Bezpečnostní projekt video dohledového přístupového systému rozsáhlé výrobní společnosti

Bc. Adam Zvara

Diplomová práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

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

Jméno a příjmení:	**Bc. Adam Zvara**
Osobní číslo:	**A15189**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnostní projekt video dohledového přístupového systému rozsáhlé výrobní společnosti**
Téma anglicky:	**A Large Scale Industry Company Security Video Surveillance Access System Project**

Zásady pro vypracování:

1. **Analyzujte funkční vlastnosti video dohledových systémů.**
2. **Pojednejte o funkčních vlastnostech systémů kontroly vstupu.**
3. **Popište technicko-technologické možnosti synergie video-dohledových systémů a systémů kontroly vstupu.**
4. **Specifikujte možnosti propojení video-dohledových systémů a systémů kontroly vstupu konkrétního výrobního podniku.**
5. **Zpracujte bezpečnostního projekt video-dohledového přístupového systému**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LUKÁŠ, Luděk. Bezpečnostní technologie systémy a management II. Zlín: VeRBuM, 2012. ISBN 978-80-87500-19-4.**
2. **VALOUCH, Jan. Projektování integrovaných systémů. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 152 s. ISBN 978-80-7454-296-1.**
3. **ČSN EN 60839-11-1: Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty. 2014.**
4. **ČSN EN 60839-11-2: Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace. 2015.**
5. **ČSN EN 62676-1-1: Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně. 2014.**
6. **ČSN EN 62676-4: Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 4: Pokyny pro aplikace. 2016.**

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

Datum zadání diplomové práce: **3. února 2017**

Termín odevzdání diplomové práce: **24. května 2017**

Ve Zlíně dne 3. února 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

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

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Jméno, příjmení: Adam Zvara

Název bakalářské/diplomové práce: Bezpečnostní projekt video dohledového přístupového systému rozsáhlé výrobní společnosti

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 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 jsem seznámen s tím, že na moji diplomovou 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 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 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 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, dne …….

ABSTRAKT

V teoretickej časti sa diplomová práca zaoberá rozborom systémov kontroly vstupu a videodohľadových systémov. Analyzuje legislatívny rámec, ich funkčné vlastnosti, integráciu a spôsoby prepojenia týchto systémov. Prvá časť praktickej časti predstavuje spoločnosť so zameraním na prístupové body a využitie jej súčasných systémov. Druhá časť praktickej časti sa zaoberá bezpečnostným návrhom vhodnej integrácie s overením funkčnosti v laboratóriu FAI UTB.

Kľúčové slova: Systém kontroly vstupu, video dohľadový systém, hardwaroví integrácia softwarová integrácia, výrobná spoločnosť, výrobná spoločnosť, návrh.

ABSTRACT

The theoretical part the Master's thesis talks about access control systems and video surveillance systems. It analyzes the legislative framework, their functional characteristics, integration and ways of interconnecting these systems. The first part of the practical part a company is introduced and after the focus shifts to the access points and the use of the company's current systems. The second part of the practical part deals with the security design of the appropriate integration, the functional verification is done in the labs of FAI UTB.

Keywords: Access control system, video surveillance system, hardware integration software integrity, manufacturing company, manufacturing company, design.

V prvom rade by som sa rád poďakoval vedúcemu mojej diplomovej práce Ing. Jiřimu Ševčíkovi za odborné vedenie a cenné rady pri vypracovávaní. Ďalej by som rád poďakovel kolektívu výrobnej spoločnosti, rodine a priateľom, ktorý ma počas štúdia podporovali.

„I keď svet ide stále dopredu, mladí ľudia musia vždy začínať od začiatku.“

Johann Wolfgang Goethe

OBSAH

ÚVOD

Diplomová práca je venovaná systémom kontroly vstupu, videonáhľadovým systémom a možnostiam ich vzájomnej integrácie pre danú rozsiahlu výrobnú spoločnosť.

V dnešnej dobe sa takmer každá výrobná spoločnosť snaží zabezpečiť svoj objekt čo najefektívnejším spôsobom. Väčšina spoločností stále využíva jednotlivé zabezpečovacie systémy separovane. Využívanie systémov týmto spôsobom je síce spoľahlivé, ale zďaleka nie je porovnateľné s integrovaným, kompaktným, funkčným celkom. Integrácia systémov je najefektívnejším prostriedkom pre ochranu zdravia, majetku pred poškodením, zničením alebo inému narušeniu spoločnosti. Integrácia ponúka niekoľko foriem prevedenia, ktoré vychádzajú z technického riešenia vzájomného prepojenia systémov. Projekt integrovaného systému závisí najmä od investora a návrhu integrovaného systému. Klasifikácia spôsobu integrácie závisí od analýzy týchto dokumentov: technických noriem, technických špecifikácií výrobcov, inštalačných manuálov a právnych predpisov.

Vďaka neustálym pokrokom a vývoju nových technológií sa objavujú stále novšie a sofistikovanejšie možnosti prístupu do stráženého objektu. Od počiatku vývoja prešla už dlhá doba. Fyzickú stráž vrátnic úplne nahradili elektronické systémy. Systém kontroly vstupu a videodohľadový systém konkrétnej rozsiahlej výrobnej spoločnosti disponuje kvalitným hardwarom a softwarom pre dané vstupy do objektov. Systém kontroly vstupu danej spoločnosti využíva RFID technológiu, ktorú spravuje software Aktion. Ako videodohľadový systém používa IP kamery, ktoré pracujú pod vizualizačným softwarom Ateas.

Cieľom teoretickej časti práce je zhromaždiť informácie o systémoch kontroly vstupu a video dohľadových systémoch a to s primárnym zameraním na ich funkčné vlastnosti, ktoré sú obsiahnuté v technických normách. Následne analyzovať všetky možnosti prepojenia týchto dvoch systémov. Praktická časť sa zameria na konkrétne informácie a možnosti spoločnosti na základe, ktorých bude vypracovaný projekt pre komplexný video-dohľadový prístupový systém.

I. TEORETICKÁ ČASŤ

1 SYSTÉMY KONTROLY VSTUPU

Systémy kontroly vstupu (SKV) sú používané v bezpečnostných aplikáciách, kde zastupujú jeden z typov poplachových systémov. Často používaným termínom je aj elektronický systém kontroly vstupu (EACS), ktorý je vlastne synonymom pre systémy kontroly vstupu. Tieto systémy je možné definovať ako systémy obsahujúce konštrukčné a organizačné opatrenia vrátane zariadení nevyhnutných na riadenie vstupu. Hlavným prínosom SKV je riadenie prístupu z hľadiska managementu, ktoré zahŕňa kedy, a kto má prístup do zabezpečeného objektu, pričom je nutné eliminovať riziko nepovolených vstupov. [1]

Dôležité je definovať rozdiel medzi prístupovým a dochádzkovým systémom. Prístupový systém riadi prístup k oblastiam, ktoré sú chránené zariadeniami k ochrane firemných aktív, informácií a dát. Dochádzkový systém zaznamenáva identitu užívateľa, čas príchodu, čas odchodu, dôvod návštevy a je skvelým pomocníkom pri evidencií pracovnej doby zamestnancov. [1]

1.1 Základné pojmy

Vymedzenie základných pojmov v oblasti SKV zohráva dôležitú úlohu najmä pri zaistení komunikácie medzi zainteresovanými osobami v oblasti jeho realizácie. V nasledujúcej časti sú vysvetlené základné pojmy z tejto oblasti. [1]

1.1.1 Prístupový bod

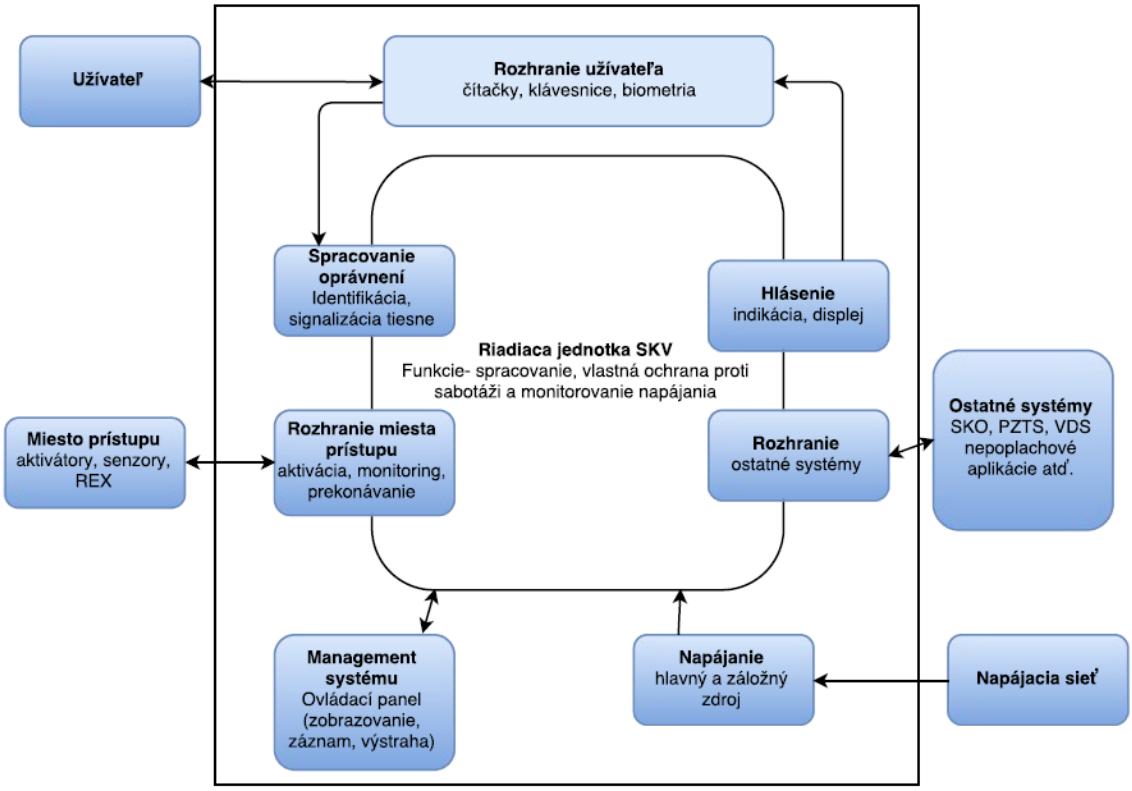
Prístupovým bodom je definované usporiadanie všetkých prvkov, ktoré spolupracujú pri povolení vstupu na danom mieste. [2]

- **Miesto prístupu (portál)-** fyzický vstup alebo výstup, ktorý obsahuje mechanicky ovládané zábranné systémy napr. dvere, závory, turnikety...
- **Riadiaca jednotka kontroly vstupu-** časť elektronického systému kontroly vstupu, ktorá je prepojená s ostatnými komponentami a jej úlohou je rozhodovanie o povolení alebo zamietnutí prístupu do priestoru na danom mieste.
- **Rozhranie miesta prístupu-** zariadenie alebo obvod, ktorý je určený na ovládanie a zaistenie miesta prístupu.
- **Senzor miesta prístupu-** elektrický prvok, ktorý je používaný na monitorovanie stavu prístupu (identifikačné zariadenie, čítačka, klávesnica, biometria).

- **APAS-** ovládacie prvky a senzory miest prístupu
  - vstupné prvky: magnetické kontakty, spínače, optické závory
  - výstupné prvky: zámok motor turniketu atď. [2,3]

1.1.2 Architektúra systému

Základná architektúra je zložená z niekoľkých základných prvkov a ich funkciami, ktoré je možné vidieť na nasledujúcom obrázku s názvom Obr. 1.



