tak i vzdáleného prostřednictvím webového prohlížeče nebo mobilní aplikace. Sběr dat z jednotlivých podsystémů může probíhat dvěma způsoby: prvním způsobem je přenos přes rozhraní RS 232 a druhý způsob, v praxi více využívaný

z důvodů využití již existující infrastruktury budovy, je přenos prostřednictvím LAN, WAN popřípadě i GPRS sítí s protokoly opc, modbus a snmp. K dispozici jsou celkem tři typy řešení integrace:

- SBI Easy,
- SBI a
- SBI Portál.

SBI Easy

Jako základní edice je SBI Easy určená pro nasazení v rámci menších a středních rozsahů integrace. Avšak i tak podporuje většinu funkcionalit jako je správa zařízení PZTS, EPS, SKV, VSS a v rámci nepoplachových aplikací: HVAC (heating, ventilating, air-conditioning neboli topeni, větráni a klimatizace), environmentální a MaR systémy. Dále nástroj umožnuje vlastní správu chráněných oblastí, grafické zobrazení průběhu veličin i s kalendářem pro regulaci s regulačními křivkami a samozřejmostí je možnost importu a exportu dat ze systému. Technické limity jsou stanoveny především v současném připojení max. 6 zařízení, VSS a digitální videorekordér může obsahovat jen 20 kamer a oprávnění a formy přístupů jsou již předdefinovány. Ohledně správy osob lze v SW evidovat maximálně 800 identit, docházka může být zpracovávaná pro 400 osob. Stravovacím subsystémem se v této verzi myslí zpracování dat jen pro jednu jídelnu. Mezi volitelné funkce patří mapová vizualizace s editací, správa návštěv, definování pokynů pro operátory integrovaného systému, zavedení mobilních klientů a notifikace stavů a událostí v systému. Hlavní předností této verze je především v pozměněné skladně systému, protože je využíváno členění podle funkcí systému nikoliv podle modulů. Tím se rapidně zjednoduší orientace při vytváření konfigurací, ovládání systému, odstraňují se nevyužité prvky a sníží se počet nutných nastavení. Nespornou výhodou je taktéž nízká cena i s možností upgradovatelnosti na vyšší verzi.

SBI

Produkt SBI je určen pro komplexní obsluhu a řízení všech systémů i v oblasti systémových integrací technologií budov a to již bez žádných limitů v rozsahu instalace. Oblast použití leží ve středních až velmi velkých projektech a to především v provozním režimu 24/7. V porovnání s předchozí edicí obsahuje veškeré uvedené funkcionality a navíc umožňuje podporu více typů identifikátorů v rámci přístupu, správu aplikovaných pro-

středků, zpracování žádostí o přístup popřípadě delegování pravomocí pro přístup. Disponuje nástroji pro pokročilé docházkové sestavy, kontrolu fondu docházky, plánování schůzek a prostředky pro krizové řízení při vzniku mimořádné události. Součástí je správa automobilů a pokročilá možnost replikace dat. Edice obsahuje licenci již pro dva databázové servery pro zvýšení redundance a tím zvýšení stability systému. Šíří použitelnosti, sofistikovaností a funkcionality poskytuje nelimitovaná řešení i mimo rámec bezpečnostních systémů.

SBI Portál

Verze Portál neboli portálové řešení je koncipováno jako virtuální instalace na dedikovaném severu společnosti C.G.C. SBI není tedy instalován lokálně v rámci klientské společnosti a není tedy nutné provozovat vlastní vyhrazený server s příslušným SW vybavením. Směrem k obsluze systému se program a jeho obsluha provádí stejně jako u verze SBI. K používání a obsluze systému je zapotřebí jen internetové připojení a webový prohlížeč bez nutnosti instalace klientských programů avšak míra bezpečnosti zůstává identická v závislosti na potřebách klienta. Z hlediska funkcionality je portálové řešení koncipováno totožně s plnohodnotnou edicí SBI bez jakýkoliv limitů. Unikátní koncept cloudového řešení je vhodné především pro domácnosti a malé podniky. Velkou výhodou je zde absence počátečních velkých investic do realizace systému, protože provoz je hrazen formou pronájmu a automatická údržba a upgrade integrovaného systému.

Všechny edice podporují vícejazyčnost (čeština, slovenština, angličtina, němčina). Integrita systému je zaručena jeho otevřeností s podporou mnoha výrobců bezpečnostní techniky. Je zcela nezávislý na použitém hardwaru, stále doplňován o nové technologie a vyvíjen s požadavky na rozšiřování funkcionality podle nejnovějších trendů. Mezi významné podporované výrobce například patří Honeywell, Paradox, DSC, Siemens, AXIS, Samsung, BOSH, Canon, JVC, Hikvision, Job Detectomat, Zettler a dalších 83 uvedených na webu výrobce.

4.1.2 Integrační bezpečnostní systém C4

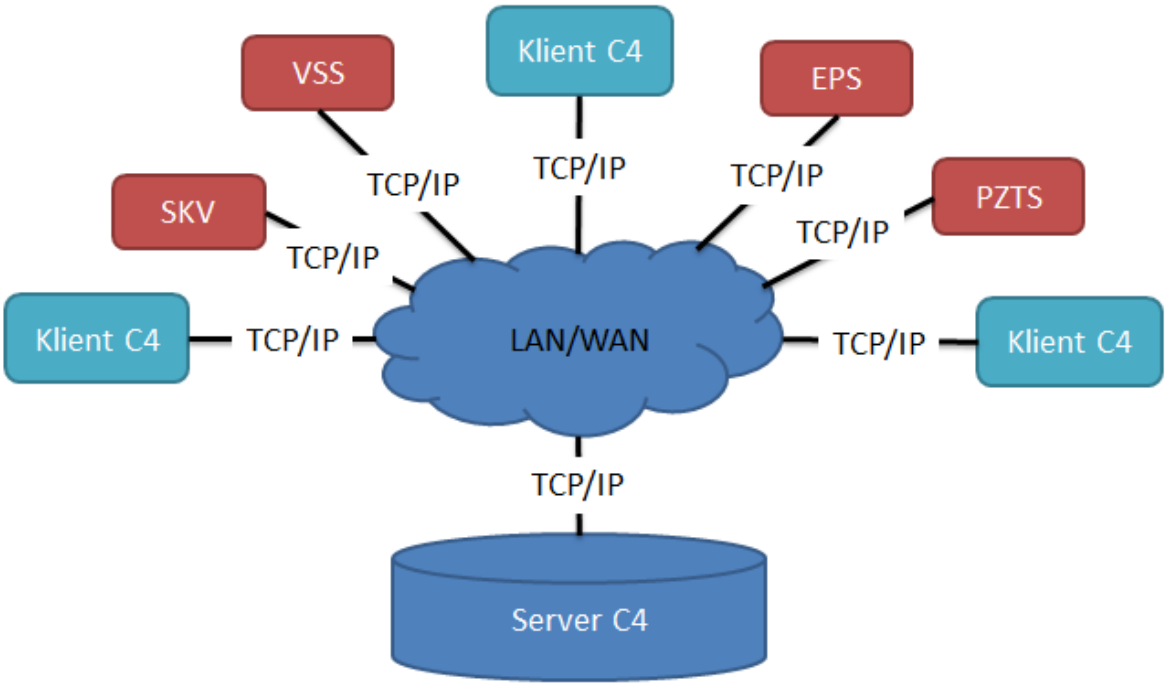
Slovenská společnost Gamanet a.s. uvádí na trh systém C4, který poskytuje softwarovou platformu pro potřeby integrace veškerých bezpečnostních systémů, jako jsou systémy PZTS, EPS, SKV, VSS a perimetrické systémy do jednoho komplexního řešení. Svojí ši-

rokou funkcionalitou a konfigurací přizpůsobenou k nepřetržitému monitorování všech technologických zařízení a subsystémů plně nahrazuje pracoviště DPPC avšak na rozdíl od typických vzdálených center umožnuje i zpětnou vazbu – řízení technologií jako je například zastřežení, odstřežení systému, přemostění zón, zrušení poplachů, zapínaní a vypínaní různých zařízení apod. Kromě uvedených systémů, které byly jmenovány, lze integrovat i klimatizační a odvětrávací systémy, nástroje pro zpracování docházky, řízení parkovišť a stravovací systémy. Oproti jiným integračním platformám tato platforma umožňuje v rámci svého monitorovacího modulu připojení na externí geografické informační systémy (zkráceně GIS) a tím obsluze systému poskytovat podpůrné informace pro podporu rozhodování a řízení při vzniklých mimořádných krizových situacích. Příkladem může být poskytnutí GIS dat ohledně lokalizace potrubí, elektroinstalace, plynovodu v prostoru, kde byl vyhlášen poplach vlivem vzniku bezpečnostního incidentu. [33]

Obr. 16: Uživatelské rozhraní systému C4 [33]

Systém je založen na klient/server architektuře a optimalizován pro centralizovanou správu podsystémů. Server obsahuje jednotnou centrální databázi jak pro data veškerých technologií, tak i data pro celkovou správu uživatelů. Jde o modulární systém s jednotným jádrem, který lze konfigurovat s ohledem na konkrétní potřeby uživatele od malých aplikací – jedna budova až po velmi rozsáhlé aplikace jako je monitoring bezpečnostních zařízení ve velkých organizacích a jejich objektech bez ohledu na vzdálenostech. Integrace jednotlivých zařízení od externích výrobců je založena na použití ovladačů se standardem snmp,

které zajišťují komunikaci se systémem C4 v maximálním rozsahu, které dané zařízení poskytuje. Komunikace probíhá prostřednictvím TCP/IP a transparentního rozhraní – Web Services, což umožnuje aplikaci veškerých funkcionalit obsažených v systému C4 a zároveň i použití nástrojů a aplikací třetích stran. [33]



Obr. 17: Architektura integračního systému C4 [34]

Otevřenost celého systému umocňuje jeho otevřenost pro externí vývojáře třetích stran pomocí standartu WSDL (Web Services Description Language). Standart WSDL je založen na jazyku pro definici webového rozhraní, který stanovuje popis funkcí, které nabízejí webové služby. Zjednodušeně tento standart poskytuje parametry, popis způsobů komunikace, typy datových struktur apod. potřebných pro integraci. V rámci platformy C4 je k dispozici podpůrný balíček SDK (Software development kit, soubor nástrojů pro vývoj software). Systémový vývojový nástroj tak dává možnost přímo výrobcům zařízení vyvinout ovladač na nový, dosud C4kou nepodporovaný systém a tím podpořit integrovatelnost svých technologií. K dispozici jsou tři edice systému C4:

- OEM,
- Standard a
- Advanced.

Mezi edicemi jsou hlavní rozdíly patrné v poskytovaných nástrojích a funkcionalit, jež jsou znázorněny v komparační tabulce. Výhodou systému C4 bez ohledu na typ edice je neomezený počet klientů, kdy se na server můžou připojovat uživatelé i vzdáleně. Počet obsluhovaných klientů je omezen jen výpočetním výkonem serveru.

Tab. 3: Porovnání různých edic systému C4 [34]

	OEM	Standard	Advanced
Správa osob	+	+	+
Správa oprávnění a přístupů	+	+	+
Správa a ovládání zařízení	+	+	+
Zobrazení stavů zařízení	+	+	+
Monitoring a vizualizace	+	+	+
Online zobrazení záběrů z kamer	+	+	+
Zobrazení kamerového záznamu	+	+	+
Import a export osob a zařízení	+	+	+
Záloha dat systému	+	+	+
Zobrazení/Tisk událostí	+	+	+
Podpora denních kontrol EPS	+	+	+
Zasílání událostí emailem/SMS		+	+
Evidence návštěv		+	+
Automatizované akce		+	+
Poplachové směrnice		+	+
Karty objektů			+
Správa obchůzek			+
Výměna dat s externími IS			+
Licence pro 2 servery (redundance)			+

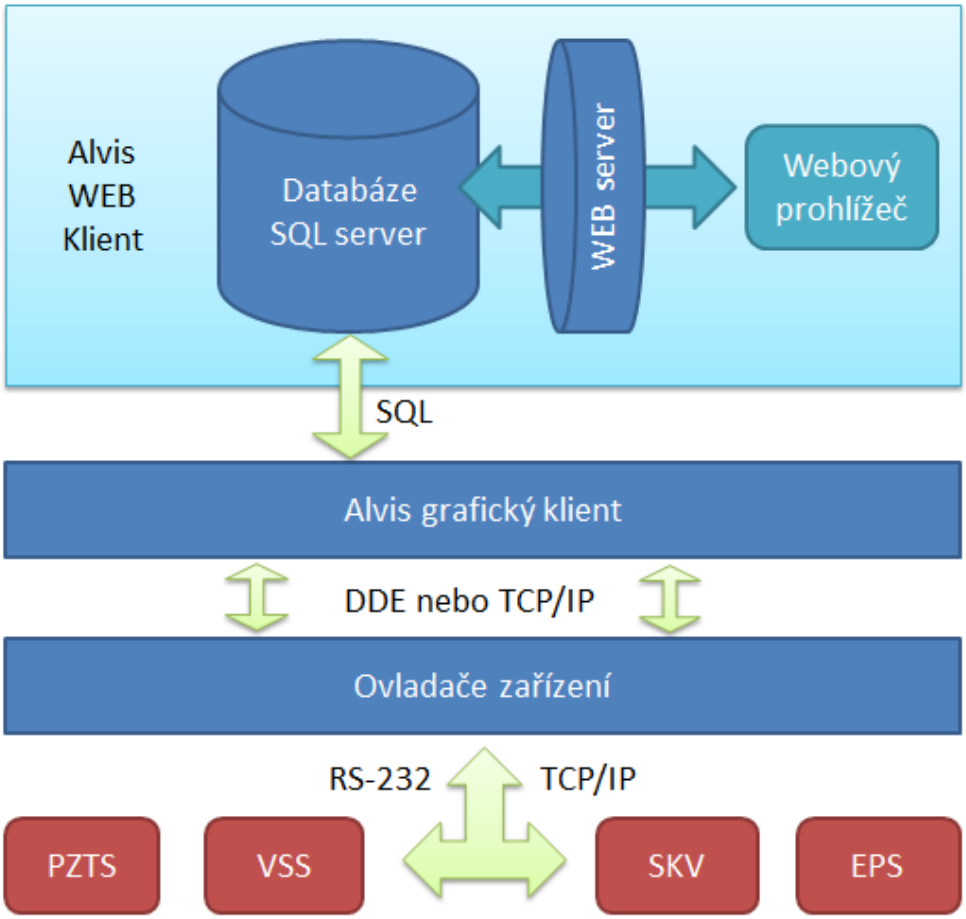
Systém C4 je vhodný pro použití v průmyslových centrech, administrativních budovách, v obchodních řetězcích a ve velkých korporací stejně jako DPPC bezpečnostních agentur. Mezi výrobce bezpečnostních systémů, kteří jsou již systémem C4 podporovány patří jmenovitě například: Satel Integra, Galaxy, ATEAS Security, Concept, Avigilon, Axis, Geviskope, Hikvision, Esser, Fibrolaser, Sinteso, Bosh, Siements, Perisys a dalších cca 57 výrobců.