Obr. 1 Architektura systému kontroly vstupu [1]

1.1.3 Prístupové práva

Jedným z najdôležitejších faktorov SKV je prideľovanie prístupových práv, ktoré sú prideľované osobám s príslušným stupňom oprávnenia vzhľadom na priestorové, časové, personálne a iné dispozície. Klasifikácia stupňa zabezpečenia je pre každé miesto prístupu normatívne definovaná pomocou triedy identifikácie a prístupu. Pri zabezpečení SKV sú používané 4 triedy identifikácie (0-3) a 2 triedy prístupu (A, B). Túto klasifikáciu zabezpečenia je možné definovať pre každé miesto prístupu (zvlášť pre vstup a zvlášť pre

výstup). Klasifikácia zabezpečenia je nezávislá na kombinácií tried identifikácie a tried prístupu. [4]

Triedy identifikácie

Trieda 0- nevyžaduje priamu identifikáciu. Prístup je umožnený pomocou tlačidla, ktoré obsluhuje fyzická osoba. Táto osoba sa nachádza pri vstupe do objektu a vizuálne kontroluje preukazy, povolenia alebo vstupenky, na základe ktorých povoľuje vstup do daného objektu. [4]

Trieda 1- vyžaduje znalosť informácie, kódu, PIN kódu a pod. Princíp funguje na overení zadaného hesla s údajom v pamäťovej jednotke. [4]

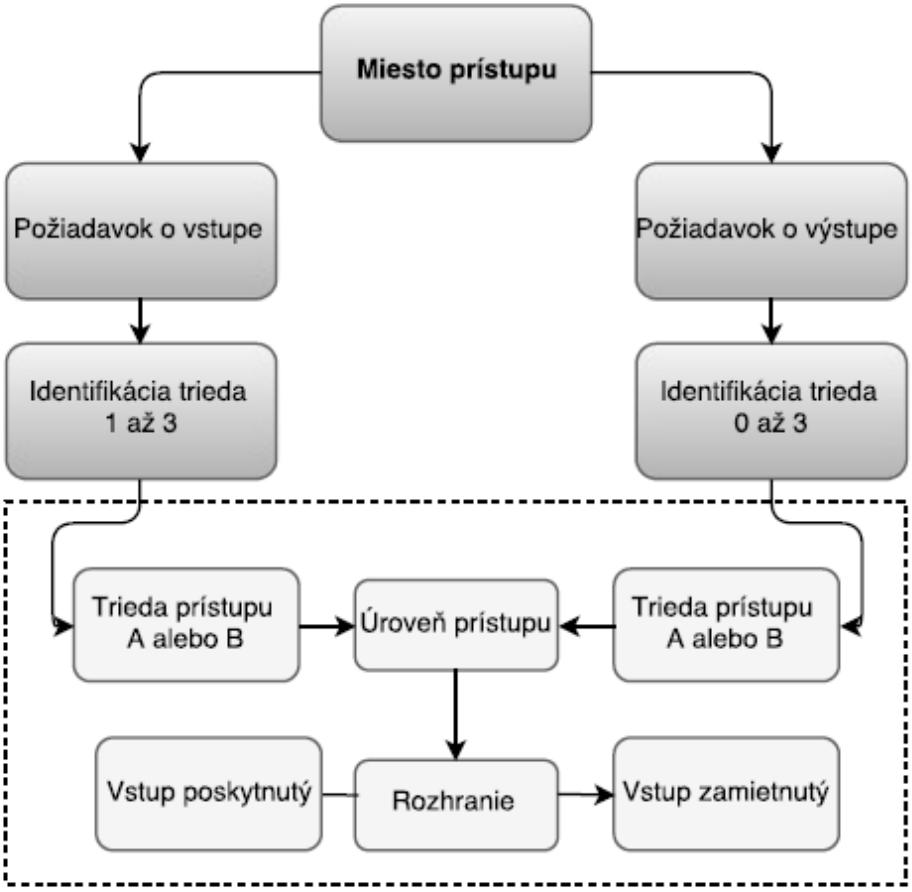
Trieda 2- vyžaduje pevný identifikačný predmet, prístupovú kartu, token alebo biometrický prvok danej osoby (odtlačok prsta, hlas, rozpoznávanie tváre, geometria ruky atď.). Každému užívateľovi musí byť priradená jedinečná identita. V tejto triede je zamedzené využitia identifikačných prvkov viditeľných ľudským okom. [4]

Trieda 3 -vyžaduje kombináciu PIN kódu, hesla a pod. (Trieda 1) s identifikačným prvkom alebo biometrickou metódou (Trieda 2). [4]

Trieda prístupu

Trieda A- nie je vyžadovaný žiadny časový filter, prístup nie je časovo obmedzený a nie je vyžadované ani archivovanie informácií o prístupe. [4]

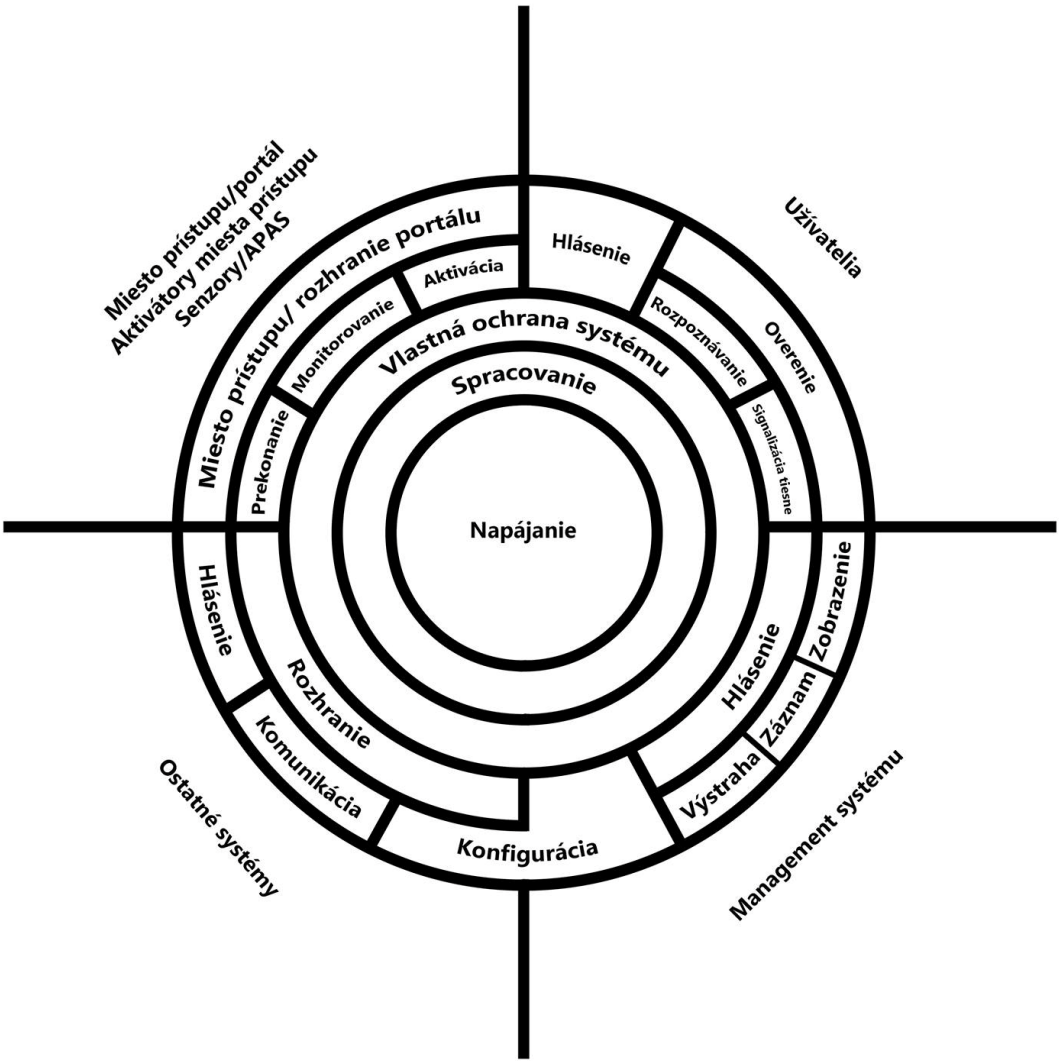
Trieda B- vyžaduje časový filter a ukladá informácie o prístupe. Kvalitnejšie systémy ukladajú do pamäti ďalšie informácie o otvorení bez oprávnenia, vrátane lokalizačných údajov daného miesta. [4]



Obr. 2 Schéma postupu povolenia prístupu [4]

1.2 Funkčné vlastnosti a požiadavky

Podľa normy ČSN EN 60839-11-1 musí SKV poskytovať pre špecifickú konfiguráciu systémov kontroly vstupu nasledujúce funkcie a požiadavky.



Obr. 3 Štruktúra funkčních vlastnosti [5]

1.2.1 Spracovanie

Spracovanie vychádza z metodiky klasifikácie a funkcií stanovenia úrovni ochrany. Všetky požiadavky na činnosť zariadení musia byť vytvorené na základe stupňov odpovedajúcej úrovni ochrany, ktoré sú dosiahnuté v klasifikácií funkcií majúcich vzťahov k bezpečnosti a vzťahov k úrovni rizika. Klasifikácia SKV musí byť určená jedným zo štyroch stupňov (stupeň 1- najnižší, stupeň 4- najvyšší). Klasifikácia zabezpečenia musí byť definovaná individuálne pre každé miesto prístupu a ich vstup a výstup. V celej inštalácií SKV je možné pre rôzne prístupové miesta použiť rôzne stupne, v prípade ak SKV a overovacie prostriedky spĺňajú aspoň požiadavky najvyššej bezpečnostnej klasifikácie prístupových miest kontrolovaných týmto systémom. [5]

Úroveň rizika je stanovená:

- na základe chráneného majetku,
- odhodlaním (znalosti a schopnosti),
- spôsobu útoku. [5]

Tab. 1 Stupne klasifikácie rizika [5]

Stupeň	1	2	3	4
Úroveň rizika	Nízke	Nízke a stredné	Stredné až vysoké	Vysoké
Aplikácie	Organizačné prostriedky, ochrana majetku nízke hodnoty	Organizační prostriedky, ochrana majetku nízke a stredné hodnoty	Menej organizačných prostriedkov, ochrana komerčných prostriedkov stredné až vysoké hodnoty	Hlavne ochrana komerčných prostriedkov veľmi vysoké hodnoty alebo kritické infraštruktúry.
Zručnosti/ znalosti páchateľa	Malá zručnosť, malá znalosť systému kontroly vstupu, identifikačných prostriedkov a IT technológií, malé finančné prostriedky pre napadnutie	Stredná zručnosť a znalosť systému kontroly vstupu, identifikačných prostriedkov a IT technológií, malé až stredné finančné prostriedky pre napadnutie	Veľká zručnosť, malá znalosť systému kontroly vstupu, identifikačných prostriedkov a IT technológií, stredné finančné prostriedky pre napadnutie	Veľmi vysoká zručnosť a znalosť systému kontroly vstupu, identifikačných prostriedkov a IT technológií, veľké finančné prostriedky pre napadnutie
Typické príklady	Hotel	Obchodní kancelárie, malé firmy	Priemysel, administratívne priestory, finančné inštitúcie	Vysoko citlivé priestory (vojenské zariadenia, vládne budovy, výskum a vývoj, kritická infraštruktúra)