4.1.3 Vizualizační a integrační program Alvis

Grafický vizualizační systém Alvis, aplikovaný rovněž pro integraci, správu, řízení a monitorování různých technologií obsažených v budovách je vyvíjen slovenskou firmou SPIRIT - informačné systémy a.s. Alarm Visualization systém, jak je nezkráceně označován, je univerzální grafické vývojové prostředí, který je určen pro tvorbu monitorovacích a řídicích systémů. Podporuje integraci víc jak sto zařízení od různých výrobců poplachových zabezpečovacích systémů, systémů požární ochrany, zařízení pro kontrolu přístupu, kamerových systémů MaR systémů. Použitím platformy Alvis může mít přínos i v automatizovaném provázání různých systémů v rámci řešení havarijních a evakuačních situací v objektu. Samotný systém však nepodporuje kontrolu docházky ani parkovací a stravovací systémy oproti předešlým programům.

Alvis systém je modulární systém založený na architektuře typu klient-server obsahující databázový server, popřípadě Web server s přístupem na veřejnou internetovou síť. Vlastní software Alvis je pouze klientem, který zprostředkovává uživateli přehlednou vizualizaci stavu monitorovaných objektů. Z pohledu informační bezpečnosti je použita kryptografická ochrana vlastního aplikačního souboru Alvisu, dále je i možnost ochrany grafických podkladů a hlavně souboru protokolů programu obsahující reporty. Pro svoji specifickou činnost využívá služeb programových serverů, jež poskytují potřebná data pro monitoring a řízení technologií a přímo komunikují s připojenými zařízeními a subsystémy. Množství programových serverů neboli ovladačů i klientů je neomezené a ke komunikaci mezi nimi se používá buď síťový TCP/IP protokol nebo standartní protokol DEE (Dynamic Data Exchange) v případě lokální komunikace. Přenos dat mezi severem s ovladači a konkrétním systémem PZTS, EPS, EKV nebo VSS může probíhat taktéž přes protokol DEE, nebo přes některý z univerzálních komunikačních protokolů OPC, Modbus, Espa-x nebo Ascii.

Je-li systém uveden již v portfoliu podporovaných zařízení na webových stránkách výrobce Alvisu, jsou již ovladače na příslušnou technologii naprogramovány a odladěny. Pro představu je uváděno jen několik výrobců poplachových systémů: BENTEL, Paradox, Honeywell , Siemens, Tyco, Bosch, Assa Abloy, Milestone a Samsung. [35]



Obr. 18: Architektura systému Alvis [35]

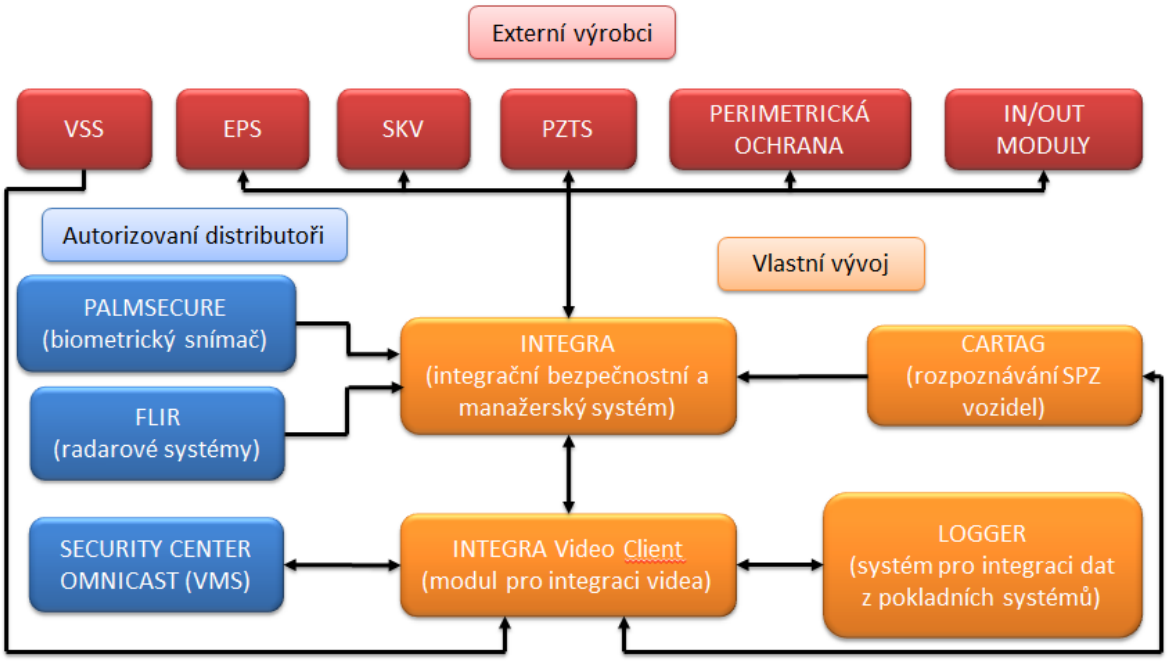
Z pohledu různých verzí programu je k dispozici Alvis a Alvis WEB. Alvis koncipován pro všechny typy a rozsahy aplikací, od malých instalací, jako je monitoring a řízení několik prvků až po velmi rozsáhlé aplikace, zahrnující velký počet připojených prvků a systémů. Alvis WEB je potom pouze programový modul jako doplněk k standartnímu systému, jež slouží pro rozšíření klientských stanic prostřednictvím internetového prohlížeče primárně pro vizualizaci systému, popřípadě k zobrazení protokolových zpráv o stavech monitorovaných bodů instalace. Při integraci platformy Alvis WEB se systém doplní o server s instalovanou SQL databází, web serverem Apache a sadou skriptů, které tvoří samotnou aplikaci Alvis WEB. Přes program Alvis WEB rozhodně nelze měnit vlastní konfiguraci integrovaného bezpečnostního systému.

Tab. 4: Technické předpoklady uvedené pro systém Alvis [35]

HW součást	Doporučená konfigurace
Procesor	min. Pentium II a lepší
Operační paměť	512MB RAM a více
Pevný disk	min. 120 GB
Operační systém	MS Windows 7, 8.1, Windows Server 2003/2008

4.1.4 Platforma Integra

Systém Integra propojuje různá bezpečnostní a slaboproudé technologie a zařízení do jednoho kompaktního a přehledného celku s cílem snadného a velmi efektivního ovládání všech různorodých zahrnutých podsystémů. Je vyvíjen českou společností Integoo s.r.o., která plní roli systémového integrátora a kromě integračního a manažerského SW Integra se zabývá vývojem systému pro rozpoznávání značek Cartag, VMS Integra Video Client a systému Logger pro zaintegrováni dat z externích systémů (především pokladních systémů). Platforma Integra tedy integruje, vizualizuje a řídí veškeré technologie ať už vlastní výroby nebo distribuované, popřípadě technologie třetích stran. Hlavní úlohou integrovaného systému je poskytovat informace pro podporu řízení a rozhodování odpovědného personálu a zároveň poskytovat nástroje pro realizaci manuálního ale především automatického ovládání i s vazbami mezi systémy jednotlivých autonomních technologií. [36]



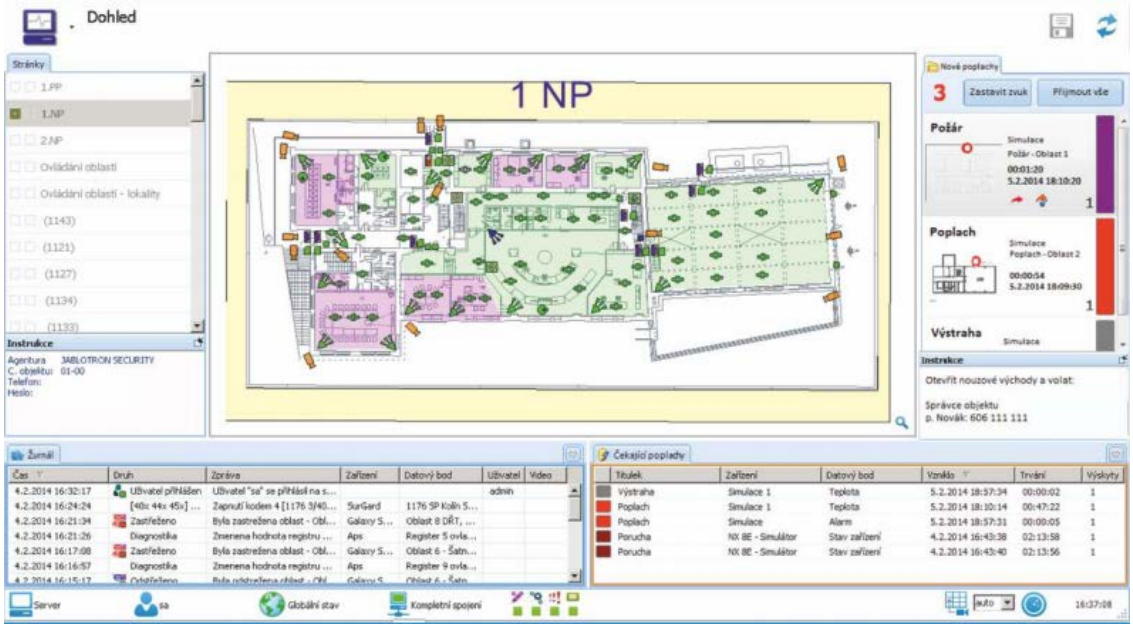
Obr. 19: Technologie obsažené v SW Integra [36]

Jak je již patrné ze schématu, lze v platformě integrovat systémy VSS, SKV, PZTS, EPS a perimetrické systémy. Začleněním modulu Integra Video Client do systému pak uživatel získává i prostředky a nástroje pro pokročilou videoanalýzu včetně integrace rozpoznávání registračních značek. Systém je koncipován na architektuře klient/server a kromě vlastního používaného rozhraní lze do systému připojit subsystémy prostřednictvím otevřených standardů Modbus, OPC, I/O a TECO. Systém Integra je na trhu nabízen ve dvou verzích Prime a Direct. Mezi základní funkcionality, které obsahují obě verze, patří půdorysné vizualizace chráněných objektů, možnost implementace směrnic k objektům a k vzniklým bezpečnostním událostem a tagování (značení) videa k určitým událostem. Odlišnosti mezi edicemi jsou pak přehledně znázorněny v tabulce níže.

Tab. 5: Rozdíly mezi edicemi Prime a Direct [36]

	Integra Prime	Integra Direct
Počet datových bodů (licence v základu)	**100**	**200**
Maximální počet zařízení	**8**	∞
Maximální počet objektu	**8**	∞
Maximální počet klientů	**4**	∞
Mobilní klient	**-**	**+**

Platforma obsahuje vlastní grafický editor pro vytváření a úpravu mapových podkladů a umožnuje dle konkrétních požadavků i vlastní konfiguraci symbolů charakterizující činnost prvků v rámci systému. Samozřejmostí je export popř. import uživatelských sctiptů a již jmenovaných symbolů. Počet událostí a jejich historie je závislá na velikosti databáze, kterou si uživatel zvolí. Obsluha pak následně může v historii vyhledávat informace podle textu nebo konkrétních parametrů.



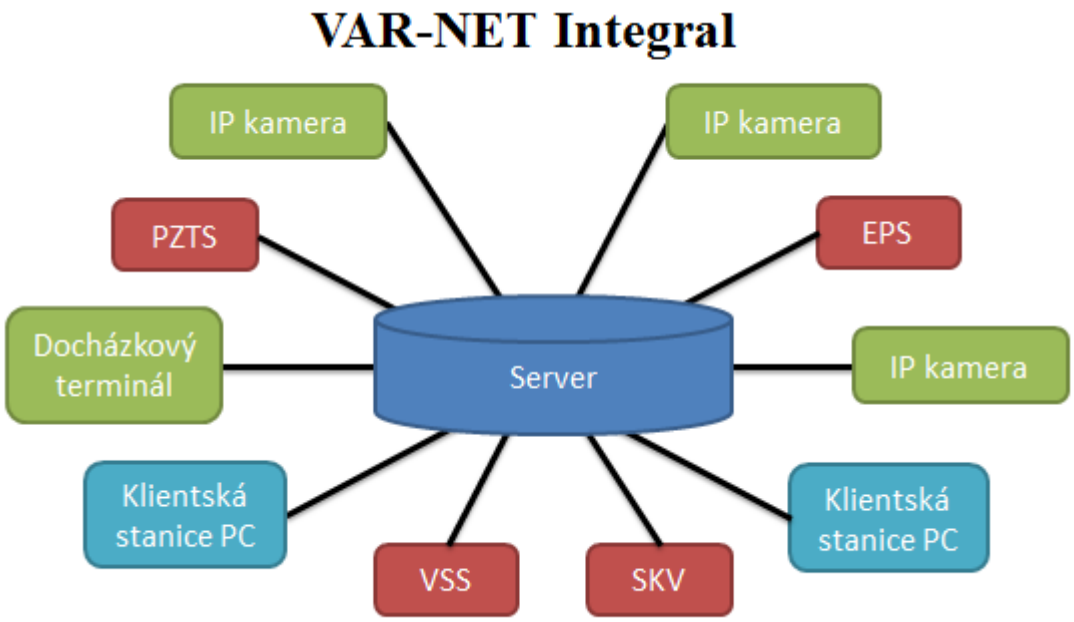
Obr. 20: Náhled do aplikace Integra Direct [36]

4.1.5 Systém VAR-NET Integral

Integrační platformu VAR-NET Integral vyvíjí a na trhu nabízí česká firma Variant plus spol. s r.o. Kromě zmíněné integrační platformy společnost vyvíjí i SW Security View, který je typickým představitelem vizualizačního programu v rámci kterého lze propojit pouze ústředny PZTS značky Digiplex Evo v maximálním počtu 6 na jednu aplikaci.