1.2.2 Komunikácia

Komunikácia zabezpečuje prenos signálu medzi SKV pre zaistenie aplikácie na základe prednastavených pravidiel a závisí na rozsahu topológií sieti. [5]

Komunikačné kanály medzi SKV a ovládacím panelom musia spĺňať nasledujúce požiadavky:

- Výpadok a/alebo vypadnutie komunikačného kanálu v úrovniach 2,3,4 nesmú uvoľniť portál.
- Overenie komunikácie (časovanie) musí byť súčasťou finálnej inštalácie a musí spĺňať požiadavky z tabuľky v prílohe P1 v 38 riadku.
- Zariadenie stupňa 2,3,4 musia umožňovať autonómny chod po prerušení komunikácie.
- Zariadenia stupňa 4 musia generovať integritu komunikácie medzi všetkými komponentami ECAS alebo prijímaných dát vzťahujúcich sa na poskytnutie prístupu.
- Integrita komunikácie musí byť dosiahnutá dohľadom nad komunikačným kanálom a bezpečnosti prenášaných signálov.
- Bezpečnosť informácií musí byť zabezpečená prostriedkami zamedzujúcimi neoprávnenému čítaniu a modifikácií prenášanej informácie.
- V priebehu skúšky zariadení musí byť poskytnutý popis, ako boli dosiahnuté opatrenia pre bezpečnosť informácii. [5]

Konfigurácia- je funkcia zameraná na softwarové vybavenie záleží na zákazníkov a jeho potrebách. Konfigurácie prebieha v dvoch bodoch:

- programovanie.
- a určovanie predvolených nastavení. [5]

1.2.3 Rozhranie miesta prístupu

Hlavnými funkciami rozhrania miest prístupu je:

- **Aktivácia miesta prístupu**- uvoľnenie alebo zabezpečenie miesta prístupu podľa prednastavených pravidiel.
- **Monitorovanie miesta prístupu-** trvalé hlásenie stavu portálu.
- **Prekonanie aktivácie miesta prístupu-** uvoľnenie/zabezpečenie podľa prednastavených pravidiel bez identifikácie. [5]

Nezanedbateľnými požiadavkami pre rozhranie miesta prístupu sú:

- **Časové uvoľnenie portálu**- RJ musí byť schopná odblokovania portálu v súlade s prednastavenými pravidlami na určitú dobu definovanú systémom alebo požiadavkami na rozhranie miesta prístupu uvedenými v tabuľke v prílohe P1. Ak je stav miesta prístupu monitorovaný, tak musí uvoľnenie aktivátora miesta prístupu prestať pôsobiť pri dobe otvorenia prístupového miesta.

- **Kontrola prístupu**- EACS musí umožňovať kontrolu vstupu v súlade s tabuľkou v prílohe P2. Požiadavky tejto tabuľky musia byť aplikované na jednotlivé miesta prístupu v súlade s ich stupňom. EACS by mali obsahovať výstupy umožňujúce ovládať: elektromagnetické zámky, elektromagnetické strelky, aktivátor umiestnený v zárubniach, elektrické závory, hydraulické závory, pneumatické závory a ďalšie elektrické zámkové systémy a tiesňové lišty.
- **Stav portálu**- je rozdelený do štyroch základných stupňov na základe jednotlivých požiadaviek na rozhranie miesta prístupu, ktoré je možné nájsť v prílohe P2. [5]

1.2.4 Identifikácia

Identifikácia je proces, kedy sa systém snaží určiť totožnosť subjektu. Informácia je uložená v systéme a porovnáva sa so všetkými uloženými vzorkami (šablónami). Tento princíp sa nazýva one-to-many. [2]

Verifikácia

Verifikácia je proces pri ktorom sa systém snaží potvrdiť totožnosť subjektu, ktorý sa preukazuje porovnávaním použitého identifikačného prvku s predom uloženou informáciou uloženej v databáze. Jedná sa o princíp one-to-one. [2]

Autentizácia

Je pojem, ktorý je spájaný s termínom rozpoznávanie. Výsledkom tohoto procesu získa subjekt určitý status oprávnenie/neoprávnenie. [2]

Subjekt je možný identifikovať spravidla tromi spôsobmi:

- niečím, čo subjekt pozná alebo si pamätá (heslo, kód, kontrolná otázka atď.),
- niečím, čo subjekt fyzicky pri sebe (ID karta, prívesok, RF ovládač atď.),
- sám sebou, svojimi typickými rysmi alebo chovaním (biometria). [2]

Identifikačné prvky

Manuálne- pasívne prvky, ktoré vyžadujú manuálny vstup od človeka napr. vypínače, kódové zámky. [2]

Čipové- sú také prvky, pri ktorých je identifikátor uložený v integrovanom obvode. Tieto obvody je možné čítať aj zapisovať.

- Kontaktné- kontaktné čipové karty (SmartCard), iButton čipy.
- Bezkontaktné- bezkontaktné čipové karty/ prívesky, RFID (Radio Frequency Identification).
- Kombinované- kombinácia kontaktných a bezkontaktných prvkov v jednej karte, prívesku alebo kľúči. [2]

Magnetické- karty, ktoré obsahujú magnetické prúžky, ktoré sa identifikujú pretiahnutím cez čítačku. [2]

Optické- sú prvky, ktoré obsahujú časový kód, dáta matrix (2D) alebo kruhový kód. Pre čítanie týchto prvkov sú využívané Laserové alebo CCD čítačky. [2]

Rádiofrekvenčné- patria sem napr. bluetooth identifikácie, ktoré využívajú bezlicenčné pásma 434/868 Mhz/2,4Ghz. [2]

Biometrické- sú také prvky, ktoré využívajú individuálne fyzické charakteristiky človeka napr. papilárne línie, očná dúhovka, 3D model hlavy, DNA a pod. [2]

Obr. 4 RFID prívesok a čipová karta [6,7]

Snímacie zariadenia

Snímacie zariadenia je možné rozdeliť poľa identifikačného média alebo z hľadiska vykonávaných funkcií:

- **Základné/neinteligentné-** zaisťujú iba zadaný kód alebo prečítané čísla identifikátoru a následne poskytujú tieto informácie riadiacej jednotke. Najčastejším používaným

rozhraním je Wiegand. Rozhrania Magstripe, 1-wire, RS-485 sú požívané veľmi zriedka. Tento druh čítačiek je najvyužívanejší v rozsiahlejších systémoch.

- **Polointeligentné**- obsahujú všetky potrebné vstupy a výstupy pre ovládanie miesta prístupu, ale neprevádzajú rozhodnutie o prístupe. Informácia je zaslaná do riadiacej jednotky, ktorá ja najčastejšie prepojená zbernicou RS-485.
- **Inteligentné**- obsahujú všetky potrebné vstupy a výstupy pre ovládanie miesta prístupu. Obohatená je pamäť prístupových údajov a rozhodovanie o prístupe. Najčastejším prepojením s RJ je využívaná RS-485. RJ má v tomto prípade na starosti aktualizáciu a príjem transakcií od čítačiek. Trendom sú IP-čítačky , ktoré sú prepojené cez eternetové siete so serverom a synchronizačnými databázami. [2]

Obr. 5 Autonómne čítačky [8,9]

Požiadavky na rozpoznávanie

Kontrola prístupu je aplikáciou viazaná k osobe, ktorá prideľuje prístupové práva jednotlivým užívateľom alebo skupinám užívateľov. Primárnou funkciou ECAS je identifikácia užívateľov, preto je nutná voľba oprávnených prostriedkov užívateľov s súlade s požadovanými stupňami (úrovni zabezpečenia).

- ECAS musia spĺňať funkcie rozpoznávania v súlade s tabuľkou Požiadavky na rozpoznávaní, ktorá je uvedená v prílohe P3.
- ECAS musia porovnávať zapamätanú informáciu s uloženými overovacími údajmi pre prijatie alebo zamietnutie požiadavky.
- RJ musí obsahovať hodiny reálneho času s presnosťou +/- 10 s za týždeň a nastavenie letného času, priestupného roku, časového pásma odpovedajúcim tabuľke v prílohe P3.

- RJ musia obsahovať pre stupne 2, 3 a 4 jedinečnú identitu pre každého oprávneného používateľa.
- RJ musí obsahovať minimálny počet úrovní prístupu ako je uvedené v prílohe P3.
- RJ musí poskytovať časové programovateľné úseky uvedené v prílohe P3.
- Rozlíšenie času musí obsahovať deň v týždni, hodinu a minútu. Stupne 3 a 4 musia obsahovať aj deň v mesiaci a rok.
- RJ musí obsahovať programovateľné sviatky podľa tabuľky v prílohe P3. [5]

1.2.5 Oznámenie

Funkciu oznámenie je možné rozdeliť na 3 základné časti:

- **Zobrazenie-** súvisí s vizuálnou alebo akustickou zmenou v systéme. SKV musia ovládacím panelom umožňovať monitorovacie a zobrazovacie udalosti a informácie
- **Výstraha-** nadviaže na aktiváciu indikátoru a pošle výzvu posúdenia obsluhe. SKV musia umožňovať aktiváciu indikátorov na ovládanie panelu k upozorneniu operátora na posúdenie udalosti v súlade s tabuľkou požiadaviek na indikáciu.
- **Záznam udalosti-** súvisí so záznamom vybavením zmien, ku ktorým v systému došlo. SKV musí zaznamenávať udalosti a informácie v súlade s tabuľkou požiadaviek na indikáciu. Prístup k zaznamenaným dátam musí byť obmedzený prístupovými právami. [5]

1.2.6 Signalizácia nátlaku

Signalizácia nátlaku je v podstate tiché varovanie užívateľa systému o stave vynucovanom v požiadavkách prístupu. Pre signalizáciu sa využíva tzv. nátlakové iniciačné zariadenie, ktorého prenos informácie nástrahy musí byť v súlade s tabuľkou „Požiadavky na signalizáciu nátlaku“ uvedenej v prílohe P4 a nasledujúcimi požiadavkami:

- Signál nátlaku prijatý na ovládacom panely musí obsahovať identifikáciu umiestnenia, čas a dáta nesúce informáciu,, kedy k nátlaku došlo.
- Signál nátlaku prijatý na ovládacom panely musí obsahovať informáciu o identifikácií užívateľa. [5]

1.2.7 Rozhranie pre spojenie s ostatnými systémami

SKV nemusia byť aplikované samostatne, ale aj s inými systémami. Systémy si navzájom môžu zdieľať zmeny s ostatnými systémami a tým vytvoriť variabilnejší a účelnejší systém.

Z tohto dôvodu je kladený dôraz na rozhranie, ktoré svojimi možnosťami uľahčuje a skvalitňuje správu systému. [5]

1.2.8 Vlastná ochrana systému

Slúži ako prevencia. Princípom je detekcia úmyselného zásahu do systému. Komponenty SKV musia pre jednotlivé stupne spĺňať požiadavky uvedené v prílohe P5, Požiadavky na vlastnú ochranu systému.. [5]

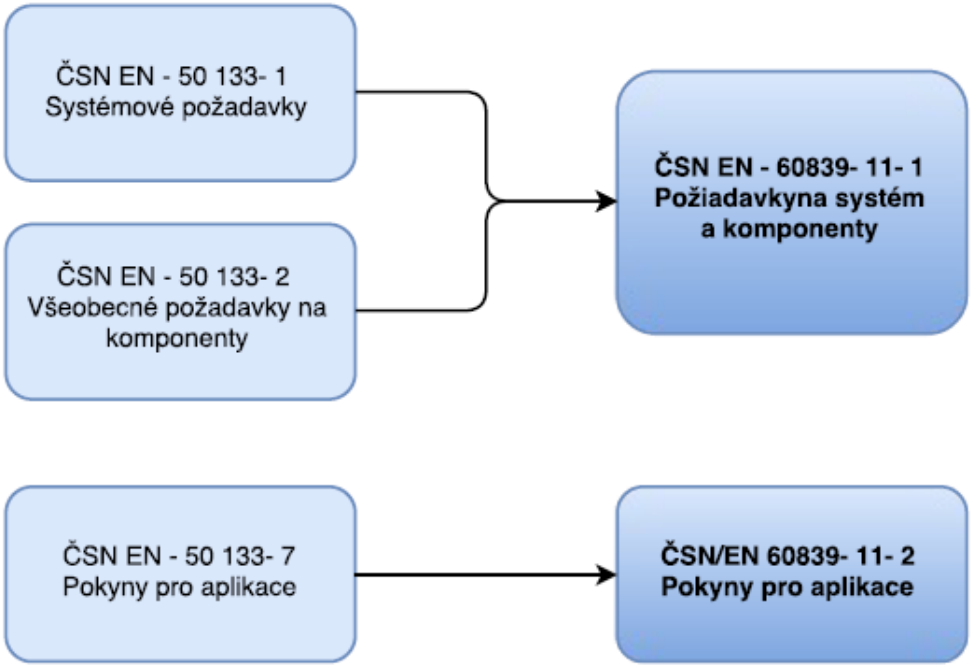
1.2.9 Napájací zdroj

Požiadavky na napájanie musia spĺňať normu IEC 626426-6. RJ a komponenty SKV môžu byť napájané buď vstavaným, alebo externým zdrojom, ktorý musí splniť požiadavky uvedené v prílohe P6 Požiadavky na napájanie. [5]

1.3 Legislatíva

Z hľadiska požiadaviek na SKV je nevyhnutné spomenúť výraznú zmenu v rámci štandardizácie:.

- Vydanie novej technickej normy (január 2014) ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy časť 11-1 Elektronické systémy kontroly vstupu – Požiadavky na systém a komponenty. Táto norma úplne nahradila normy ČSN EN 50133-1 a ČSN EN 50133-2.
- Vydanie novej technickej normy (apríl 2015) ČSN EN 60839-11-2 Poplachové a elektronické bezpečnostní systémy časť 11-2 Elektronické systémy kontroly vstupu – Pokyny pro aplikácie. Táto norma čoskoro úplne nahradí normu ČSN EN 50133-7, ktorá má platnosť do konca roku 2018. [1]



Obr. 6 Prehľad aktualizácie noriem

1.3.1 Štruktúra platných noriem

Tab. 2 Technické normy platné pre SKV

Číslo technickej normy	Názov technickej normy
ČSN EN 60839-11-1	Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty
ČSN EN 60839-11-2	Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace
ČSN EN 50133-7	Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace
ČSN EN 50130-4 ED.2	Poplachové systémy - Část 4: Elektromagnetická kompatibilita - Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci
ČSN EN 50130-5 ED.2	Poplachové systémy - Část 5: Metody zkoušek vlivu prostředí
ČSN CLC/TS 50131	Poplachové systémy - Elektrické zabezpečovací systémy - Část 7: Pokyny pro aplikace

Vzhľadom na zameranie práce sú v práci primárne využité poznatky z technických noriem : ČSN EN 60839-11-1 a ČSN EN 60839-11-2.

ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy časť 11-1 Elektronické systémy kontroly vstupu – Požiadavky na systém a komponenty.

Norma ČSN EN 60839-11-1 rieši nové štandardy pre SKV v nasledujúcich oblastiach:

- terminológia,
- architektúra systému,
- stupne klasifikácie,
- požiadavky na funkčnosť systému,
- požiadavky na odolnosť proti vplyvom prostredia,
- spôsoby skúšok. [5]

Oproti pôvodnej technickej norme došlo ku zmene v nasledujúcich bodoch:

- nové stanovenie klasifikácie zabezpečenia,
- zvýšil sa rozsah a podrobnosť spracovania funkčných požiadaviek,
- zvýšila sa miera vlastností funkčných požiadaviek pre jednotlivé aplikácie SKV,
- rozšírená terminológia. [5]

ČSN EN 60839-11-2 Poplachové a elektronické bezpečnostní systémy časť 11-2 Elektronické systémy kontroly vstupu – Pokyny pro aplikácie.

Norma ČSN EN 60839-11-2 rieši nové štandardy pre SKV v nasledujúcich oblastiach:

- terminológie,
- požiadavky na odolnosť proti vplyvom prostredia EMC,
- plánovanie systému a analýz rizika,
- montáž systému,
- uvedenie do chodu a predania,
- údržba,
- dokumentácia. [11]

Požiadavky na prvky systémov kontroly vstupu

Nevyhnutnou podmienkou všetkých prvkov SKV je spĺňať požiadavky:

- Na Elektrickú bezpečnosť ČSN EN 60950, ČSN EN 60065.
- Na Elektromagnetickú kompatibilitu a odolnosť ČSN EN 61000, ČSN EN 55022, ČSN EN 50082, ČNS EN 50130.
- Na telekomunikácie ČSN EN 50529 .
- Na kombinované a integrované systémy ČSN CLC/TS 50398 (v prípade integrácií s inými systémami). [11]

1.4 Rozsah a topológia

Podľa veľkosti a topológie je možné systémy SKV rozdeliť na autonómne a modulárne systémy.

Autonómny systém

Autonómny systém je tvorený maximálne dvoma snímacími zariadeniami, u ktorých je RJ integrovaná, alebo je oddelená ako samostatný modul. Prístupové práva sú programované prostredníctvom špecifického postupu (master kód/karta, špeciálny HW mód, prepojenie s PC) a uložené priamo v RJ. Autonómne systémy sú vhodné pre systémy, kde nie je vysoký počet miest prístupu a zároveň nie je vysoká početnosť pohybu osôb. [1]

Modulárny systém

Modulárny systém je vhodný pre rozsiahlejšie koncepcie, ktoré sú tvorené miestami prístupu, RJ a riadiacim počítačom (Personal Computer, ďalej PC). Najčastejšie je využívaná zbernicová alebo hviezdicová topológia s centrálnym prvkom, ústredňou (hlavná RJ alebo PC). V zbernicovej konfigurácií sú všetky miesta prístupu prepojene zbernicou (najčastejšie RS-485) s ústrednou SKV alebo cez prevodník s PC. Hviezdicová topológia prepája miesta prístupu cez eternet. Z hľadiska usporiadania prvkov SKV je možné topológie, rozdeliť na:

- **Zbernicové prepojenie riadiacej jednotky-** všetky RJP (riadiace jednotky prístupu) sú prepojené s hlavnou riadiacou jednotkou (HRJ), buď prostredníctvom RS-485 alebo prostredníctvom prevodníku RS-485/USB RS-232. Sú prepojené s PC. Výhodou tejto konfigurácie je spoľahlivosť RS-485 a pomerne veľká dosiahnutá vzdialenosť (1200m). Medzi nevýhody patrí obmedzenie rýchlosti komunikácie a odozvy, problémy s impedančným zákonom zbernice a obmedzenie na max 32 kontrolérov.

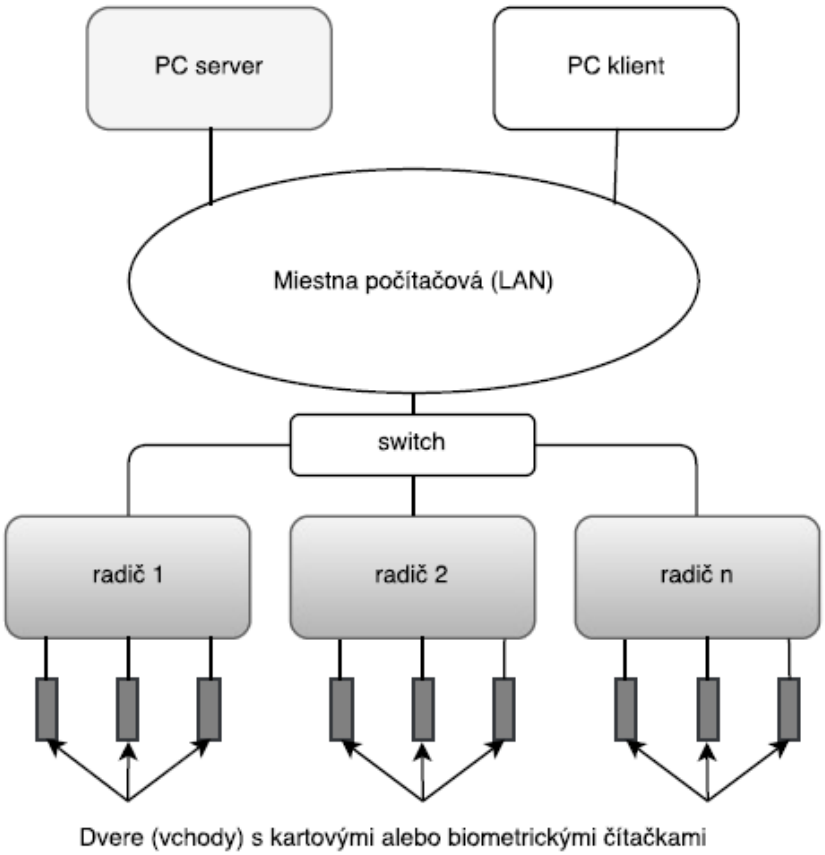
- **Zbernicové prepojenie inteligentnej čítačky-** polointeligentné alebo inteligentné (bez potreby RJP) čítačky sú priamo prepojené zbernicou s HRJ. Rozhodovacia funkcia sa nachádza buď v HRJ alebo v PC. V systému je možné zosieťovať aj viacero HRJ, ale musí byť použitá iná zbernica. Medzi výhody je možné zaradiť jednoduchosť kabeláže a naopak medzi nevýhody patrí obmedzené portfólio inteligentných. čítačiek.
- **Zbernicové prepojenie systému s prevodníkmi LAN-** topológie s využitím zbernice RS-485, môžu byť obohatené o prevodníky RS485/LAN. Využitie prevodníka umožní distribúciu signálu po stávajúcej eternetovej sieti. Na PC je obvykle nainštalovaný „virtuálny sériový port“, ktorý umožní prepojenie s HRJ (pomocou RS-232 alebo prevodníka RS-485). Výhodou tohto prepojenia je variabilita a využite existujúcej siete. Nevýhody zostávajú komunikačná rýchlosť RS-485 a nestabilita pri väčšom množstve prvkov.
- **IP riadiace jednotky (kontroléry)-** kontroléry sú s PC prepojené prostredníctvom LAN alebo WAN siete. Obvykle sa využije existujúca sieť. Tým pádom odpadá obmedzenie rýchlosti a počtu prvkov z RS-485. Kontrolér dokáže inicializovať udalosti, čím zbytočne nezahlcuje sieť v kľudovom režime. Touto cestou sa otvárajú široké možnosti na budovanie siete s využitím optiky, WiFi, PoE (Power over Ethernet) apod. Toto riešenie je vhodné pre riešení rozsiahlych systémov s veľkým počtom užívateľov, kde je potrebný prenos veľkých počtov dát veľkou rýchlosťou (môžu sa prenášať aj biometrické záznamy). Pri tejto konfigurácii sa otvára aj ďalšia nevýhoda a to napadnutie siete LAN z vonku.
- **IP čítačky-** inteligentné čítačky sú vybavené eternetovým rozhraním a sú väčšinou prepojené prostredníctvom LAN alebo WAN k radiacemu PC. Väčšina IP čítačiek umožňuje možnosť napájania PoE, čo zjednodušuje inštaláciu. Pri využití IP čítačiek je výhodou jednoduché rozšírenie systému, keď porucha jednej čítačky neovplyvní zvyšok systému. Na druhej strane sa jedná o integráciu čítačky a kontroléru, ktorá sa nachádza na mieste prístupu, kde je jednoduchšie napadnutie kabeláži. [1]