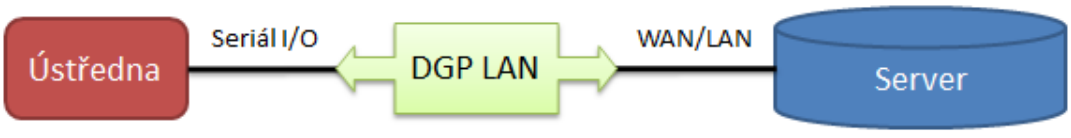
VAR-NET Integral je systém pro správu, ovládání, sledování a vyhodnocování elektronických systémů instalovaných v budově a to v reálném čase. Integrační řešení, které firma Variant plus nabízí je určeno spíše pro objekty menšího až středního rozsahu. Umožňuje integraci technologií PZTS, EPS, VSS, SKV, ENVIRO a také kontrolu docházky a stravovací systém. Jde taktéž o modulární systém jako u většiny integračních platforem. Limitující faktory jsou pro tento systém následující:

- aplikace max. 6 volitelných okruhů (subsystémů),
- v rámci podsystémů je možné použít jen 2 VSS okruhy pro max. 20 kamer,
- celkově lze použít a pracovat s 2000 prvky,
- kontrola vstupu je omezena pro max. 800 osob se stanovenými přístupovými právy,
- registrace docházky až pro 400 osob (z 800 osob s přístupovými právy).



Obr. 21: Systém VAR-NET Integral [37]

Jako další volitelné funkce SW nástroje jsou k dispozici vizualizační mapové podklady, ze kterých lze ovládat veškeré připojené technologie s integrovaným nástroji pro konfiguraci vizualizačního modulu, prvky pro grafické plánování individuální docházky i s možností exportu dat do jiných, především mzdových systémů, modul pro plánování a správu návštěv a stravovací modul s praktickou kalkulací výdeje stravenek zaměstnancům. Charakterizující informace o systému a jeho funkcionalit jsou výrobcem uváděny pro základní verzi programu. V případě požadavků o rozšíření instalace o více okruhů nebo přesáhnutí některých z limitů nad rámec základní verze je možné přejít na vyšší verzi, která je k dispozici pouze v rámci konkrétního zakázkového řešení. V takovém případě může být uživateli poskytnut systém s žádným omezením v počtu ani v kombinaci okruhů, modulů a prvků, osob a půdorysů. Z pohledu poskytnutých funkcionalit by systém mohl být obohacen o nástroje krizového řízení a správy prostředků. [38]



Obr. 22: Komunikace zabezpečovací ústředny se serverem [38]

Platforma VAR-NET Integral používá architekturu klient/server, jak je znázorněno na obrázku 22. Operační systém serveru je Windows Web Server 2008 nebo Windows Server 2008. Pro centrální správu systému a osob je použita jediná databáze MS SQL Server 2008 popřípadě MS SQL Server 2008 Express, ve kterém probíhá logování všech vzniklých událostí ze všech subsystémů, stejně jako zaznamenávání všech uživatelských přístupů a ovládání jak z lokální sítě, tak z externí veřejné sítě (internetu). Vzhledem k plné podpoře TCP/IP protokolu nemusí být aplikace instalována pouze na lokální síti. Ústředny PZTS a EPS jsou k serveru připojeny pomocí modulu DGP LAN V+, který převádí procesorový výstup Seriál I/O základní desky ústředny do Ascii znaků do sítě LAN. Na straně počítače (serveru) se následně nainstaluje speciální SW Redirector, jež vytvoří na PC virtuální COM ze sítě LAN, na který se bude směrovat komunikace mezi serverem a ústřednou. Komunikace s uživateli je realizováno kromě klientské stanice s webovým prohlížečem pomocí volitelného modulu Notifikace, který zabezpečuje zasílání jen vybraných informací o systému prostřednictvím emailu a SMS a nebo modulu PDA klient, který ovládá integrovaný systém z smartphonu.

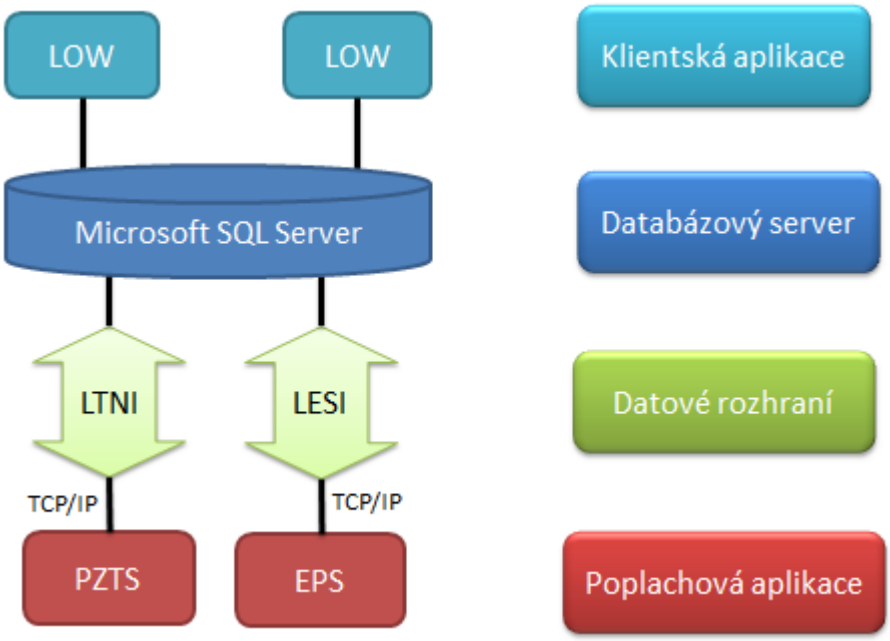
Tab. 6: Doporučená konfigurace serveru pro VAR-NET Integral [38]

Součást serveru	**Doporučená konfigurace**
Procesor	Dual Core 2GHz a nebo lepší
Operační paměť	4GB RAM nebo více
Pevný disk	min. 120 GB
Operační systém	Windows Web Server 2008, Windows Server 2008
SQL Server	MS SQL Server 2008, MS SQL Server 2008 Express

Zvláštností integrační platformy a zároveň jejím limitujícím prvkem oproti jiným platformám je systém kontroly vstupu, který lze začlenit do integrovaného bezpečnostního systému pouze jako nadstavbu konkrétního systému PZTS, kterým je systém Paradox Digiplex Evo. Systém VAR-NET Integral přímo podporuje integraci PZTS systémů: Honeywell Galaxy, GE-Aritech a zmíněný systém Paradox Digiplex Evo. Z řad systémů VSS jsou to produkty od firem ACTi, Axis, Canon a Pelco. V rámci EPS jsou přednostně integrovány ústředny Job Detectomat a dále systémy Lites a Esser. V případě požadavku na připojení HW, který není ve výčtu podporovaných systémů, sama společnost nabízí odborné konzultace s technickým oddělením ohledně dostupnosti vhodného ovladače.

4.1.6 Monitorovací a integrační systém Latis SQL

Produkt jménem Latis SQL je monitorovací a integrační systém české firmy Trade FIDES a.s., který může spravovat veškeré autonomní bezpečnostní systémy (PZTS, EPS, VSS a SKV) a technologie používané k ochraně budov i rozsáhlých technologických areálů. Kromě bezpečnostních systémů SW může ovládat i systémy měření a regulace. Latis SQL má dvě základní využití, která lze i vzájemně kombinovat. Platformu je možné použít pouze jako lokální grafickou nadstavbu umístěnou na vrátnici nebo recepci nebo jako plnohodnotný DPPC pro vzdálený dohled nad chráněnými objekty. V případě aplikace obou variant dohledu, ISB používá tzv. kaskádovité spojování pultů s interním protokolem i s vlastní kompresí dat. Obě varianty však disponují obousměrnou komunikací mezi dálkovým popřípadě lokálním pracovištěm dohledu a zabezpečovanými objekty. Díky této přednosti je možné spravovat jakoukoliv činnost systému, který je v dané budově řízen jednotkou bezpečnostního systému. Mezi časté prováděné činnosti řízení patří např. vypnutí sirény, zrušení poplachu, otevření nebo zamčení dveří apod. popřípadě lze nastavit opakující se události v určitý čas a dny prostřednictvím plánovacího kalendáře. [39]



Obr. 23: Schéma systému Latis SQL [39]

Integrační platforma Latis SQL je postavena na již osvědčené databázové technologii Microsoft SQL Server 2008. Použitím této technologie umožnuje efektivní zpracování a prezentaci velkých objemů dat a nabízí tak rozsáhlé možnosti pro zajištění redundanci dat

a tím i jejich bezpečnost zálohováním, archivací a replikací. Vysokou úroveň bezpečnosti deklaruje použití AES-128 kryptografické ochrany přenášených dat mezi systémy. Skladba systému je navržena jako rozsáhlá modulární za účelem sestavení podle potřeb zákazníka. Ke komunikaci využívá několik komunikačních kanálů jako je morse radio, SMS, email, telefon, GPRS, LAN RS232 a RS485 které používá k připojení a integraci veškerých technologií. Přenos dat mezi jednotlivými autonomními systémy a serverem je realizován prvky LTNI nebo LESI. Nástroj LOW je určen pro dohled nad hlídaným objekty a slouží jako klient k databázovému serveru. V rámci přesné lokalizace sledovaných objektů či oblastí je program navázán na vlastní mapové podklady pro obrazovou vizualizaci s reálnými souřadnicemi GPS. K editaci a správě mapových podkladů je k dispozici vlastní mapový editor zvaný FIDES Map Editor. Výhoda je i v možnostech exportu jakýkoliv dat z databáze SQL a to i metadat obsahující informace o přístupech a činnostech operátorů v rámci celého systému. Data tohoto typu pak lze zahrnout do reportů přizpůsobených podle konkrétních potřeb uživatele.

Mezi realizované projekty ochrany a ostrahy, kde byl systém Latis SQL již nasazen patří především budovy a objekty státní správy, armády ČR včetně muničních skladů a bankovní střediska stejně jako soukromý sektor (především nákupní centra).

4.1.7 SW Axxon

AxxonSoft je přední softwarová vývojářská společnost, která především vyvíjí unikátní inovativní nástroje pro budování inteligentních bezpečnostních systémů pro ochranu objektů všech velikostí a složitosti. Software Axxon kombinuje VMS, IP systémy, inteligentní analýzu obrazu, prvky pro rozpoznávání obličeje, systémy pro sledování průvodních jevů spojených se silničním provozem a hlavně plně integrované řešení bezpečnostních aplikací. Produkty, které firma AxxonSoft nabízí, jsou následující:

- Axxon Next a
- Axxon Intellect Enterprise. [40]

Axxon Next představuje generaci otevřené softwarové platformy pro správu videa. Neexistují zde žádná omezení týkající se počtu video serverů, pracovní stanic nebo video kamer. Axxon Next umožnuje pracovat s jinými zařízeními a systémy, podporuje více než 1500 modelů IP kamer různých světových výrobců prostřednictvím protokolu Onvif, stejně jako

vzdálený přístup z mobilních zařízení a samozřejmě z webového rozhraní. Každá licence zahrnuje plnou, neomezenou funkčnost VMS, a to i v systémech, kde je použita jen jedna kamera. Je tedy ideální pro velmi rozsáhlé distribuované systémy. Pro systém o velikosti maximálně 16 kamer, popřípadě k vyzkoušení je však k dispozici bezplatná verze programu. SW platforma Axxon Next umožňuje použití neomezeného počtu:

- serverů v distribuovaném systému,
- klientů, kteří jsou připojeni k serverům,
- serverů, z kterých je současně přenášen videostream,
- videostupů na serveru,
- současně zpracovávaných signálů z mikrofonů,
- kamer s funkcí PTZ a
- zobrazených záběrů z kamer na klientské stanici.

Mezi základní funkce VMS patří automatické vyhledávání zařízení v síti, současný záznam a živé sledování, správa uživatelů a skupinových práv, synchronizované přehrávání záznamu z více kamer, audio a video analýza, sestavení scénářů s činnostmi jako je generování alarmu, záznam, aktivace akčního relé, spuštění předem definované funkce PTZ kamer a také odeslání upozornění prostřednictvím SMS, emailu nebo i reproduktoru v monitorovaném objektu. Jako speciální funkce lze považovat aplikaci Micro-modulu pro zabezpečení spolehlivosti distribuované architektury systému, interaktivní 3D mapové vyobrazení objektu spolu s praktickými náhledy z jednotlivých kamer.

Obr. 24: 3D zobrazení interaktivní mapy [40]

Software Axxon Next obsahuje pozoruhodný výkonný systém pro správu, zpracování videa a analýzu obrazových snímků. Obsahuje následující nástroje pro detekci:

- pohybu v obraze a změny v pozadí,
- ztráty kvality obrazu (rozmazání, znečištění či zaslepení objektivu nebo ztmavení obrazu),
- opuštěného objektu (např. kufřík ve scéně zůstává nehybně stát po nějakou dobu),
- překročení čáry v daném směru,
- pohybu zastávka (sledovaný objekt se zastaví a zůstane bez hnutí po určitou dobu v rámci uživatelsky stanovené oblasti),
- potulka (objekt zůstane v uživatelem určené oblasti po nějakou dobu) a
- detekci zmizení objektu (objekt v oblasti zmizí ze zorného pole kamery).

Kromě videoanalytických funkcí, nástroj obsahuje i dvě zvukové detekce:

- detekce šumu - překročení určité úrovně hlasitosti a
- detekci ticha.

Produkt Acfa Intellect, představuje sadu modulů pro integraci systému kontroly vstupu, elektrickou požární signalizaci a poplachový zabezpečovací systém do VMS systému Axxonsoft. Kromě zmíněných systémů umožňuje integraci i nepoplachových systémů, jako jsou zavlažovací systémy, klimatizační a vytápěcí systémy, osvětlení a parkovací systémy. Architektura umožňuje připojit jakýkoli typ digitálního systému nebo hardwaru, bez ohledu na typ zařízení, výrobce nebo technické vlastnosti.

Princip komunikace mezi zařízeními je založen na TCP/IP architektuře. Je použitá kombinace klasické hierarchie klient-server a třístupňové architektuře pro distribuovaný model systému. Axxon Intellect Enterprise používá tři základní prvky: server, klient a bránu. Servery tvoří segment sítě s komunikací peer-to-peer, kde veškerá data nebo události jsou přenášeny ze serveru na server. Klienti se mohou připojit k jednomu nebo k více serverům, popřípadě napřímo prostřednictvím bran. Brány slouží jako routery definující segmenty distribuované sítě. Peer-to-peer síť využívá mnoha typů připojení (LAN, WAN, mobilní) mezi účastníky v síti a centralizovaných zdrojů (serverů), kde relativně nízký po-

čet serverů poskytuje jádro poskytovaných služeb nebo aplikací. Ke komunikaci s podsystémy jsou používány protokoly opc, ascii a xml. [40]

Distribuovaný systém znamená, že v případě problému v odkazu na modul nebo problému se síti se komunikace automaticky přepne na jiný funkční server. Serverová část v současné době běží na NT, Linux a AIX zařízeních. SW integrace spolupracuje a podporuje především protipožární, přístupové a zabezpečovací systémy od výrobců: Honeywell, Siements a Paradox.