1.5 Architektúra siete

Na Obr. č. 7 je zobrazená typická schéma praktického hardwarového zapojenia SKV. V architektúre SKV sú definované 3 existujúce úrovne:

- **Prvá úroveň**- je úroveň, na ktorej sú čítačky prepojené komunikačným rozhraním. Najčastejšie je využívane trojdrôtové rozhranie Wiegand, s ktorým sú čítačky spojené s radičmi. Ak majú čítačky rozhranie RS 232 alebo USB, je nutná konverzia na Wiegand.
- **Druhá úroveň**- je úroveň, na ktorej prebieha zlúčenie dát z čítačiek. Pri väčšom rozsiahlejšom systéme s vysokým počtom čítačiek je úroveň rozdelená na úroveň hlavných a vedľajších radičov. Jednotlivé radiče sú k vyššej úrovni pripojené najčastejšie prostredníctvom zbernice RS 485 (dvojdrôtová verzia zbernici, ktorá funguje na princípe master/slave). Táto zbernica je prevedená pomocou STP káblu so štyrmi vodičmi, kde signál A, B predstavuje vlastný krútený pár. Vcc a Gnd sú využívane ako rozvod jednosmerného napájania medzi jednotlivými radičmi.
- **Tretia úroveň**- je úroveň, ktorá slúži k zlúčeniu a prepojeniu dát z jednotlivých radičov do vlastnej PC siete. Táto úroveň môže byť riešená dvomi spôsobmi :
    - pri návrhu SKV sa vyberajú radiče, ktoré obsahujú eternetový výstup a následne sú zlúčené pomocou switcha.
    - v prípade že radiče neposkytujú eternetový výstup, ale len RS 485, je nutná konverzia na eternetový výstup prostredníctvom hardwarového prevodníku (nazývaný aj terminálový server).

V moderných budovách začínajú radiče nahrádzať IP čítačky (čítačky s eternetovým rozhraním). Výhodou tohto riešenia je väčšia dátová priepustnosť, čo sa prejaví využitím pokročilejších identifikačných zaradení napr. 3D rozpoznávanie tváre, rozpoznávanie dúhovky či žilného riečiska. Nevýhodou je samozrejme výrazne vyššia cena.



Obr. 7 Schema najčastejšieho hardwaroého zapojenia SKV

Vyhodnotenie prístupu môže byť prevádzané :

- v serveri- plne centralizované riešenie,
- v radiči,
- v čítačke- plne decentralizované riešenie. [1]

Obľúbenou, v praxi najviac využívanou, je druhá alternatíva s vyhodnotením prístupu priamo v radiči. Plne centralizovaná alternatíva sa v praxi nepoužíva z dôvodu, že v prípade výpadku servera by bol odopretý prístup do všetkých strážených priestorov. Vyhodnocovanie v čítačke je najnovšou alternatívou, jej výhoda spočíva priamo v decentralizácií. V tomto prípade tiež prúdia dáta do serveru, ale len za účelom evidencie a dochádzky. Pri výpadku spojenia so serverom sa dáta aktualizujú až pri opätovnom spojení. V najnovších inštaláciách sa pomaly popularizuje práve táto alternatíva. Avšak oblasť fyzického prístupu je stále kontroverznou možnosťou, práve preto je alternatíva s vyhodnocovaním v radiči stále najpoužívanejšou. [1]

1.6 Integrácia s inými systémami

SKV môžu byť aplikované samostatne alebo v komunikácií s inými poplachovými systémami, čím tvoria spoločne jednu bezpečnostnú aplikáciu. Dnes sú využívané tieto typy kombinácie:

- **Dochádzkové systémy-** v systéme sú použité dochádzkové a prístupové systémy.
- **Stravovacie systémy-** sú v podstate samostatné systémy, ktoré využívajú rovnaké identifikačné média ako SKV.
- **Poplachový zabezpečovací a tiesňový systém (PZTS)-** sofistikovanejší zbernicový systém PZTS podporuje základné funkcie SKV. Hlavnou výhodou je možnosť ovládať systém PZTS prostredníctvom prístupových identifikátorov, monitorovať stav PZTS za dverami.
- **Elektronická požiarna signalizácia EPS-** je vždy samostatný, ale pri spustení evakuácie alebo detekcii požiaru je nutné zaistiť správnu funkciu všetkých prístupových bodov, uvoľniť priechodnosť všetkých únikový ciest a zablokovať šírenie požiaru. EPS poskytuje tieto signály prostredníctvom relé.
- **Kamerový systém (CCTV)-** pri prepojení s SKV môže pri časovej synchronizácií poskytnúť doplnkové obrazové informácie ku každej prístupovej udalosti na daných prístupových bodoch.
- **IT systém-** pri použití samostatných čítačiek ako identifikačných médií, prepojením s PC, je možné riadiť prístup k PC, sieti atď.
- **Meranie a regulácia-** prítomnosť fyzickej osoby, môže obohatiť funkcionalitu SKV a radu funkcií ako napr. osvetlenie vytápanie a pod. [2]

1.7 Čiastkový záver

Systémy kontroly vstupu sú variabilné a môžu byť zložené z rôznych prvkov. Hlavným účelom týchto systémov je identifikácia, ktoré je overovaná na základe identifikačných prvkov. Zloženie systému kontroly vstupu je odvodené z funkčných vlastností a požiadaviek, ktoré sú zhrnuté v podstate nových technických normách ČSN EN 60839-11-1 a ČSN EN 60839-11-2. V kapitole boli opísané rôzne možnosti typológie týchto systémov a bol vypracovaný prehľad právneho rámcu požitia daného systému a jeho integrácia. Kapitola uvádza, že systémy kontroly vstupu je možné integrovať s inými poplachovými a nepoplachovými aplikáciami (PZTS,EPS,VDS atď.).

Výrobná spoločnosť disponuje s hardwarom, ktorý na identifikáciu využíva RFID technológiu a je riadená softwarom Aktion 5.1. Tento software riadi a zabezpečuje dochádzku danej spoločnosti prostredníctvom evidencie prechodov osoba a vozidiel v objekte. SKV danej spoločnosti je možné hardwarovo aj softwarovo integrovať.

Typy kombinovaných štruktúr a integrovaných poplachových systémov sú uvedené v norme ČSN EN CLC/TS 50398, ktorá je podrobnejšie rozobratá v 3. kapitole teoretickej časti práce.

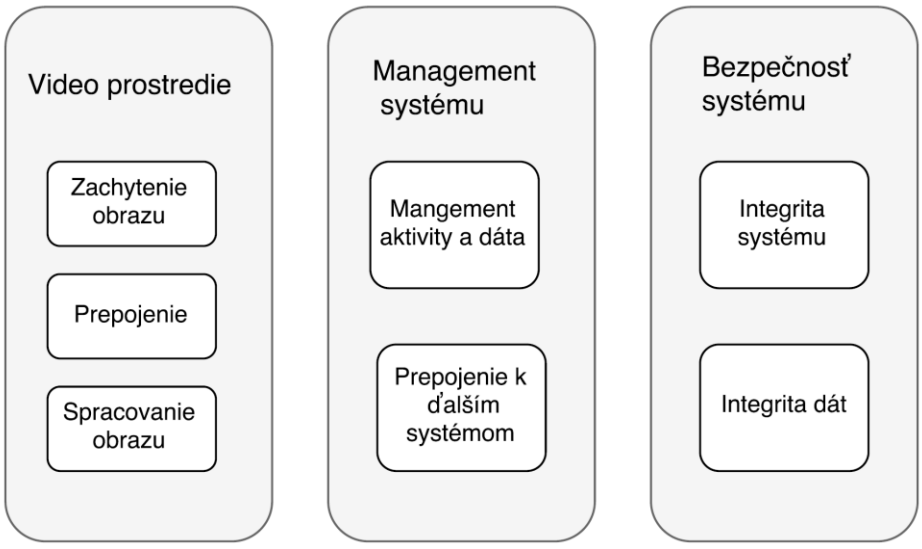
2 VIDEODOHĽADOVÉ SYSTÉMY

Videodohľadové systémy (VDS) sú všeobecne nazývané aj kamerové systémy. Dohľadové systémy alebo CCTV („Closed Circuid Televizion“, čo v preklade znamená uzavretý televízny okruh). Táto práca bude využívať pojem dohľadové videosystémy, ktorý vychádza z technickej normy ČSN EN 62676-1-1 (Dohledové videosystémy pro použití v bezpečnostních aplikacích část 1-1 Systémové požadavky – Obecně). V tejto norme má dohľadový videosystém skratku VSS (z anglického video surveillance system) a je definovaný ako „ *systém skládající se z kamerového vybavení, úložiště, monitorovacího zařízení a souvisejících zařízení pro účely přenosu obrazu a ovládaní“.* [2,12]

VDS primárne slúžia na identifikáciu, rekognoskáciu, detekciu osôb či monitorovanie skupiny osôb. Súčasné inteligentné VDS umožňujú oveľa širšie možnosti využitia v oblasti priemyslu komerčnej bezpečnosti. Môžu detekovať podozrivé/neprimerané správanie osôb v objekte (smer pohybu, rýchla chôdza, sledovanie teploty osôb, rozpoznávanie predmetov identifikácia evidenčných čísle vozidiel atď.). [12]

2.1 Funkčné vlastnosti

VDS do svojej štruktúry zahŕňa aj analógové a digitálne zariadenia. Medzi dôležité súčasti patrí aj softwarové vybavenie, a to z dôvodu rýchlej evolúcie technológií a VDS zariadení. Norma ČSN EN 62676-1-1 definuje a popisuje VDS ako časti a spoločné vzťahy medzi nimi pričom ich rozdeľuje do troch funkčných blokov. Tieto bloky sú zobrazené na Obr. č. 8 a zobrazujú jednotlivé funkcie VDS pre bezpečnostné aplikácie.



Obr. 8 Funkcie VDS [12]

2.1.1 Video prostredie

2.1.1.1 Zachytenie obrazu

Bezpečnostné kamery je možné rozdeliť podľa spracovania obrazu na analógové bezpečnostné kamery a IP bezpečnostné kamery. Vzhľadom na technické parametre digitálnych kamier je aplikácia analógových kamier na ústupe. Avšak v praxi je stále možné stretnúť čisto analógovou alebo hybridnou kombináciou, ktorá obsahuje oba typy bez. kamier. [13]

Analógové kamery

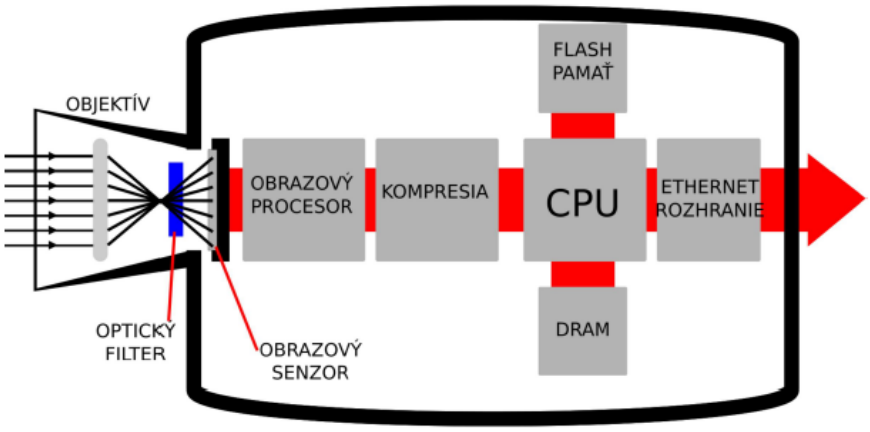
Analógové bezpečnostné kamery zachytávajú analógový signál, ktorý je prenášaný nesymetrickým vedením v podobe koaxiálneho káblu do DVR (digitálny videorekordér). Jednou z podmienok analógových bez. kamier je samostatné napájanie každej kamery. Príklad analógovej kamery je možné vidieť na Obr. 9. [13]

Obr. 9 Analógová kamera[14]

Digitálne IP kamery

Digitálne IP kamerové systémy zachytávajú analógový obraz, ale na rozdiel od analógových bezpečnostných systémov IP kamera tento signál rovno prevádza na digitálny. Tento digitálny signál je prenášaný cez miestnu sieť LAN s použitím UTP, STP alebo FTP káblov. Pri IP kamerách je väčšinou využitý ten istý kábel na napájanie aj prenos dát, tento spôsob je

nazývaný PoE. Tieto kamery sú pripájané do sieťového videorekordéru (NVR), ktorý môže využívať funkciu zdroja elektrickej energie pre PoE. Na blokovej schéme IP kamery Obr. 10 je možné vidieť základné zložky z ktorých sa kamera skladá. Obraz je snímaný cez objektív, kde pomocou clony redukuje množstvo prechádzajúceho svetla a pomocou šošovky zaostruje snímaný obraz. Pred tým ako sa obraz dostane na obrazový senzor prechádza cez optický filter, ktorý odstraňuje svetlo a zabezpečuje kvalitu obrazu. Obrazový senzor prevádza elektromagnetické vlny na elektrický signál. Najčastejšie využívané sú CCD (Charged Coupled Device) a CMOS (Complementary Metal Oxide Semiconductor). Obrazový procesor snímaný obraz prevádza do digitálnej formy a následne v spolupráci s kompresným čipom vykonáva kompresiu. Od obrazového procesoru závisí aj schopnosť kamery prenášať obraz. RJ CPU synchronizuje celý proces spracovania obrazu. Flash pamäť uchováva software kamery. DRAM pamäť slúži na dočesané ukladanie obrazu pred odoslaním prostredníctvom eternetového rozhrania do siete. [13]



Obr. 10 Schema IP kamery [15]

IP kamery sa pohybujú na svetovom trhu už okolo 15 rokov a od ich počiatku prešli značným vývojom. Dnes je dostupné veľké množstvo IP kamier, ktoré sa líšia najmä konštrukčným prevedením. Modely IP kamier je dnes možné rozdeliť do týchto skupín:

- Fixné kamery
  - Fixné IP dome kamery
- PTZ IP kamery
  - Mechanické IP PTZ kamery
  - Nemechanické IP PTZ kamery
  - IP PTZ dome kamery [15]

2.1.1.2 Prepojenie

Pri monitorovaní objektu VDS je značným aspektom vzdialenosť kamery a zariadenia pre spracovanie videosignálu s monitorom. Pre prenos videosignálu sú k dispozícií rôzne varianty riešenia(od bezdrôtových až po optické vlákna). Druh prenosu závisí od počtu kamier, vzdialenosti jednotlivých komponentov videosystému, ekonomického porovnávania náročnosti jednotlivých variant, druh a vplyv prostredia do ktorého je systém určený. [16]

Možnosti prepojenia VDS:

- prenos po koaxiálnom kábli,
- prenos po symetrickom vedení(UTP),
- prenos po optických vláknach,
- bezdrôtový prenos. [16]

Komunikačná časť IP kamier

IP kamera má svoju vlastnú IP adresu a vstavané funkcie, ktoré sa starajú o sieťovú komunikáciu. Jednotka kamery obsahuje zabudované všetko, čo potrebuje na sieťovú komunikáciu, vrátane vstavaného softwaru pre web server, FTP server, FTPS klienta a emailového klienta. Ďalej je opatrená jedným alebo viacerými logickými vstupmi (alarm input) a výstupmi (realy output). Riadiaci procesor spolu s FLASH pamäťou a DRAM sa starajú o inteligentné analýzy obrazu, ovládanie I/O či komunikáciu so sieťou webovým serverom. Hardwarové riešenie záleží na výrobcovi, čiže je individuálne a záleží na modeli kamery. Schopnosť fungovania v eternetovej sieti robí z IP kamier progresívny prvok sieťového videa, keď nepotrebuje ďalšie periférià. Pre komunikáciu jej stačí PC alebo DVR, ktoré je vybavené VMS softwarom. [15]

Komunikačná časť IP kamier je tvorená základnými kategóriami:

- hardwarové komunikačné rozhranie IP kamery,
- prenosové technológie sieťového videa,
- Komunikácie s IP kamerami v sieti. [15]

Hardwarové komunikačné rozhranie IP kamier

Rôzne modely IP kamier, môžu využívať rôzny počet a rôzne typy konektorov na prenos videa. V praxi sú na prenos videa používané tieto typy konektorov:

- koaxiálny kábel,

- UTP kábel,
- dvojica antén na bezdrôtový prenos. [15]

IP kamery bývajú vybavené logickými I/O, audio výstupom pre pripojenie externého mikrofónu a konektorom pre napájanie. Funkcie spomenutých konektorov môžu byť realizované prostredníctvom jedného UTB káblu, pomocou PoE alebo u vonkajších PTZ HiPoE(zvýšený výkon na spotrebu). [15]

Logické vstupy (I/O) sú využívané na prenos logickej informácie z externých zariadení(najčastejšie PZTS alebo SKV). Informácia je spracovaná procesorom kamery a na základe nastavení IP kamera vykonáva autonómne činnosti (zmena polohy, spustenie nahrávania). [15]

Logické výstupy (I/O) sú naopak využívané na odoslanie informácií externým zariadeniam, ktoré vykonávajú samostatnú činnosť (napr. využitie elektrických brán alebo blokovacích zámkov). [15]

Prenosové technológie sieťového videa

Uvedená časť je zameraná na jednotlivé možnosti komunikácie prostredníctvom sieťového videa. [15]

IP (Internet protokol) a Ethernet

Dnes je najvyužívanejším počítačovým komunikačným protokolom IP. Je základný protokol používaný pre internet, e-mail a každú novo nainštalovanú sieť. Jednou z najväčších predností tohto protokolu je škálovanosť, ktorá umožňuje rozšírenie o ďalšie prvky. V dnešnej dome väčšina systémov firiem a domácností obsahuje LAN a WLAN ethernetovú sieť, ktorá funguje na protokole TCP/IP. Postupom času sa ethernetové siete stále vyvíjajú, čím sa zvyšuje aj prenosová rýchlosť dátovej siete. Pre prepojenie jednotlivých kamier sa spravidla využíva štandard 100BASE-T, ktorý umožňuje rýchlosť 100Mbit/s prostredníctvom krútenej dvojlinky. Na prepojenie viacerých kamier je využívaný sieťový prepínač (Network Switch), ktorý zároveň zabezpečuje kompatibilitu so starším štandardom 10BASE-T. Tieto prepínače môžu byť obohatené o technológiu Poe/ HoPoe a zabezpečiť tak napájanie kamier cez dátovú sieť. Smerom od prepínačov k ostatným prvkom siete narastajú nároky na prenosovú rýchlosť, čo často vyžaduje okrem spomínaného využitia UTP káblu tiež optické vlákna. Táto technológia je využívaná v rozsiahlejších systémoch, ktoré kladú dôraz na prenosovú rýchlosť a prenosovú vzdialenosť v praxi sú využívanie tieto štandardy:

- 100BASE-T (SX, LX,LH)- prenosová rýchlosť 1 Gbps

  Indexy SX, LX, LH poskytujú rovnakú prenosovú rýchlosť , ale líšia sa v prenosových vzdialenostiach:

  - od 100m – T,
  - cez 550 m SX,
  - do 100km- LH.

- IEEE 802.3ae: prenosová rýchlosť 10 Gbps

  Je štandard pre lokálne siete (LAN, Man, WAN) s prístupovou metódou CSMA/CD s rýchlosťou od 10 do 1000 MB/s. Špecifikujúcou je implementácia fyzickej vrstvy a MAC podvrstvy spojovej vrstvy. [15]

Bezdrôtové prenosové siete

Bezdrôtové prenosové siete sú najčastejšie využívané tam, kde je nutné sa vyhnúť priamemu zásahu do fyzickej štruktúry budov alebo je to voľba príslušného projektanta vzhľadom na jednoduchosť nadstavby. Bezdrôtové siete sa stále vyvíjajú a prinášajú čím ďalej vyššiu prenosovú rýchlosť, spoľahlivosť, priepustnosť a dosah pokrytia. V prípade použitia bezdrôtovej siete je spravidla využívaný (Wireless Access Point), ktorý je drôtovo prepojený cez prepínače a prostredníctvom bezdrôtového rozhrania s použitými bezdrôtovými prvkami. [15]

Sieť založená na TCP/IP využíva štandard IEE 802.11. Tento štandard sa stále vyvíja a v súčasnosti sú známe tieto verzie:

- IEEE 802.11a

  Využíva pásmo 5Ghz a poskytuje až 24 Mbps reálnej priepustnosti na 30 m vo vnútornom prostredí. Nevýhodou je to, že podporuje obmedzený počet produktov (teoretická priepustnosť je 54 Mbps).

- IIEEE 802.11b

  Využíva pásmo 4,4 Ghz a poskytuje 5 Mbps reálnej priepustnosti na vzdialenosť 100 m vo vonkajšom prostredí. Podporuje skoro všetky súčasné produkty (teoretická priepustnosť je 11 Mbps).

- IEEE 802.11g

  Využíva pásmo 2,4 Ghz a poskytuje 24 Mbps reálnu priepustnosť (Teoretická priepustnosť je 54 Mbps). [15]

Prenosové protokoly sieťového videa

Protokol TCP/IP

TCP/IP je najpoužívanejším protokolom, ktorý je využívaný pre širokú škálu aplikácií. Je základným komunikačným protokolom pre prenos sieťového videa. Prenáša dátové pakety cez prípadné medziľahlé uzly, na miesto určenia. IP časť protokolu zabezpečuje samostatné prúdenie dát, TCP riadi tok dát. Každá zložka IP VDS má svoju vlastni IP adresu, ktorá slúži na identifikáciu zariadenia v sieti. [17]

Protokol UDP

UDP nenavažuje priame spojenie medzi komunikujúcimi počítačmi ako TCP/IP. Jeho výhodu tvorí nepotrebnosť jedinečnej IP adresy k doručeniu dát. Čím umožňuje strémovať video viacej účastníkom sieťové prevozu naraz. [17]

Protokol RTSP ((Real Time Streaming Protocol))

RTSP slúži k streamovaniu audia a videa v reálnom čase. Tento protokol využíva takmer každý výrobca VDS. [17]

ONVIF (Open Network Video Interface Forum)

ONVIF predstavuje združenie výrobcov v oblasti VDS (dnes okolo 500 spoločností vzájomnou kompatibilitou). Združenie zjednocuje kompresiu, prenos audia a videa streamu, spracovanie udalostí, ovládanie zariadení a mnoho ďalších parametrov. Cieľom je zjednotiť platformy k zaisteniu kooperačných funkcií. [18]

2.1.1.3 Spracovanie obrazu

Medzi funkcie spracovania obrazu partií:

- analýza dát,
- uloženie,
- zobrazenie dát.