4.2 Komparační studie integračních platforem

Z analýzy všech integračních platforem IBS vyplývá, že veškeré tyto systémy jsou koncipovány na architektuře klient/server s podporou protokolu TCP/IP. Velkou předností této technologie přenosu je možnost použití již realizované datové infrastruktury LAN a WAN v rámci nasazení v chráněných objektech. Základem systémů je SQL databáze, v které se koncentrují veškeré informace z dílčích subsystému připojených k platformě a informace vložené uživatelem. K přenosu dat z jednotlivých podsystémů do databázového systému jsou používány otevřené komunikační standarty umožňující softwarovou integraci externích výrobců technologií. Z hlediska aplikace různých funkcionalit v jednotlivých platformách jsou všechny systémy řešeny jako modulární. Zadavatel a budoucí uživatel bezpečnostního systému má při realizaci možnost si zvolit různé moduly z hlediska jejich využitelnosti v ohledu na konkrétní bezpečnostní rizika a požadavky, popřípadě legislativních nařízeních. Použití modulární koncepce systému má výhody ve flexibilitě změny použití, vybavenosti, rozsahu nebo konfigurace IBS systému a tím navýšit i vlastní funkcionalitu celého systému. Mezi jednotlivá hlediska pro objektivní porovnání integračních platforem byly použity následující kritéria:

- počet aktuálně podporovaných externích výrobců,
- poplachové a nepoplachové funkcionality,
- způsoby předávání dat a ovládání integrovaného systému,
- podporované komunikační rozhraní a
- vhodnost použití platforem v závislosti na velikosti a typu aplikace.

4.2.1 Statistika podpory externích výrobců

Mezi obecná kritéria pro komparaci integračních SW platforem patří porovnání analyzovaných platforem v závislosti na počtu aktuálně podporovaných externích výrobců bezpečnostních systémů a jiných nepoplachových systémů, jako jsou např. systémy MaR. Uvedené údaje jsou orientační s ohledem na aktuálně poskytnuté informace od výrobců popř. distributorů. Vývojáři platforem disponují souborem nástrojů pro vývoj jejich SW (balíček SDK), s kterým lze vytvořit ovladač na ještě nepodporované zařízení. V případě platformy C4 je tento podpůrný balíček dokonce volně k dispozici pro externí vývojáře.

Tab. 7: Porovnání platforem

podle počtu podporovaných výrobců

Platforma	**Počet výrobců**
SBI	95
C4	71
Alvis	55
Integra	52
VAR-NET Integral	10
AxxonSoft	157 (138 VSS, 19 ostatní BT)

Z první tabulky je zřejmé, že nejvíce výrobců různých technologií podporuje integrační platforma SBI, následovaná systémy C4, Alvis a Integra. Naopak nejmenší počet podporovaných systémů nabízí ve svém portfoliu systém VAR-NET integral, jehož podpora je soustředěna především na technologie, které sama firma Variant plus distribuuje. SW nástroj AxxonSoft s celkovým počtem 157 podporovaných výrobců zařízení se však vymyká objektivnímu hodnocení podpory, jelikož tento systém je představitelem video management systému jako umbrelasoftu zastřešující i integraci s dalšími systémy. Tento systém podporuje především výrobce VSS kamerových systémů aplikováním standardu Onvif a v menší míře výrobce ostatních bezpečnostních technologií.

Tab. 8: Nejvíce podporovaných výrobců systémů

Výrobce	**Technologie**	**Podpora integrace**
Honeywell	PZTS, EPS, SKV	5
Pelco	VSS	5
Paradox	PZTS, SKV	4
Axis	VSS	4
Samsung	VSS	4
ACTi	VSS	4
Satel	PZTS	4
Sony	VSS	3
Hikvision	VSS	3
Bosch	VSS	3
Job Detectomat	EPS	3
Tyco	EPS	2
Siemens	PZTS, EPS	2
ASSA ABLOY	SKV	2
Concept	PZTS	2

Statistika uvádějící již konkrétní výrobce prezentuje, kteří výrobci systémů jsou nejvíce podporováni integračními platformami. Jak vyplývá z tabulky, systémy od firmy Honeywell a Pelco jsou nejvíce podporovány spolu s dalšími, převážně kamerovými systémy. Z těchto skutečností vyplývá, že v praxi se integrační platformy a posléze integrační bezpečnostní systémy aplikují v objektech, ve kterých se již nacházejí zmíněné systémy nebo se spolu s integračními SW nasazují pro efektivní zabezpečení. V případě bezpečnostních systémů od firmy Honeywell zde rozhodně hraje určitou roli i všestrannost výrobce těchto systémů, který na trh uvádí systémy PZTS, EPS i SKV.

4.2.2 Komparace funkcionalit integračních platforem

Zdaleka nejdůležitějším kritériem při vzájemném porovnání platforem je podpora různých funkcí ať už poplachového bezpečnostního rázu, nebo nepoplachového rázu.

Tab. 9: Komparace platforem podle možnosti integrace poplachových aplikací

Platforma	PZTS	VSS	SKV	EPS	Perim. Ochrana	ENVIRO	Videoanalýza
SBI	+	+	+	+		+	
C4	+	+	+	+	+		
Alvis	+	+	+	+	+		
Integra	+	+	+	+	+	+	+
VAR-NET Integral	+	+	+	+	+	+	
Latis SQL	+	+	+	+			
AxxonSoft	+	+	+	+			+

Veškeré platformy, které byly předmětem analýzy, podporují integraci všech čtyř systémů, které se primárně podílejí na zvýšení bezpečnosti a snížení bezpečnostních rizik spojených s provozem objektů. Podporu systémů PZTS, VSS, SKV a EPS můžeme považovat jako funkcionální standard všech integračních platforem. Perimetrická a environmentální ochrana bývá většinou součástí některého z již zmíněných systémů, avšak na trhu jsou k dispozici i zcela samostatné environmentální a perimetrické systémy, jako je např. plotový perimetrický systém Perysys nebo Peridect. Naopak videonalýza zde není brána jako samostatný systém, ale jako pokročilá funkce systému VSS, která nezahrnuje nejen obyčejnou detekci pohybu v obraze, kterým je již vybaven každý kamerový systém, ale již pokročilou videoanalytiku zahrnující detekci opuštěného objektu, zastavení pohybu, zmizení objektu apod. Těmito videoanalytickými nástroji, podle analýzy platforem disponují ty systémy, jejíž součástí je video managemet systém neboli VMS.

Tab. 10: Komparace platforem podle možnosti integrace nepoplachových aplikací

Platforma	MaR	Docház. sys.	Strav. sys.	Park. sys.	KŘ	GIS	Ex. IS
SBI	+	+	+	+	+		+
C4	+	+	+	+	+	+	+
Alvis	+						
Integra	+	+		+			+
VAR-NET Integral	+	+	+				
Latis SQL	+	+		+	+	+	+
AxxonSoft	+			+			

V oblasti nepoplachových aplikací jsou ze strany analyzovaných platforem nejvíce podporovány systémy pro měření a regulaci zahrnující vytápěcí, větrací a klimatizační systémy. Další často podporované systémy, jež bývají většinou součástí systémů pro kontrolu vstupu, jsou systémy pro záznam docházky, parkovací systémy a stravovací systémy. Mezi poměrně specializované a méně podporované funkcionality patří nástroje krizového řízení (KŘ) pro podporu rozhodování a řízení při vniku mimořádných popřípadě krizových událostech a nástroje pro propojení s geografickými informačními systémy, které poskytují mapové podklady. Pod pojmem externí informační systémy se považuje možnost integrační platformy exportovat data v určitém formátu do jiných, např. mzdových systémů.

4.2.3 Porovnání podle způsobů ovládání a předávání dat

Následující komparace programů se zabývá ovládáním a předáváním dat a to v první řadě mezi serverovou stanicí a klientskou stanicí v tabulce č. 11. V další tabulce se na platformy nahlíží z pohledu podpory otevřených komunikačních rozhraní, kterých se může využívat při propojení zabezpečovací ústředny nebo řídící jednotky k serveru na kterém by běžela instalace integrační platformy.

Tab. 11: Komunikační a ovládací nástroje platforem

Platforma	**WEB**	**Email**	**SMS**	**GSM**	**GPRS**
SBI	+	+			+
C4	+	+	+		
Alvis	+	+			
Integra	+	+	+		+
VAR-NET Integral	+	+	+	+	+
Latis SQL	+	+	+	+	
AxxonSoft	+	+			

Způsoby, jak lze IBS ovládat, popřípadě z něj získávat potřebné informace je hned několik. Veškeré systémy jsou realizovány na architektuře klient/server, z čehož logicky vyplývá, že nejrozšířenějším a nejpreferovanější způsob ovládání je přes webový prohlížeč a to bez ohledu na jeho druhu. Jako doporučovaný typ prohlížeče bývá však uváděn Microsoft Internet Explorer, který je implementován v rámci instalace nejrozšířenějšího operačního systému Microsoft Windows. Výhodou ovládání systému prostřednictvím webového prohlížeče spočívá také v hardwarové nenáročnosti klientské stanice. Kvantitativně stejně podporovaná je jednosměrná komunikace emailem, kdy informace o jednotlivých činnos-

tech nebo událostech v systému mohou být odeslány uživatelům, u kterých se většinou nepředpokládá okamžité jednání (majitel, vedení firmy). Méně využívanými komunikačními prostředky jsou SMS zprávy, telefonní hovory (GSM) a GPRS síť s použitím ovládací smart aplikace.

Tab. 12: Souhrn podporovaných komunikačních standardů

Platforma	**Podporované rozhraní**									
	OPC	Espa-x	Modbus	Ascii	DDE	snmp	xml	teco	Html	Onvif
SBI	+		+			+			+	+
C4	+		+		+	+			+	
Alvis	+	+	+	+	+	+	+		+	
Integra	+		+					+	+	
VAR-NET Integral				+					+	
Latis SQL	+		+				+		+	
AxxonSoft	+			+			+		+	+

Různé integrační platformy podporují různé komunikační standardy, jejichž charakteristika je uvedena v podkapitole o komunikačních standardech. Platforma, která podporuje nejvíc standardů a udává tak největší možnosti při volbě typu komunikace je SW Alvis. Naopak produkt VAR-NET Integral striktně podporuje pouze komunikaci v Ascii znacích mezi podsystémy a integrační nadstavbou a komunikaci prostřednictvím html kódu pro přenos dat s klientskou stanicí nebo prvky VSS. I z těchto důvodů vyplývá, proč tento SW prostředek pro integraci je nejméně podporován externími výrobci. Z komparační studie vyplývá, že nejrozšířenější podporované komunikační otevřené standardy jsou OPC a Modbus stejně jako html, který se kromě komunikace s podsystémy používá pro komunikaci s klienty. Protokol Onvif podporují jen ty platformy, které jsou koncipovány jako VMS nebo přímo podporují přídavný modul pro pokročilou videosprávu.

4.2.4 Vhodnost použití platforem v závislosti na velikosti aplikace

U jednotlivých platforem je vhodné dále posoudit jejich vhodnost použití a to v závislosti na velikostech objektů, v kterých by bylo vhodné jejich nasazení pro zvýšení bezpečnosti a efektivnosti monitoringu. Dříve, než provedeme samotné posouzení vhodnosti nasazení, je vhodné si charakterizovat klasifikační parametry rozhodující pro porovnání. Velikost aplikace rozlišujeme na:

a) malou aplikaci, představující objekty s menším počtem subsystémů a technologických prvků s důrazem na komfort, menší složitost systému a celkovou cenu aplikace, u které se nepředpokládá 24h provoz obsluhy IBS,
b) pod pojmem střední aplikace si můžeme představit větší objekty s vícero aplikovaných subsystémů a technologií s podstatným nárůstem doplňujících modulů zajišťující specifické úkony, kde se již předpokládá 24h provoz obsluhy a
c) velkou aplikací rozumíme velmi komplexní IBS, v kterém neexistují téměř žádné limity co do počtu podsystémů, aplikovaných technologií či přídavných modulů.

Tab. 13: Komparace SW podle velikostí aplikace

Platforma	**Velikost aplikace**		
	Malá	Střední	Velká
SBI	+	+	+
C4		+	+
Alvis		+	+
Integra		+	+
VAR-NET Integral	+	+	
Latis SQL		+	+
AxxonSoft		+	+

Integrační platformy byly dle provedených analýz a uvedených charakteristik výše roztříděny do třech kategorií. Všechny SW nadstavby jsou svojí stavbou systému a koncepcí vhodné pro aplikace střední velikosti. V oblasti použití platforem do velkých aplikací je možné konstatovat, že téměř veškeré platformy s různými moduly a konfiguracemi jsou taktéž vhodné pro nasazení. Výjimku tvoří pouze VAR-NET Integral, který se svými omezujícími faktory nelze zahrnout do této kategorie. Limitující faktory jsou již uvedeny v kapitole věnující se této integrační platformě. Co se týče velikostně malých aplikací, je tento systém naopak velmi vhodný pro svoji jednoduchost a přehlednost nasazení. Do rozsahově menších objektů je vhodná i platforma SBI a to především edice Easy, která je koncepčně zaměřená na instalace s požadavky: zjednodušeného ovládání, snadného nastavení a jednoduché přizpůsobitelnosti podle potřeb konkrétně dané kategorie uživatelů. Atraktivní je pro malé aplikace i verze SBI Portál, která svou cloudovou koncepcí zaručuje značné finanční úspory při realizaci IBS bez starostí o HW, jeho aktualizací a zdlouhavého nastavování.

4.2.5 Vhodnost použití platforem v závislosti na specifickém typu aplikace

Závěrečné klasifikace integračních platforem se věnuje vhodnosti použití platforem do konkrétních modelových objektů a je rozdělena na dvě sféry podle povahy objektů na objekty sféry soukromé a sféry státní. Porovnání SW nadstavbových nástrojů vychází ze všech provedených analýz a syntéz uvedených v této kapitole věnující se integračním platformám.

4.2.5.1 Specifikace aplikace pro soukromou sféru

Pro prvotní objektivní vyhodnocení SW nástrojů je vhodné specifikovat modelové objekty soukromé sféry:

Rezidenční objekt

Rezidenčním objekt je představitelem typicky velikostně menší aplikace. U těchto objektů se předpokládá použití dvou bezpečnostních systémů PZTS a VSS a systému MaR. Detekce požárního nebezpečí je součástí systému PZTS, který můžeme považovat jako kombinovaný. Počet prvků v jednotlivých systémech je v řádu desítek pro systém PZTS a jednotek pro VSS. Hlavním kritériem pro výběr platformy do objektu tohoto typu je komfort, snadná ovladatelnost, nastavitelnost a údržba. Naopak nepodstatným faktorem jsou omezující maximální limity v počtech technologických prvků.