Analýza obrazu

Analýza obrazu je proces skúmania snímaného záznamu alebo obrazu. Jej cieľom je získať relevantné informácie o detekcií narušenia, identifikácií narušenia, poruchu kamery atď. Získavanie informácií môže byť uskutočnené prostredníctvom obsluhy alebo výpočtovej techniky. [19]

Najčastejšie video-analytické funkcie:

- detekcia pohybu,
- detekcia manipulácie s kamerou,
- rozpoznávanie reg. značiek,
- počítanie osôb,
- počítanie objektov, ktoré prekonajú virtuálnu priamku,
- detekcie vstupujúcich/opúšťajúcich oblasť,
- detekcia odstránenia objektu,
- detekcia prekročenia čiary. [19]

Analytické funkcie zachytávajú dáta o všetkých objektoch v stráženom priestore. Proces analýzy v pozadí zaznamenáva a automaticky generuje tzv. metadáta. Metadáta sú jednoduché textové reťazce, ktoré popisujú detaily v obraze, môžu obsahovať rôzne identifikačné informácie o osobách, objektoch a registračných značkách automobilov. Metadáta majú veľký význam pri rozpoznávaní, umožňujú stavanie podmienok pre rôzne akcie (poplach). [19]

Záznamové zariadenia

DVR (digitálny videorekordér) je nevyhnutnou súčasťou analógového systému. V systéme zabezpečuje tieto funkcie:

- transformáciu analógového signálu do digitálnej formy,
- komunikáciu systému,
- plánovanie nahrávania,
- detekciu pohybu,
- digitálny zoom
- zobrazenie na zobrazovacie zariadenie. [13]

NVR (sieťový videorekordér) spĺňa všetky funkcie ako DVR u analógových systémov, pričom poskytuje vyššie rozlíšenie a kvalitu videa. Toto zariadenie je využívané pri IP kamerových systémoch a hlavnou výhodou je, že ak je zariadenie vybavené PoE, nie je nutné privádzať ďalší kábel pre napájanie kamier. [13]

Zobrazovacie zariadenia

Monitory sú výstupné zariadenia VSD, na ktorých je zobrazený dej snímaný kamerami alebo dej zaznamenaný na videorekordéri. V praxi sú využívané CRT, LCD a plazmové monitory. [13]

Obr. 11 LCD monitor [20]

Kamerové prepínače umožňujú zobraziť pohlaď z viacerých kamier na jednom monitore, ale nie súčasne. Podľa typu je možné zobrazované vstupy voliť ručne alebo automaticky s naprogramovaním pre jednotlivé vstupy. Najčastejšie sú typy s poplachovými vstupmi, ktorých aktivácia poplachu spôsobí automatické zobrazenie konkrétnej kamery. [13]

Deliče obrazu (kvadrantový sektor) slúžia k súčasnému zobrazeniu viacerých kamier na jednom monitore. Zariadenia majú 2, 4, 8, 16 vstupov a pracujú s digitalizáciou vstupných dát. Okrem základných funkcií môžu mať aj poplachové vstupy, vkladanie textu, dát, času atď. [13]

Multiplexery umožňujú realizáciu multikamerových systémov, čo sa prejaví najmä pri požiadavkách na záznam a analýzu. Multiplexer je priamo pripojený s videorekordérom a spolupracujú pri zázname a prehrávaní. Oproti videoprepínačom dokáže skrátiť tzv. „mŕtvy čas“ v sekvencií zberu. [13]

Kompresia dát

Kompresia videa slúži k zníženiu objemu dát alebo dátového toku pri čo najmenšej degradácií obrazu. Na prevod videa s rôznych komprimovaných súborov slúži kodek videa. Dôvodom kompresie môže byť pamäťová náročnosť a archivácia video záznamu alebo zníženie doby nutnej na prenos informácie cez sieť. Hlavnými parametrami kompresie je kompresný pomer a dátový tok. Obecne rozlišujem dva typy kompresie:

- **bezstratová kompresie-** Nestratový spôsob kompresie dát, ktorý sa používa na programy alebo texty, kde nie je možné so stratou počítať. Nestratovou kompresiou v obrázkoch a videách je tzv Huffmanovo kódovanie.
- **stratová kompresia-** hlavnou úlohou je odstránenie nadbytočných informácií z obrazu. Výhodou stratovej kompresie je vyšší kompresný pomer, čo as odzrkadlí väčšou rýchlostou. Stratová kompresie je využívaná pre tieto formáty obrazu: JPEG, MJPEG, MPEG nebo H.261- H.265. [21]

V praxi sú najvyužívanejšie kodeky H.264 a H.265. Novinkou je špeciálny kompresný algoritmus H.265+ od spoločnosti Hikvison, ktorý uviedol na trh Ultra HD bezpečnostnú kameru. Vysoké rozlíšenie kamery potrebovalo veľkú skladovaciu kapacitu, preto spoločnosť vyvinula H.265+, ktorá vychádza zo štandardu H.265. [22]

2.1.1.4 Príslušenstvo kamier

Medzi základné príslušenstvo kamier radíme rôzne kryty.

Držiaky

Držiaky je možné rozdeliť na vonkajšie a vnútorné. Podľa umiestnenia na tyč, stenu alebo roh atď. Pri výbere správneho držiaka je nutné brať ohľad na:

- nosnosť,
- použitý materiál,
- možnosť a rozsah natočenia,
- spôsob vedenia káblov. [16]

Kryty

Hlavnou funkciou krytov je ochrana kamery pred poškodením (poveternostné vplyvy, prach, nesprávna manipulácia, ukradnutie, zamaskovanie kamery). Kryty je tiež možné rozdeliť na vnútorné a vonkajšie podľa použitia.

Parametre krytov sú:

- materiál,
- vyhrievanie,
- ventilátor,
- pracovná teplota,
- napájanie vykurovania,
- ochrana pred vplyvom počasia,
- plynotesnosť. [16]

IR reflektory

IR reflektory sa používajú na presvietenie scény infračervenom pásme od 700 nm do 1200nm, kde je predpokladaná zlá viditeľnosť. Tieto reflektory je možné rozdeliť na halogénové a LED diódové (určené na kratšie vzdialenosti). Medzi základné vlastnosti patria:

- odolnosť voči poveternostným vplyvom,
- dosah reflektoru (3-150m)
- pre LED počet diód a ich životnosť,
- prevádzková teplota,
- napájanie,
- príkon,
- vyžarovací uhol,
- vlnová dĺžka. [16]

Polohovacie hlavice

Polohovacie hlavice slúžia na pohyb kamery, ktorý je možné riadiť diaľkovo. Kamera môže byť nastavovaná horizontálne alebo vertikálne. Túto variantu nahrádzajú Doom a Speed Dome kamery, ktoré sú drahšie, ale ovládacie vlastnosti majú oveľa rýchlejšie. Polohovacie hlavice sú teda využívané len na menší uhlový rozsah pri približovaní statickej kamery poprípade na sledovanie scén s menšou frekvenciou. Tieto hlavice môžeme rozdeliť na vonkajšie a vnútorné. Medzi základné parametre patrí:

- napájanie,
- nosnosť,
- rozsah naklápania a natáčania,
- rýchlosť naklápania a natáčania. [16]

Softwarové doplnky

Medzi softwarové doplnky je možné zaradiť tieto funkcie:

- automatické riadenie osvetlenia (Authomatic Light Control, ALC),
- automatické vyváženie bielej (Auto White Balance, AWB),
- rozšírené automatické sledovanie bielej (Automatic Tracing White, ATW),
- kompenzácia voči svetlu (Back Light Compensation, BLC),
- bodová kompenzácia voči svetlu (Peak White Inversion, PWI),
- funkcia Auto Black zvyšuje kontrast a dynamický rozsah,
- gama korekcia umožňuje zmenu lineárnej svetelnej prenosovej charakteristiky,
- funkcia deň/noc - prepínanie kamery z farebnej na čiernobielu,
- detekcia sabotáže (tamper detection). [16]

2.1.2 Správa systému

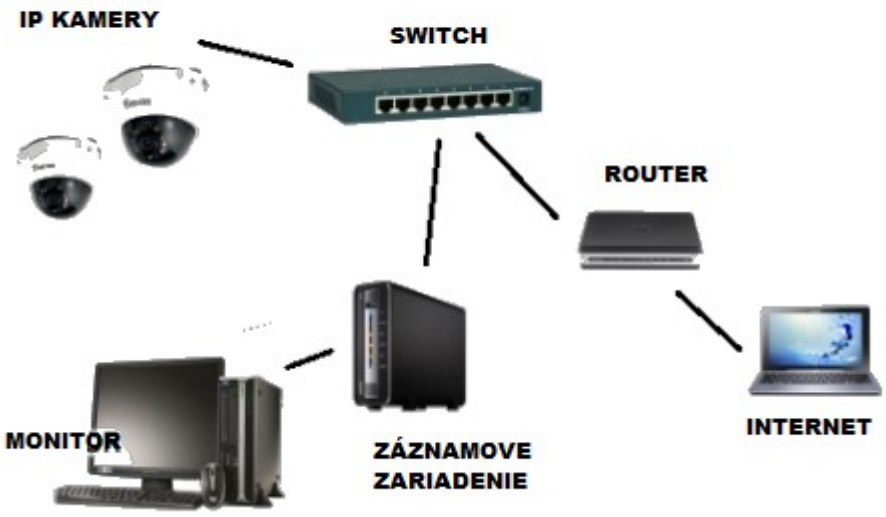
Pre správu aktivít a dát v rámci VDS je dôležité užívateľské rozhranie, ktoré môže výrazne ovplyvniť komfort, funkcionalitu a bezpečnosť VDS. Správu systému vo VDS určujú dve hlavné funkcie:

- Správa aktivít a dát pre snímanie, prenos, ukladanie a zobrazenie snímok, ich dát a metadát. Táto funkcia teda zahŕňa riadiace príkazy a systémom generované aktivity ako napr. poplachové postupy, upozornenie operátora atď.
- Rozhranie, ktoré prepája VDS s inými systémami.