Ubytovací zařízení

Zařízení pro ubytovací služby můžeme charakterizovat jako budovu větších rozměrů s více nadzemními patry a větším počtem osob. Z toho plynou větší nároky na počet podsystémů i počet detekčních, akčních a monitorovacích členů. Systémy PZTS a VSS je vhodné již doplnit systémem EPS, popřípadě SKV. V rámci nepoplachových aplikací se nabízí vybavit IBS systémem MaR a parkovacím systémem.

Obchodní centrum

Objekt, ve kterém se nachází desítky obchodů s velkými počty lehce odcizitelnými aktivy, je obecně kladen velký význam na aplikování systému VSS s velkým rozsahem. S nutností nasazení VSS souvisí i velký počet pohybujících se cizích lidí po objektu. Většina těchto nákupních a obchodních center svou rozlohou převyšují 10 000m^2, je tedy z legislativních požadavků nutnost aplikovat systém EPS s grafickou SW nadstavbou. Kromě jmenovaných systémů můžeme v obchodních centrech předpokládat nasazení PZTS a to buď:

a) jednoho systému PZTS s velkým počtem podsystémů a prvků anebo
b) několik systémů PZTS co do rozsahu i typu výrobce pro jednotlivé obchody.

Důležitý nepoplachový systém, který by měla integrační platforma podporovat je systém parkovací, protože tato centra se většinou nacházejí v blízkosti městské zástavby, kde obecně bývají parkovací místa přeplněná, a mohlo by docházet k zneužívání parkovacích míst centra k jiným, než nakupovacím účelům.

Administrativní budovy

V objektech administrativního typu se do popředí dostává, oproti předešlým typům objektů, vhodnost vybavení IBS systémem SKV a v návaznosti i systém pro evidenci a kontrolu docházky. Své opodstatnění pro vybavení IBS nabývají i stravovací a parkovací systémy spolu se systémy MaR. Vhodnost nasazení systémů PZTS, VSS a EPS do tohoto typu budov můžeme brát už jako samozřejmost.

Výrobní objekty

Samotný typ výroby a objekty, v kterých se výroba realizuje, může sebou brát určité specifické nároky na složení funkcionalit integrační platformy. Specifické požadavky na IBS může klást např. na slévárenskou budovu (nasazení EPS a MaR pro odvětrávání) a jiné požadavky mohou být kladené na prostory pro skladování a přechovávání zboží (vybavení VSS a SKV s evidencí zboží). Z těchto důvodů je na místě počítat s nasazením integračních platforem, které obecně disponují s velkými možnostmi co do funkcionalit, tak i do počtu aplikovaných technologií.

Tab. 14: Porovnání SW nástrojů podle specifikace aplikace – soukromá sféra

Platforma	**Rezidenční Objekt**	**Ubytovací Zařízení**	**Obchodní centrum**	**Administrativní Budovy**	**Výrobní Objekty**
SBI	+	+	+	+	+
C4		+	+	+	+
Alvis		+	+	+	+
Integra		+	+	+	+
VAR-NET Integral	+	+			
Latis SQL				+	+
AxxonSoft		+	+	+	+

Z tabulky porovnání SW nástrojů pro nasazení v oblasti soukromé sféry vyplývá, že platformy SBI a VAR-NET Integral jsou nejvhodnější pro nasazení do rezidenčních objektů, což se rovněž odráží v komparační tabulce podle velikostí aplikace, kde jsou jmenované platformy uvedeny jako vhodné pro aplikace velikostně malého typu. VAR-NET integral je avšak oproti SBI dále nevhodný pro ostatní aplikace, což má opět na svědomí limitní parametry platformy. Jinak je poměrně většina platforem svými funkcemi a rozsahy všestranná co do použití v různých typech budov a objektů.

4.2.5.2 Specifikace aplikace pro státní sféru

Pro oblast použití ve státní sféře je taktéž vhodné tyto modelové případy specifikovat. Charakteristika jednotlivých oblastí použití se částečně odráží z dostupných referencí o nasazení jednotlivých platforem v praxi. Uvedené jsou především hlavní požadavky na skladbu systému

Doprava

Specifickou oblastí, kde by instalace IPS mohla být určitým přínosem, je oblast telematiky v dopravě. Součástí integrovaného systému pro takovéto použití by byl především propracovaný systém VSS s pokročilou videoanalýzou např. pro detekci vozidel a monitoring hustoty silničního provozu za účelem řízení dopravy prostřednictvím proměnlivých elektronických tabulí. Systém by doplňoval i systém SKV spolu s parkovacím systémem.

Zdravotnictví

Ve zdravotnictví kromě systémů PZTS, SKV, VSS a EPS by měla integrační platforma podporovat spojení se specifickými tísňovými systémy a systémy pro přivolání pomoci, které nejsou přímo součástí systému PZTS. Mezi tísňové systémy přivolání pomoci považujeme pagery či tísňová tlačítka, hlásiče a interkomy podporující komunikaci přes Espa-x standard.

Školství

Školské zařízení se vyznačuje potřebou integrovaného systému, který by kromě čtyř základních bezpečnostních systémů podporoval stravovací systém, který je běžným vybavením jakékoliv školní jídelny.

Pracoviště městské policie

Na pracovišti městské policie bývá aplikován městský kamerový a dohlížecí systém, zkráceně uváděný jako MKDS, jež můžeme taktéž považovat za jistou formu IPS. Jak už z názvu MKDS vyplývá, jeho hlavním systémem pro zvýšení bezpečnosti je právě kamerový systém. Součástí MKDS může být i systém SKV pro kontrolu vjezdu do městských prostor (např. náměstí) a systém PZTS budov chráněných policií.

Objekty zvláštního významu

Objektem zvláštního významu ve státní sféře můžeme považovat objekty národního a vyššího významu. Důležitou požadovanou vlastností nasazeného IPS a jednotlivých podsystémů PZTS, VSS a SKV je certifikace pro nejvyšší stupeň zabezpečení 4 pro vysoká bezpečnostní rizika.

Tab. 15: Porovnání SW nástrojů podle specifikace aplikace – státní sféra

Platforma	**Doprava**	**Zdravotnictví**	**Školství**	**Pracoviště Městské policie**	**Objekty zvláštního významu**
SBI		+	+		
C4		+	+	+	
Alvis		+	+		
Integra	+	+	+	+	
VAR-NET Integral					
Latis SQL				+	+
AxxonSoft	+		+	+	

Z komparace SW platforem v kontrastu s výčtem specifických aplikací ve státní sféře vychází nevhodnost nasazení systému VAR-NET Integral ve všech případech. Naopak všestranným systémem se zdá SW Integra, což vyplývá i v návaznosti na předešlé syntézy. Latis SQL je certifikován pro vyšší stupně zabezpečení a je tedy vhodné ho aplikovat do objektů městské policie, popř. do objektů zvláštního významu. Programy Integra a AxxonSoft je vhodné nasazovat do objektů, u kterých se obecně požadují pokročilé videoanalytické funkce.

Dílčí závěr kapitoly

Poměrně obsáhlá kapitola, věnující se analýze integračních platforem a následně syntéz dostupných informací, nastiňuje současné možnosti SW produktů pro jednotné řízení bezpečnosti v zájmových objektech. Z provedených analýz vyplývá, že veškeré platformy podporují integraci poplachových systémů PZTS, VSS, SKV a EPS. Jednoznačně preferovaná je architektura klient/server a uspořádání systému bývá modulové z důvodu volby jen potřebných funkcí. To, co v jednotlivých analýzách integračních platforem není zohledněno, avšak může mít rozhodující význam pro volbu a nasazení konkrétní platformy, je licenční politika. Z dostupných informací o produktech, popř. po konzultacích s výrobci či distributory vyplývá, že v mnoha případech je cena licence závislá na konkrétní požadované zakázce, čili v závislosti na typu, velikosti a obtížnosti instalace. Závěrečné zkategorizování platforem podle vhodností použití je provedeno obecně v závislosti na pravděpodobně požadovaných technologiích. Konkrétní volba typu systému, ať už poplachové nebo nepoplachové povahy je však velmi závislá na konkrétních požadavcích vznesené zadavatelem. Nicméně je možné uvést, že integrační platformy, které byly předmětem analýzy (kromě jednoho systému), splňují svými funkcionalitami nároky kladené na aplikace soukromé sféry. Z pohledu státní sféry rozhodují o vhodnosti nasazení platforem spíše konkrétní vlastnosti a přednosti subsystémů.

5 MODELOVÉ NÁVRHY INTEGROVANÝCH POPLACHOVÝCH SYSTÉMŮ

Stanovení modelových řešení návrhů integrovaných poplachových systémů vychází z předešlých analýz integračních platforem. Byly vytipovány celkem čtyři modelové případy, v kterých je vhodné aplikovat nadstavbový integrační software. Mezi objekty, pro které budou zpracovány modelové návrhy, patří:

1. rezidenční objekt,
2. ubytovací zařízení,
3. zdravotnické zařízení a
4. výrobní podnik,

5.1 Modelový návrh IPS pro rezidenční objekt

Rezidenčním objektem považujeme typ objektu, který je určen především k bydlení. Kategoricky patří mezi menší aplikace představující v praxi rodinné domy, byty, popř. i menší rodinné společnosti apod. Hlavní motivací, proč v těchto objektech nasadit v nějaké podobě integrovaný systém, vychází z následujících nároků:

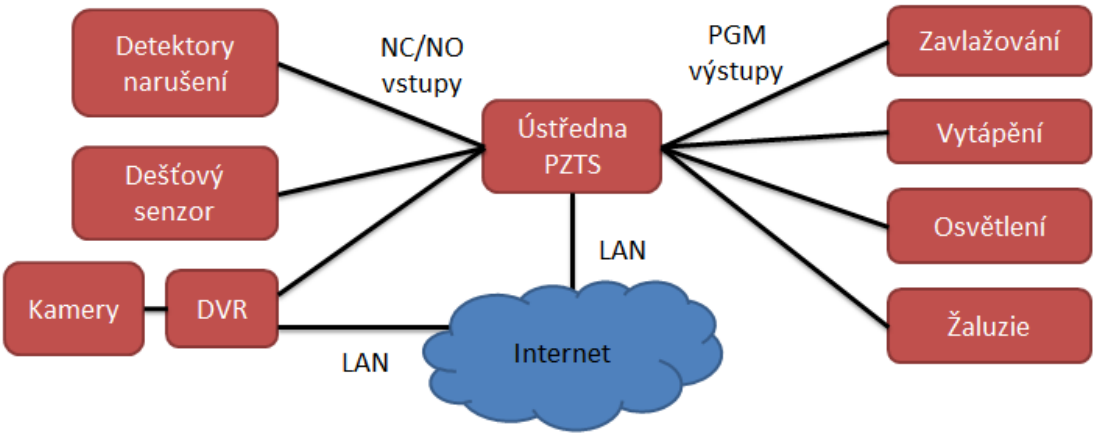
- komfortní, snadné a intuitivní ovládání,
- jednoduchost instalace a údržby,
- možnost navázání na již stávající techniku a také
- cenově dostupné řešení.

Modelový objekt rezidenčního typu z hlediska použitých technologií, je pro účel návrhu IPS charakterizován následovně:

a) V budově je instalován systém PZTS DSC Power PC1832 obsahující 32 drátových nebo bezdrátových zón, které lze rozdělit do čtyř nezávislých subsystémů. Zabezpečovací systém je vybaven celkem 14cti PGM výstupy.
b) Dále je aplikován IP kamerový systém o počtu 5 kamer značky Canon taktéž s PGM poplachovými výstupy a dále DVR (digitální videorekordér) pro záznam.
c) Ohledně nepoplachových aplikací bude budova doplněna systémem MaR za účelem řízení vytápění, osvětlení, ovládání žaluzií a zavlažování.

5.1.1 Volba vhodné integrační technologie

Pro aplikaci tak malého rozsahu s technologiemi, které byly vyspecifikovány, se jako nejsnazší řešení jeví integrace na nižší hardwarové úrovni. Přednost takovéto volby spočívá v jednoduchosti realizace, vlivem malého počtu zařízení a finanční nenáročnost. Jednotlivé systémy budou mezi sebou provázány prostřednictvím svých vstupů a výstupů. Systém zprostředkovávající mezi systémové vazby, lze považovat v tomto případě systém PZTS. Není tedy zapotřebí pořizovat další technologie, které by byli nutné pro propojení a centrální správu systému.



Obr. 25: Schéma systému v rezidenčním objektu

Jako dvoustavové vstupy jsou do ústředny PZTS přivedeny veškeré detektory narušení, jako jsou pohybové detektory, detektory otevření apod. současně i se senzorem pro detekci deště a poplachové vstupy z DVR. Na výstupních svorkách PGM je připojeno zavlažování, vytápěcí systém, osvětlení domu a žaluzie. Základní ovládání systému se možné prostřednictvím klávesnice systému PZTS umístěné lokálně v objektu. Vzdáleně je možné ovládat systém přes internet stejně jako nahlížet na záběry z kamerových bodů rozmístěných po chráněném objektu.

5.1.2 Nastavení vazeb mezi vstupy a výstupy

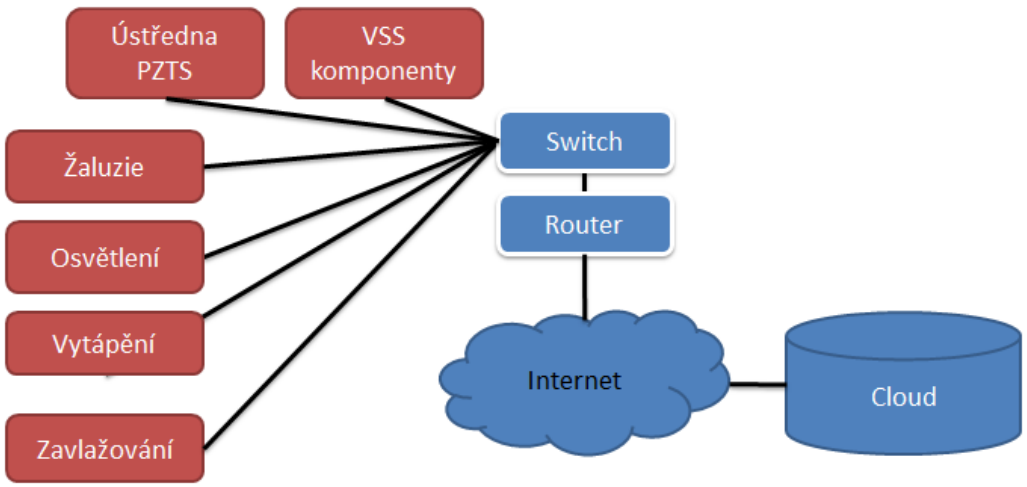
V namodelovaném systému je zapotřebí naprogramovat automatické vazby mezi vstupy a výstupy (PGM, LAN) pro ty situace, které používáním systému běžně nastávají. Provedení automatické činnosti vždy předchází nějaká iniciační událost. Následuje výčet těchto událostí spolu s činnostmi, které budou provedeny bez zásahu uživatele.

1) Při zastřežení objektu dojde k centrálnímu vypnutí veškerého osvětlení v budově a zatažení venkovních žaluzií.
2) Při odstřežení objektu se opětovně zapne osvětlení a vytáhnou žaluzie.
3) Detekováním narušení nebo pokusu o narušení objektu se vyhlásí poplach lokálním signalizací spolu s odesláním zprávy prostřednictvím internetu. Pokud bude narušení detekováno v prostorech, které budou snímat kamery, poplachová zpráva bude obsahovat i obrazové informace narušení. Vlivem aktivace poplachového výstupu kamery na vstup DVR dojde k záznamu.

Výstupy PGM, na kterých je připojen vytápěcí systém a zavlažování, budou řízeny v závislosti na rozvrhu uvedeném v kalendáři systému PZTS. Činnosti termostatu vytápěcího systému se bude řídit povelem z ústředny PZTS v závislosti na režimu objektu. Spínání zavlažování tak bude možné ovládat vzdáleně za podmínky, že dešťové čidlo nebude signalizovat srážky v časovém horizontu cca 2 dny.

5.1.3 Alternativní řešení integrace

Na trhu je k dispozici integrační SW nástroj, jež je taktéž vhodný pro aplikaci IPS v malých objektech rezidenčního typu. Vhodnost použití spočívá v tom, že stejně jako integrace na HW úrovni, není nutností pořizovat další technologii kvůli propojení a centrální správu. Integrační platforma SBI ve své verzi Portál nabízí efektivní řešení pro centrální řízení a vzdálený monitoring veškerých technologií, které byli jmenovány v souvislosti s rezidenčním objektem.



Obr. 26: IPS v rezidenčním objektu s použitím platformy SBI Portal

Server, na kterém bude instalována integrační platforma, se nachází na vzdáleném úložišti (cloudu), který se nachází v prostorách společnosti CGC, jež je výrobcem této technologie a současně se stará o servis, údržbu, aktualizace a bezproblémový chod SW SBI Portal. Veškeré technologie a systémy jsou propojeny se serverem standardem TCP/IP a to přes router, který je bránou mezi lokální a globální sítí zajišťující tak vzájemnou komunikaci. Užívání platformy SBI Portal je řešeno formou pronájmu a bez velkých vstupních realizačních nákladů, což může být velmi zajímavou alternativou k IPS, který je realizován na základě HW integrace.

5.2 Integrovaný systém v ubytovacím zařízení

Ubytovací zařízení pro účelné navržení poplachového integrovaného systému je charakterizováno jako vícepodlažní budova se stovkou místností s poměrně velkým počtem pohybujících se osob. Na základě určitých přístupových práv je povolen přístup do jednotlivých místností, které jsou určeny pro klienty ubytovacího zařízení. Navržený systém bude proto disponovat systémem kontroly vstupu oproti předchozímu modelovému případu rezidenční budovy, kde tento požadavek nebyl vznesen. V objektu budou instalovány následující konkrétní bezpečnostní technologie:

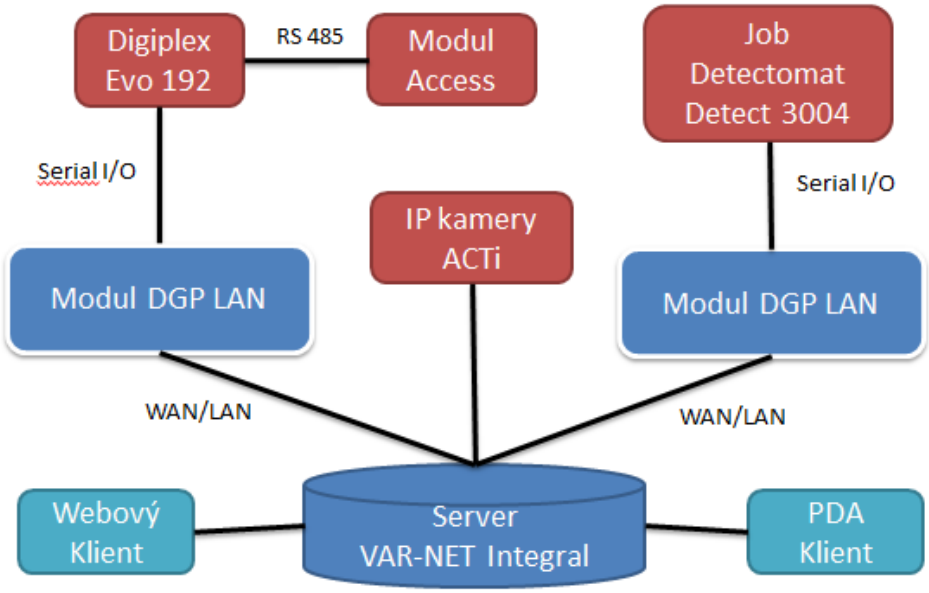
1) Sběrnicový systém PZTS Paradox Digiplex EVO 192, který má celkem 192 detekčních zón, které lze roztřídit do osmi na sebe nezávislých podsystémů. Systém lze ovládat klasickým způsobem přes klávesnici. Součástí ústředny je prvek pro IP komunikaci.
2) Systém kontroly vstupu je již integrovaný v rámci ústředny PZTS jako jeho doplňující modul. Nadstavba ACCESS umožnuje monitorovat max. 32 dveří a kontrolu vstupu až pro 800 uživatelů. Připojení čteček karet, otisků prstů popřípadě jakékoliv jiné čtečku je podmíněna kompatibilitou s výstupem dat ve formátu Wiegand 26 bitů.
3) Systém EPS Job Detectomat založený taktéž na sběrnicové technologii umožňující adresaci jednotlivých prvků. Adresace prvků systému Job Detectomat je totožná s adresací prvků systému Paradox Digiplex EVO 192. Zvolený typ ústředny je Detect 3004 umožňující připojení 4 analogových smyček, kdy na každé smyčce je možné připojit až 126 požárních hlásičů.
4) Instalovaný kamerový systém v prostorách objektu je o velikosti deseti IP kamer značky ACTi typu fixních dome, ve vnitřním i venkovním provedení.

5.2.1 Volba nadstavbové platformy

Vyjmenované bezpečnostní systémy lze velmi jednoduše a efektivně integrovat použitím nadstavbového integračního systému VAR-NET Integral, který je již od samého počátku jeho vývoje dimenzován na specifické konfigurace jmenovaných technologií, které se v objektu ubytovacího typu nacházejí. Již z referencí realizovaných systémů, kde byla platforma od firmy Variant plus nasazována, vyplývá jeho vhodnost pro tento modelový návrh IPS.

5.2.1.1 Vazby mezi systémy

Provázání systémů Paradox Digiplex EVO, Job Detectomat s integrační platformou VAR-NET Integral je založené na komunikaci prostřednictvím zasílání příkazů a odpovědí mezi systémy a to ve formě Ascii znaků. Pro tyto systémy byly definovány konfigurační příkazové soubory, které stanovují parametry komunikace.



Obr. 27: Architektura modelového IPS

PZTS

Proto, aby ústředna Digiplex Evo 192 mohla být připojena k serveru, kde bude instalována nadstavbová integrační platforma, je zapotřebí vybavit ústřednu HW modulem DGP LAN V+. Tento modul transformuje procesorový výstup základní desky, označený jako Seriál I/O, na komunikační protokol Ascii ve formátu TCP/IP díky němuž lze pak ústřednu připojit k LAN síti.

SKV

Systém pro kontrolu přístupu, jak už bylo uvedeno, je realizován integrací se systémem PZTS na HW úrovni. Modul ACCESS komunikuje po sběrnici RS-485 ústředny Digiplex Evo, který zajišťuje správu uživatelů a jejich přístupových práv. V rámci integrační platformy je funkce pro kontrolu vstupu zajištěna modulovým okruhem EKV.

EPS

Ústředna Job Detectomat Detect 3004 je k integrační platformě připojena stejným způsobem jako ústředna Digiplex Evo. Rozdílnost při komunikaci je ovšem v definici komunikačního příkazového souboru, protože obecně systémy EPS a PZTS disponují zcela rozdílnými funkcemi a vlastnostmi. Příkazy jsou proto modifikovány v závislosti na těchto požadavcích.

VSS

Kamery ACTi jsou k integrační platformě připojeny přímo bez vlastního NVR nebo VMS systému, který by se staral o jejich správu a zabezpečoval by tak obrazový záznam. SW VAR-NET Integral bude vybaven vizualizačním modulem pro správu, záznam a monitoring 10 IP kamer vybraného druhu. Modul VSS integrační platformy bude komunikovat s jednotlivými kamerovými body prostřednictvím specifického protokolu Dynacolor.

5.2.1.2 HW a SW nároky na server IPS

Skladba systému VAR-NET Integral je modulová, v závislosti na počtu a typu technologií bude integrační platforma doplněna o SW licenční modulové okruhy ve skladbě:

- základní jádro, které bude využito pro sledování, správu a vyhodnocování systému Paradox Digiplex EVO,
- okruh CCTV pro správu deseti kamerových bodů k platformě,
- okruh EPS pro vizualizaci systému Job Detectomat detect 3004 v grafickém prostředí,
- okruh pro SKV uváděný jako modul pro přístup 800 osob.

Kromě jmenovaných modulů bude instalace taktéž doplněna o modul mapového rozhraní pro vizualizaci. Pro efektivní a rychlý přehled je systém doplněn o ovládání přes mobilní telefon prostřednictvím modulu PDA klienta. V případě požadavku o stravovací nebo do-

cházkový systému, je možné kdykoliv systém doplnit o moduly zastřešující tyto specifické nepoplachové funkce.

Samotný server pro centralizaci dat a řízení IPS bude vybaven následujícími komponenty uvedenými v tabulce níže. Parametry serveru jsou stanoveny v závislosti na SW vybavení a náročnosti integrační platformy VAR-NET Integrál v navržené konfiguraci.

Tab. 16: Konfigurace serveru pro IPS

Součást serveru	**Zvolená konfigurace**
Procesor	Intel Core i5-4460
Operační paměť	4GB RAM
Pevný disk	500 GB
Operační systém	Windows Web Server 2008
SQL Server	MS SQL Server 2008 Express

5.3 Návrh systému IPS ve výrobní společnosti

Ve výrobní společnosti se nachází objekty jak administrativního typu, tak i objekty výrobní povahy. Nachází se tu spousta, v řádu desítek objektů a tím souvisí počet poplachových i nepoplachových technologií poměrně velkých rozsahů. Z těchto předpokladů vycházejí obecné požadavky na integrovaný poplachový systém:

- přehledná správa podsystémů,
- efektivní řízení velkého množství technologií,
- zvýšení efektivity ostrahy,
- zabezpečení řízené evakuace,
- a zvýšení bezpečnosti v chráněných prostorech.

Mezi konkrétní poplachové technologie, které jsou do modelového objektu aplikovány, patří následující systémy:

1) PZTS systém Honeywell Galaxy GD520, disponující 520 drátových a 192 bezdrátových zón pro detektory, 32 podsystémů a podporou IP komunikace.
2) Systém EPS Esser typu FlexES Control obsahující maximálně 18 kruhových linek s kapacitou až 2286 požárních hlásičů. Esser FlexES Control disponuje i prvky pro řešení řízené evakuace v rámci chráněných objektů.

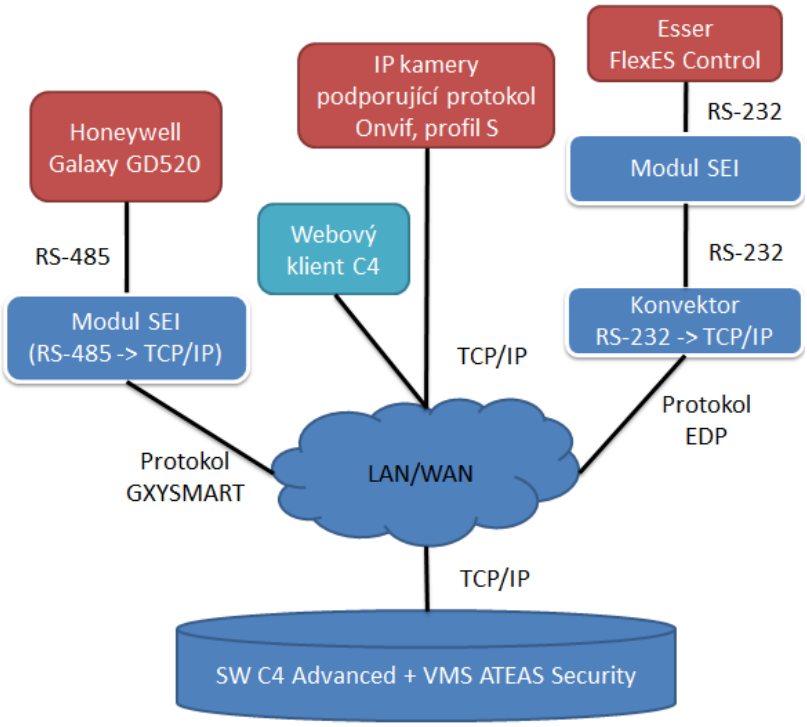
3) VSS je realizovaný formou video management systému ATEAS Security ve verzi Unlimited bez omezeného počtu IP kamerových bodů. Součástí VMS je modul pro rozpoznávání registračních značek vozidel.
4) SKV bude řešen jako doplňující modul ústředny Honeywell Galaxy GD520.
   V tomto případě jde o integraci již na nižší, hardwarové úrovni formou modulačního systému PZTS. Rozšiřující modul C081 je určen pro ovládání dvou přístupových bodů a tím, že lze do systému GD520 připojit až 32 těchto modulů, může být celkově ovládáno až 64 přístupových bodů.

5.3.1 Volba Integrační platformy

Na základě specifických technologií, které jsou charakterizovány v typizovaném firemním areálu, je pro zrealizování integrovaného poplachového systému nejvhodnější nasadit integrační SW platformu C4. Pro nejefektivnější správu velkého množství objektů je vhodné zvolit tu verzi systému, která objekty člení do záložek neboli karet s podrobnými informacemi o provozu a taktéž poskytuje správu a kontrolu obchůzek bezpečnostní agentury. Těmto zvláštním požadavkům odpovídá nejvyšší verze Advanced programu C4. Typ edice je koncipovaná na monitoring 24 hodin v 7 dní v týdnu a lze ji používat jako plnohodnotné DPPC spolu s režimovými opatřeními.