Spomenuté funkcie neodkazujú na samostatné zariadenia, pretože jedno zariadenie môže vykonávať viacero úloh (napr. rekordér- ukladá spracováva, posiela obraz na výstup, analyzuje obsah videa a upozorňuje operátora). c

Správa dát

VDS spravuje video dáta a tiež môže spracovávať ďalšie získané dáta (audio či iné metadáta), ktoré môžu byť získané alebo generované iným systémom. Tento obsah dát je najčastejšie spracovávaný systémom v spolupráci s operátorom. Správa dát zahŕňa ich získavanie (napr. snímanie obrazu), prenos dát medzi prvkami systému (napr. prenos snímok z kamery do rekordéru), ukladanie snímok (napr. záznam na pevný disk alebo server) a zobrazenie dát (napr. zobrazenie snímok na monitore). Na Obr.12 je možné vidieť príklad štruktúry VDS. [12]



Obr. 12 Štruktúra VDS [23]

Správa dát zahŕňa aj ovládanie a generovanie metadát. VDS pracuje s rôznymi druhmi metadát:

- dáta spojené s video dátami (dáta z pokladní, dáta ŠPZ, dáta upresňujúce pozíciu). Tieto dáta môžu byť získavané z iného systému alebo generované systémom.
- logovacie súbory generované a archivované systémom popisujúceho aktivity systému alebo operátora.
- systémové dáta, ktoré sú vo forme systémových stavov (využitie pamäťových úložísk). [12]

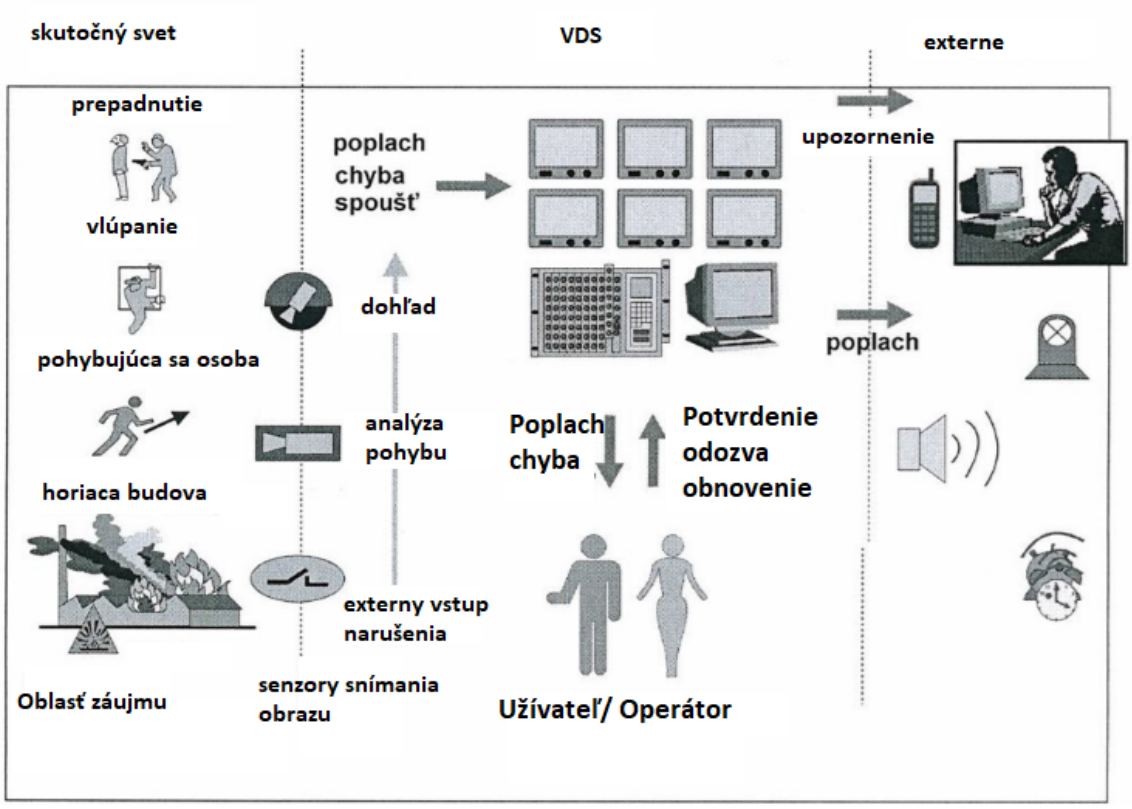
V prevádzkových požiadavkách sú uvádzané informácie o tom, ako je operátor zodpovedný za dané relácie. Operátor musí byť schopný flexibilného obsluhovania daného systému aj za nepredpokladaných skutočností. [12]

Správa aktivít

Správa aktivít zahŕňa všetky činnosti, ktoré sú riadené udalosťami alebo akýmikoľvek užívateľskými akciami. Pod pojmom udalosť si môžeme predstaviť akékoľvek udalosti, ktoré môžu spôsobiť nebezpečie, ohrozenie ľudských životov alebo majetku (napr. požiar, poškodenie perimetra, pohyb po objekte atď.). Udalosťou tiež môže byť jav zmeraný na VDS (napr. neoprávnená manipulácia so systémovými prvkami). Všetky tieto udalosti môžu spustiť poplachový postup. Spúšťacím mechanizmom môže byť:

- výstupný signál zo spracovaného obrazu:
    - VCA(video analýza objektu)
    - VMD (video detekcia pohybu)
- Signál z optických senzorov dymu alebo pohybu
- EAS (elektrický dohlaď na tovar) brány
- ANPR systém (automatické rozpoznávanie ŠPZ) [12]

Ak dôjde k spusteniu poplachu, VDS pracuje podľa predom definovaných úloh, ktoré sú zaznamenané v prevádzkových požiadavkách. Jedná sa o odozvu na zaznamenané nebezpečenstvo. Odpoveď na poplach môže zahŕňať aj vonkajšie aktivity (napr. úmyselné mechanické presmerovanie kamery) alebo aj upozornenie externého systému (napr. riadenie prístupu alebo dohľadové prijímacie poplachové centrum). Úlohou poplachového postupu je aj upozornenie operátora, ktorý môže reakciou spustiť ďalšie činnosti, ktoré sú uvedené v prevádzkových požiadavkách. Obr. 13 zobrazuje činnosť spustenej udalosti. [12]

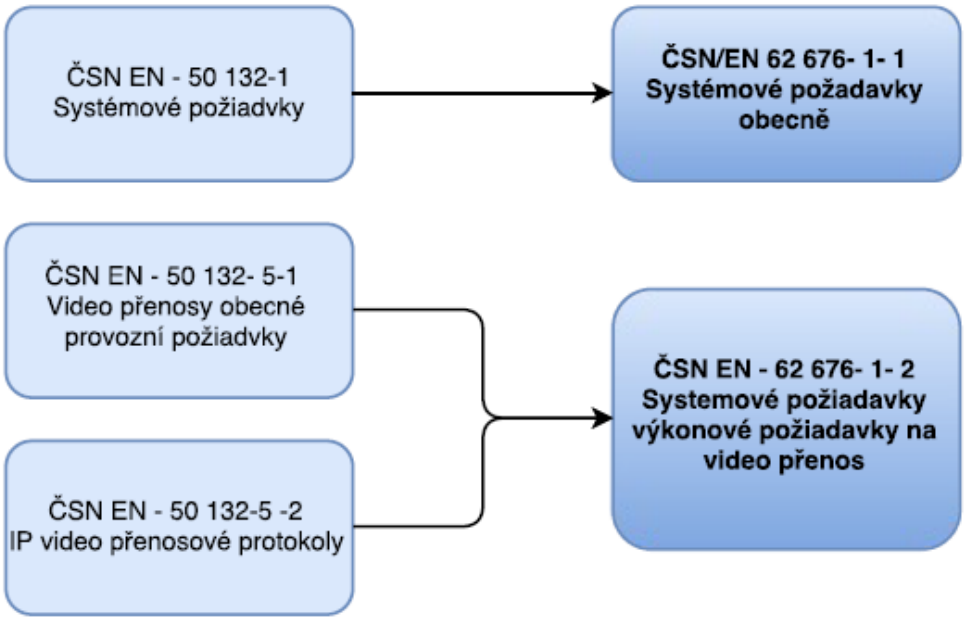


Obr. 13 správa aktiv [12]

Pod správu aktív patrí aj konfigurácia systému, riadenie systému, spätná analýza udalostí a ďalších činností prevedené operátorom. Príkladom týchto činností môže byť nastavenie pozícií PTZ kamier, presmerovanie snímok na monitor, zálohovanie dát, export a tlač. [12]

2.2 Legislatíva

Rok 2016 mal pre štandardizáciu noriem dohľadových systémov výrazný vplyv. Koncom tohto roku zanikla norma ČN EN 50 132 pre dohľadové systémy v oblasti bezpečnostných aplikácií. Od roku 2014 však prebiehalo vyvíjanie novej normy ČN EN 62 676 -x, ktorá dnes úplne nahradila normu ČSN EN 50 132 v danej oblasti. Na obrázku č. 14 je možné vidieť prehľadnú schému procesu nahradenia normy v určitých oblastiach.



Obr. 14 Prehľad aktualizácie noriem

Tab. 3 *Technické normy platné pre VDS*

Číslo technickej normy	Názov technickej normy
ČSN EN 62 676 - 1 - 1	Systémové požadavky - Obecně
ČSN EN 62 676 - 1 - 2	Systémové požadavky Výkonové požadavky na video přenos
ČSN EN 62 676 - 2 - 1	Video přenosové protokoly Obecné požadavky
ČSN EN 62 676 - 2 - 2	Video přenosové protokoly - Implementace vzájemné spolupráce IP systémů založených na využití HTTP a REST
ČSN EN 62 676 - 2 - 3	Video přenosové protokoly - Implementace vzájemné spolupráce IP systémů založené na síťových (web) službách

ČSN EN 62 676 - 3	Analogové a digitální video rozhraní
ČSN EN 50 132 - 5 - 3	Video přenosy - Analogový a digitální video přenos
ČSN EN 50 132 - 7	Pokyny pře aplikace

Vzhľadom na zameranie práce sú v práci primárne využité poznatky z technických noriem : ČSN EN 62676-1-1, ČSN EN 62676-1-2 a ČSN EN 62676-2-1.

Technická norma ČSN EN 62676-1-1 Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně

Norma zavádza pojem videosystémy (VSS- Video Surveillance System), ktorý nahrádza názov CCTV. Popisuje minimálne požiadavky a odporučenia pre bezpečnostné aplikácie, špecifikuje minimálne výkonové a funkčné požiadavky. [12]

Technická norma ČSN EN 62676-1-2 Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-2: Systémové požadavky - Výkonové požadavky na video přenos

Uvádza všeobecné požiadavky na prenos videa. Obsahuje požiadavky na video prenos z hľadiska výkonu, zabezpečenia a zhody na základe IP konektivity v súlade s dostupnými medzinárodnými normami. [24]

Technická norma ČSN EN 62676-2-1 Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 2-1: Video přenosové protokoly - Obecné požadavky

Norma sa venuje IP sieťovému rozhraniu pre aplikáciu dohľadových aplikácií. Špecifikuje sieťové protokoly pre plnú interoperabilitu videozariadení. [24]

Pri spracovaní údajov musia byť dodržované :

- zákon č. 262/2006 zakonník práce,
- Zákon 101/2000 Sb o ochrane osobných údajov.

Tak ako prvky SKV tak aj prvky VDS musia spĺňať nasledujúce požiadavky:

- elektrickú bezpečnosť ČSN EN 60950, ČSN EN 60065
- elektromagnetickú kompatibilitu a odolnosť ČSN EN 61000, ČSN EN 55022, ČSN EN 50082, ČNS EN 50130
- telekomunikácie ČSN EN 50529

- kombinované a integrované systémy ČSN CLC/TS 50398 (v prípade integrácií s inými systémami)

Samostatne je riešená oblasť integrovaných systémov VDS:

- požiadavky na integráciu VDS odkazujú na normu ČSN CLC/TS 50398,
- nutnosť špecifikácie rozhrania s ďalším systémom,
- integrátor vyvíja implementáciu pre rozhranie
- možnosť voľby otvorených systémov video managementu alebo skriňových sústav, dovoľujú integráciu rôznych výrobcov
- IP zariadenia by mali byť kompatibilné v oblasti konektivity, prenosu