5.3.1.1 Způsoby propojení s podsystémy

Způsoby a komunikační technologie, které budou jednotlivé systémy využívat pro obousměrný přenos dat se SW nadstavbou, jsou znázorněny na schématu níže.



Obr. 28: Modelový návrh IPS

PZTS a SKV

Ústředna Honeywell Galaxy GD520 za účelem integrace do softwarové nadstavby bude vybavena komunikačním rozhraním Galaxy GxySmart. Tento interface je připojen k ústředně sběrnicí RS-485 a k integrační platformě je připojen technologií TCP/IP. Pracuje s komunikačním protokolem GXYSMART, jež integrační platforma C4 plně podporuje.

EPS

Systém Esser FlexES Control se systémem C4 bude komunikovat na základě ovladače Esser SEI připojeného ke sběrnici ústředny. Výstup z tohoto zařízení je ve formě sériové sběrnice RS-232 a k tomu, aby bylo možné propojit systém EPS s integrační platformou je zapotřebí HW konvektoru, převádějící RS-232 na standard TCP/IP. Jako komunikační protokol modul SEI používá specifický datový protokol Esseru uváděný pod zkratkou EDP.

VSS

Kamerový systém je složený z jednotlivých IP kamer a to bez ohledu na výrobce. Podmínkou připojení konkrétního typu kamery je však podpora protokolu Onvif profil S, který taktéž podporuje ATEAS Security v neomezeném počtu. VMS je s integrační SW nadstav-

bou provázán protokolem html, přenášející veškerá obrazová data spolu s metadaty. Jak je již z obrázku zřejmé, pro integrační platformu a VMS bude použit společný HW server.

Ostatní technologie nepoplachového rázu, jako jsou MaR, parkovací, stravovací popřípadě mzdové systémy můžou být připojeny k integrované platformě s pomocí otevřených standardů, jež platforma C4 podporuje a mezi které patří OPC, Modbus, SNMP atd. Verze Advanced taktéž podporuje export dat do jiných informačních systémů.

5.3.1.2 HW a SW nároky na realizování IPS

Z důvodu zabezpečení dat proti ztrátě nebo zničení a především pro zajištění již zmíněného režimu 24/7 je zcela na místě zvolit určitou redundanci dat a systémových prostředků. Z těchto požadavků vyplývá vhodnost navržený systém vybavit nikoliv jedním, ale dvěma servery, které by byly zcela duplikační. Úložiště je navrženo jako síťové úložiště (NAS) tvořené polem RAID 1, kdy se provádí zrcadlení identických disků na serverech. Architektura NAS RAID 1 tak poskytuje poměrně efektivní ochranu dat proti ztrátě. V případě výpadku jednoho z nich nebo v případě údržby serveru, by ten druhý, záložní server přebral veškerou činnost systému. Systém C4 ve verzi Advanced již obsahuje licenci pro dva servery.

Tab. 17: Konfigurace serveru pro platformu C4 a VMS

Součást serveru	**Konfigurace**
Procesor	Intel Xeon E3-1276 V3
Operační paměť	8GB RAM
Diskové pole	NAS – RAID 1
Velikost úložiště	1T
Grafický čip na CPU	Intel HD Graphics P4600
Operační systém	Windows Server 2008
SQL Server	MS SQL Server 2008 Express

Vzhledem k tomu, že platforma C4 a VMS jsou nainstalovány na jednom serveru, je zvolená konfigurace především dimenzována pro potřeby VMS systému, který má o mnohem hardwarově větší nároky, než samotná nadstavba C4. O zpracování a komprimaci dat se bude starat serverový čtyřjádrový procesor Intel Xeon E3-1276 V3 o taktu 3,6 GHz. Velikost úložiště je přímo závislé na počtu kamerových bodů, obrazovém rozlišení a kompri-

mačním formátu. Hodnota úložiště pro 100 kamer, kdy obrazová data jsou v rozlišení 720p ve formátu H.264 je úložiště orientačně vypočtena na cca 700 GB při uchovávání záznamu na 7dní. Zvolené je však úložiště o velikosti 1T zahrnující i instalaci integrační platformy a VMS systému.

5.4 Modelový návrh IPS pro zdravotnické zařízení

Zařízení zdravotnického typu pro účel modelového návrhu IPS můžeme charakterizovat jako areál s mnoha objekty obsahující poměrně cenná aktiva ve formě specializovaných zařízení, přístrojů, zdravotnického materiálu apod. Stupeň zabezpečení celého navrhovaného bezpečnostního systému bude proto odpovídat trojce, zahrnující opatření pro střední až vysoká bezpečnostní rizika. Aplikované bezpečnostní systémy v namodelovaných objektech zdravotnického zařízení jsou následující:

1) PZTS sběrnicový systém Siemens SPC6000 nabízející až 512 drátových zón spolu se 120 bezdrátovými zónami, které lze rozčlenit dokonce na 60 oblastí. Systém je vybavený Ethernetovým portem a je certifikovaný dle standardu ČSN EN 50131 pro stupeň zabezpečení 3.
2) Modulární EPS systém Bosh FPA-5000, který je charakteristický analogovými okruhy, kterých může být maximálně 32, kde je možné zapojit až 46 různých modulů (např. komunikační modul, reléový modul, modul požární ochrany apod.) a 4096 adresovatelných detekčních a signalizačních prvků.
3) Kamerový systém VSS je řešen aplikováním řadou IP kamer značky Hikvision v celkovém počtu 30.
4) SKV v modelovém objektu je řešen systémem ASSA ABLOY ARX, v kterém může být neomezený počet Access kontrolérů, obsahující čtečky karet, klávesnice, elektronické zámky, detektory otevření a odchodová tlačítka, jež mohou ovládat až 16 dveří. Systém ASSA ABLOY ARX je taktéž certifikovaný pro zabezpečení stupně 3.

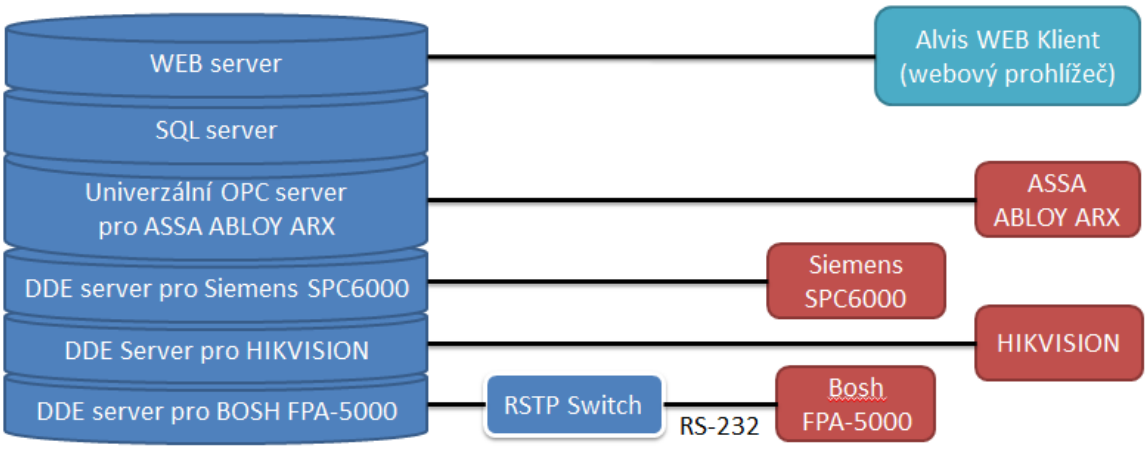
5.4.1 Typ integrační platformy

Modelový návrh, obsahující bezpečnostní systémy Siemens SPC6000, Bosh FPA-5000, ASSA ABLOY ARX a kamery značky Hikvision, je pro centrální správu a vizualizaci nejlépe vybavit integrační platformou Alvis. SW Alvis, kromě jmenovaných systémů, taktéž

podporuje komunikační standard Espa-x, který je používán pro komunikaci se specifickými systémy přivolání pomoci, jež by mohly být taktéž integrovány do IPS.

5.4.1.1 Způsoby propojení platformy s bezpečnostními systémy

Propojení platformy Alvis se systémy Siemens SPC6000, Bosh FPA-5000, ASSA ABLOY ARX a kamery značky Hikvision bude realizováno podle nákresu a následujícího popisu.



Obr. 29: Schéma propojení IPS

PZTS a VSS

Zabezpečovací systém Siemens SPC6000 a kamerový systém Hikvision komunikuje s platformou Alvis prostřednictvím protokolu DDE pro vzájemnou výměnu dat. Server platformy Alvis je rozšířen o jednotlivé DDE servery zajišťující komunikaci s DEE klienty systémů PZTS a VSS, které jsou již implementovány do firmwarů bezpečnostních systémů.

EPS

Systém Bosh FPA-5000 je s integrační platformou Alvis propojen prostřednictvím tzv. RSTP switche, který zabezpečuje konvergenci topologie komunikačního standardu RS-232 na komunikaci TCP/IP. Server Alvisu je taktéž doplněn o DDE server pro zajištění komunikace s ústřednou systému Bosh FPA-5000.

SKV

Přístupový systém ASSA ABLOY ARX bude s nadstavbovým systémem Alvis komunikovat prostřednictvím univerzálního OPC serveru, jak je zřejmé ze schématu propojení IPS.

5.4.1.2 Předpoklady na HW a SW vybavení

V návaznosti na zvolené technologie, které jsou součástí modelového návrhu IPS pro objekty zdravotnického rázu, je stanovená konfigurace serveru zastřešující komplexní sběr, správu a reprodukci informací následující dle tabulky 18.

Tab. 18: Vlastnosti serveru pro SW Alvis

Součást serveru	**Zvolená konfigurace**
Procesor	Intel Core i3-4370
Grafický čip na CPU	Intel HD Graphics 4600
Operační paměť	2 GB RAM
Pevný disk	320 GB
Operační systém	Windows Server 2008
SQL Server	MS SQL Server 2008

Dvoujádrový procesor Intel Core i3-4370 s taktem 3,80GHz je zcela dostačující pro činnost serveru a integrační nadstavby Alvis, která není z hardwarového pohledu příliš náročná na výpočetní výkon. Velikost datového úložiště je taktéž dimenzováno převážně na nároky kladené platformou Alvis, protože úložiště obrazových záznamů je řešeno v rámci zařízení NVR systému VSS Hikvision. Kromě zmíněného databázového serveru bude instalace vybavena DDE servery a univerzálním serverem OPC, o kterých již byla zmínka v ohledu na způsoby komunikace se subsystémy.

5.5 Komparační studie modelových návrhů integrovaných poplachových systémů

Na modelové návrhy IPS lze pohlížet z několika úhlů v závislosti na typických vlastnostech. Komparace neboli vzájemné posouzení specifických vlastností navržených systémů je založeno na čtyřech stanovených hodnotících kritériích, mezi která patří:

a) typ, verze a velikost použitých bezpečnostních subsystémů a zvolené integrační platformy,
b) porovnání obecných charakteristických vlastností, mezi které patří modulárnost, velikost, rozšiřitelnost a nákladnost navržených systémů,
c) zhodnocení z pohledu použitých komunikačních standardů, stupňů zabezpečení a výpočetní náročnosti a

d) komparace vlastností navržených architektur IPS.

Tab. 19: Porovnání modulových návrhů podle použitých technologií

Modelový návrh IPS	**PZTS**	**EPS**	**VSS**	**SKV**	**Integrační Platforma**
Rezidence	DSC Power PC 1832	-	Canon	-	SBI Portál
Ubytovací zařízení	Paradox Digiplex EVO192	Job Detectomat Detect 3004	ACTi	Paradox Digiplex EVO 192	VAR-NET Integral
Výrobní společnost	Honeywell Galaxy GD520	Esser FlexES Control	ATEAS Security Unlimited	Honeywell Galaxy GD520	C4
Zdravotnické zařízení	Siemens SPC6000	Bosh FPA-5000	Hikvision	ASSA ABLOY ARX	Alvis

Obecně lze modelové návrhy porovnat podle specifických bezpečnostních technologií, na základě kterých byly zvoleny i vhodné integrační platformy pro ucelené řešení správy, řízení a vizualizaci. Volba integrační platformy byla provedena především na základě podpory komunikace výrobcem SW platformy, popřípadě podpory jednoho z univerzálních komunikačních standardů ze strany nadstavbového systému i bezpečnostního poplachového systému. V typizovaných modelových návrzích pro ubytovací zařízení a výrobní společnost, se v částech tabulky PZTS a SKV objevují identické systémy, protože integrace těchto subsystémů je provedena již na hardwarové úrovni formou doplňkového modulu pro kontrolu přístupu.

Tab. 20: Komparační tabulka charakteristických vlastností modelových návrhů IPS

Modelový návrh IPS	**Rozšiřitelnost**	**Modulárnost**	**Velikost IPS**	**Nákladnost realizace**	**Použití jako DPPC**
Rezidence	-	-	Malá	Nízká	-
Ubytovací Zařízení	+	+	Střední	Střední	+
Výrobní Společnost	+	+	Střední	Velmi Vysoká	+
Zdravotnické zařízení	+	+	Střední	Vysoká	+

V komparační tabulce číslo 20 jsou návrhy posuzovány dle uvedených vlastností. Návrh systému pro objekt rezidenčního typu se v porovnání s ostatními návrhy značně odlišuje, protože navržený IPS nedisponuje rysy jako je modulárnost, rozšiřitelnost a především koncepce není vhodná pro použití plnohodnotného samostatného pracoviště DPPC v režimu 24/7. Důvodem je nasazení systému do malého objektu a s tím související požadavky na malou nákladnost systému, přehlednost integrace, nízkou HW a SW náročnost, která je zmíněná v následující tabulce.

Tab. 21: Komparační tabulka specifických vlastností návrhů IPS

Modelový návrh IPS	**Stupeň Zabezpečení**	**Komunikační Standard**	**HW a SW Náročnost**
Rezidence	**2**	**-**	**Žádná**
Ubytovací Zařízení	**2**	**Ascii**	**Střední**
Výrobní společnost	**2**	**GXYSMART, EDP a ONVIF**	**Vysoká**
Zdravotnické zařízení	**3**	**DDE a OPC**	**Střední**

Všechny modelové návrhy jsou navrženy v určitém stupni zabezpečení, přičemž platí, že všechny součásti IPS jsou schváleny a certifikovány minimálně pro stanovenou úroveň zabezpečení. Tabulka rovněž sumarizuje komunikační standardy, které byly použity pro vzájemný přenos dat mezi jednotlivými systémy a integrační nadstavbou. HW a SW náročnost se týká serveru, na kterém běží instalace SW IPS, centralizující veškerá data. V objektu rezidence se nenachází žádný HW ani SW pro centrální správu, jelikož je integrace systému provozována jako služba v cloudovém úložišti.

Tab. 22: Porovnání návrhů dle architektury

Modelový návrh IPS	**Úroveň integrace**	**Typ integrace**	**Redundance**
Rezidence	**IN/OUT**	**Typ 1**	**-**
Ubytovací Zařízení	**Modul/SW**	**Typ 2B**	**-**
Výrobní Společnost	**Modul/SW**	**Typ 2B**	**+**
Zdravotnické zařízení	**SW**	**Typ 2A**	**-**

V poslední tabulce komparační studie je uveden přehled použité úrovně integrace, na kterou částečně navazuje typ navržené integrace. Provedená integrace v rezidenčním objektu je typu 1, protože jde o aplikaci, kde jsou instalovány jen jednoúčelové poplachové a nepoplachové systémy, a zároveň jsou dále připojeny ke společnému doplňkovému zařízení prostřednictvím doplňkové přenosové trasy. Dle technického předpisu ČSN CLC/TS 50398 lze navržené systémy pro ubytovací zařízení a výrobní společnost zahrnout do konfigurace Typu 2B spočívající v integraci systému PZTS a SKV již na HW úrovni. Případná porucha ústředny PZTS může mít negativní účinek na systém SKV, jelikož je doplňkovým modulem zabezpečovací ústředny. Proto jsou tyto návrhy zahrnuty do Typu 2B. Naopak IPS ve zdravotnickém zařízení je koncipován tak, že jsou pro vlastní činnost využívány společné přenosové trasy, společná zařízení a vybavení s tím rozdílem, aby případně vzniklá porucha v kterékoliv jedné aplikaci neměla žádný negativní účinek na jinou další aplikaci. Tomuto typu integrace odpovídá Typ 2A. Jako redundantní je označen navržený systém pro výrobní společnost, protože součástí návrhu je druhý duplikační záložní server pro zajištění služeb v případě výpadku primárního serveru.

Dílčí závěr kapitoly

Provedené modelové návrhy IPS vycházejí ze zpracovaných informací z předešlých částí práce. Pro skladbu samotných návrhů byla pak zásadně rozhodující kapitola týkající se analýz jednotlivých integračních platforem. Koncepty jednotlivých IPS jsou zpracovány s důrazem na kompatibilitu zvolené integrační platformy s jednotlivými bezpečnostními subsystémy. Veškeré návrhy je možné rozšířit o další systémy poplachového i nepoplachového rázu v závislosti na specifické požadavky, které se můžou v praxi vyskytnout. Integrace je proveditelná za předpokladu, že daný systém bude podporovat přinejmenším jeden z otevřených komunikačních standardů, který je zároveň podporován i aplikovanou integrační platformou. V případě nekompatibility systémů je ještě možnost požadavky zkonzultovat se systémovým integrátorem platformy od dané vývojové společnosti a s pomocí nástroje SDK sjednotit typ přenosu dat.

ZÁVĚR

Dříve, než se systémový integrátor jako dodavatel služby systémové integrace začne zabývat samotným vlastním návrhem integrovaného poplachového systému, měl by svou pozornost věnovat nejprve legislativě. Legislativní postuláty ohledně návrhů IPS, vychází především z technických norem, které stanovují požadavky na systémovou integritu, komunikaci, doplňková ovládací zařízení, použité komponenty a propojení mezi nimi. Zvláštní požadavky jsou pak kladeny na nutnost vybavení systému EPS grafickou SW nadstavbou a to v konkrétních případech uvedených v normách. Po legislativní části je vhodné se věnovat části technické, neboli té pasáži práce, kde jsou systematicky rozebrány konstrukční způsoby realizování integrovaných systémů. Principiálně lze integrované systémy rozdělit dle koncepce na HW a SW integraci, přičemž u méně rozsáhlých a složitých aplikací dáváme přednost integraci HW typu. V případě velkých a poměrně složitých aplikací je naopak vhodné aplikovat spíše SW integraci, disponující pokročilými nástroji pro efektivní správu, řízení a vizualizaci komplexního IPS. S problematikou integrace neboli procesu spojování ve vyšší celek úzce souvisí komunikační rozhraní a posléze komunikační standardy. Ty lze rozčlenit na univerzální tzv. otevřené standardy, jejichž princip a struktura je volně k dispozici pro zrealizování komunikace a specifické standardy, vytvořené jen pro přenos dat mezi konkrétními systémy. Při návrhu vzájemných datových vazeb mezi systémy je v případě existence obou typů standardů vhodné přednostně použít ten specifický a to z toho důvodu, že již od začátku jeho vývoje bylo počítáno s nasazením do konkrétních systémů a tím došlo k jeho modifikaci s ohledem na určité požadované funkcionality. V důkladně provedené analýze a následné komparační studii integračních platforem se komunikační standardy objevují jako jeden z hlavních aspektů posuzovaných kritérií. Mezi ostatní kritéria, mající podstatný vliv na obsahovou koncepci modelových návrhů, patří porovnání podle dostupných funkcionalit, způsobů ovládání a vhodnost v závislosti na velikosti a specifickém typu aplikace. Veškeré legislativní a technické poznatky, provedené analýzy a komparační studie z dané problematiky byly zúročeny v celkem čtyřech konečných návrzích IPS. Modelové koncepce jsou provedeny v souladu s vytyčenými výchozími požadavky, vztahující se na požadovanou funkcionalitu systému a charakterizované typem zvolených objektů. Jedním z důležitých vlastností navržených systémů je možnost rozšíření či modifikace realizovaného IPS. Obsah této diplomové práce může sloužit jako technologický postup činnosti systémového integrátora v rámci realizace SW vybavení pracoviště dohledového poplachového přijímacího centa.

SEZNAM POUŽITÉ LITERATURY

[1] DRGA, Rudolf. *Speciální technologie komerční bezpečnosti*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-146-9.

[2] ČSN CLC/TS 50398. *Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. 20s. Třídící znak 334597.

[3] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.: [teorie a praxe ochrany majetku a fyzické bezpečnosti]*. 1. vyd. Zlín: VeRBuM, 2011. ISBN 978-808-7500-057.

[4] ČSN CLC/TS 50131-1. *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy, Část 1: Systémové požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2007. 40s. Třídící znak 334591

[5] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II.: [teorie a praxe ochrany majetku a fyzické bezpečnosti]*. 1. vyd. Zlín: VeRBuM, 2012. ISBN 978-808-7500-194.

[6] ČSN EN 50132-1. *Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích, Část 1: Systémové požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. 40s. Třídící znak 334592.

[7] ČSN EN 50132-7 *Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích, Část 7: Pokyny o aplikaci*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. 28s. Třídící znak 334592.

[8] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management IV.: [teorie a praxe ochrany majetku a fyzické bezpečnosti]*. 1. vyd. Zlín: VeRBuM, 2014. ISBN 978-808-7500-576.

[9] MIKULA, Tomáš. ČSN EN 60839-11-1 nová definice standardu ACS. ALARM FOCUS: technika - řešení - teorie - firmy - legislativa. 2014, roč. 2014, č. 1, ISSN 1805-9007.

[10] ČSN EN 60839-11-1. *Poplachové a elektronické bezpečnostní systémy, Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 55s. Třídící znak 334593.

[11] ČSN EN 50133-1. *Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích, Část 1: Systémové požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2001. 28s. Třídící znak 334593.

[12] ČSN EN 50133-7 *Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích, Část 7: Pokyny o aplikaci*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2000. 16s. Třídící znak 334593.

[13] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management III.: [teorie a praxe ochrany majetku a fyzické bezpečnosti]*. 1. vyd. Zlín: VeRBuM, 2013. ISBN 978-808-7500-354.

[14] Česká republika. Zákon č. 133/1985 Sb. o požární ochraně, ve znění pozdějších předpisů. In: *Sbírka zákonů*. 1985.

[15] Česká republika. Vyhláška č. 23/2008 Sb. o technických podmínkách požární ochrany staveb. In: *Sbírka zákonů*. 2008.

[16] Česká republika. Vyhláška č. 246/2001 Sb. o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru. In: *Sbírka zákonů*. 2001.

[17] ČSN EN 73 0875. *Požární bezpečnost staveb - Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. 20s. Třídící znak: 730875.

[18] ČSN EN 34 2710. *Elektrická požární signalizace - projektování, montáž, užívání, provoz, kontrola, servis a údržba*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. 100s. třídící znak: 342710.

[19] SOUKUP, Jiří. *Integrace systémů elektrické požární signalizace*. 2013. Diplomová práce. UTB ve Zlíně. Vedoucí práce Ing. Jan Valouch, Ph.D.

[20] VALOUCH, Jan. *Projektování integrovaných systémů*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj (152 s.). ISBN 978-80-7454-296-1.

[21] RONEŠOVÁ, Ing. Andrea. *Přehled protokolu MODBUS*. 2005. Dostupné také z: http://home.zcu.cz/~ronesova/bastl/files/modbus.pdf.

[22] NOSEK, Jiří. Administrace počítačových sítí. : *OPC Server - funkce a využití v průmyslové automatizaci*. 2011. Dostupné také z: http://www1.fs.cvut.cz/cz/u12110/site/Nosek-OPC_server.pdf.

[23] BRÁBLÍK, Radim. *Datalogger pro zaznamenávání měřených veličin* [online]. Brno, 2008 [cit. 2015-05-19]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=8292. Bakalářská práce. VUT Brno. Vedoucí práce Ing. Zdenek Bradáč, Ph.D.

[24] VÖRÖŠ, Juraj. 2004. *Inteligentné riadenie pomocou PLC Simatic S7 s podporou Matlabu*. Bratislava. Diplomová práce. Slovenská technická univerzita v Bratislave. Vedoucí práce Ján Mikleš.

[25] Brainboxes - RS422/485 RS232 Serial Cards. *ASCII protocol and commands* [online]. 2015 [cit. 2015-05-19]. Dostupné z: http://www.brainboxes.com/faq/items/ascii-protocol-and-commands.

[26] Extensible Markup Language. *Wikipedia: The free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2015 [cit. 2015-05-19].

[27] The European Selective Paging Manufacturer's Association. 2015. General Information on ESPA-X [online]. [cit. 2015-05-17]. Dostupné z: http://www.espa-x.org/en.html.

[28] BOUŠKA, Petr. *SNMP - Simple Network Management Protocol* [online]. 2006 [cit. 2015-05-19]. Dostupné z: http://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/.

[29] JANOVSKÝ, Dušan. *Jak psát web* [online]. Slaný: Dušan Janovský, 2015 [cit. 2015-05-19]. ISSN 1801-0458. Dostupné z: http://www.jakpsatweb.cz.

[30] ONVIF*: The IP-based Security Standard* [online]. 2015 [cit. 2015-05-19]. Dostupné z: http://www.onvif.org.

[31] ABBAS, a.s. *Produkty a služby: Integrace* [online]. 2015 [cit. 2015-05-19]. Dostupné z: http://www.abbas.cz/produkty-a-sluzby/integrace.

[32] ESTELAR S.R.O. *SBI: Nadstavbový systém pro sledování, správu a vyhodnocování elektronických systémů budov* [online]. 2014 [cit. 2015-05-19]. Dostupné z: http://www.estelar.cz/media/document/docsbi.pdf

[33] METEL S.R.O. *C4 software: Integrační bezpečnostní systém C4* [online]. 2014 [cit. 2015-05-19]. Dostupné z: http://www.metel.eu/produkty/aplikace?itemCat=5&itemId=3.

[34] DOMINUS MILLENNIUM, ABBAS, A.S. *SW C4* [online]. 2015 [cit. 2015-05-19]. Dostupné z: http://www.dominus.cz/software/c4.

[35] SPIRIT - INFORMAČNÉ SYSTÉMY, A.S. *Alvis: Alarm Visualization System* [online]. 2013 [cit. 2015-05-19]. Dostupné z: http://www.alvis.sk/index.php.

[36] INTEGOO S.R.O. *INTEGRA: SW pro správu a řízení bezpečnosti* [online]. 2015 [cit. 2015-05-20]. Dostupné z: http://www.integoo.cz/produkty-v2/integra-v2.html#i08.

[37] VARIANT PLUS, SPOL. S R.O. *Obor integrace systémů budov: VAR-NET Integral* [online]. 2015 [cit. 2015-05-20]. Dostupné z: http://www.variant.cz.

[38] VARIANT PLUS, SPOL. S R.O. *Systém VAR-NET Integral: Popis technologie, modularita systému a integrované hardwarové technologie* [online]. 2015 [cit. 2015-05-20]. Dostupné z: http://www.integracebudov.cz.

[39] TRADE FIDES. A.S. *LATIS SQL: Monitorovací a integrační systém* [online]. 2015 [cit. 2015-05-20]. Dostupné z: https://www.fides.cz/nase-produkty/latis-sql.html.

[40] AXXONSOFT CORPORATION. *Axxon Next and Axxon Intellect Enterprise: Video Surveillance and Security Solutions* [online]. 2015 [cit. 2015-05-20]. Dostupné z: http://www.axxonsoft.com.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DPPC Dohledové poplachové a přijímací centrum.

PZTS Poplachový zabezpečovací a tísňový systém.

CCTV Uzavřený televizní okruh.

SKV Systém kontroly vstupu.

EPS Elektrická požární signalizace.

IPS Integrovaný poplachový systém.

CCF Centrální ovládací zařízení.

BOZP Bezpečnost a ochrana zdraví při práci.

VSS Video dohledový systém.

SHZ Stabilní hasicí zařízení.

VFD Video fire detection.

PBZ Požárně bezpečnostní zařízení.

ZDP Zařízení dálkového přenosu.

OPPO Obslužný pult požární ochrany.

KTOP Klíčový trezor požární ochrany.

SBI Secure Building Inteligence.

MaR Systémy pro měření a regulaci.

HVAC Heating, ventilating, air-conditioning (topeni, větráni, klimatizace).

GIS Geografický informační systém.

WSDL Web Services Description Language.

SDK Software development kit.

IS Informační systém.

PLC Programovatelný logický automat.

PDU Protocol Data Unit.

ADU	Application Data Unit.
OPC	Open Proces Control.
DDE	Dynamic Data Exchange.
PGM	Programovatelný výstup.
XML	eXtensible Markup Language.
Espa-x	Enhanced Signaling Protocol for Alarm Processes – XML-based.
VoIP	Voice over IP.
SNMP	Simple Network Management Protocol.
UDP	User Datagram Protokol.
HTML	Hyper Text Markup Language.
IBS	Integrovaný bezpečnostní systém.
KŘ	Krizové řízení
MKDS	Městský kamerový a dohledový systém.
DVR	Digitální videorekordér.
NAS	Datové úložiště na síti.
RAID	Vícenásobné diskové pole nezávislých disků.
NVR	Network video rekordér.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK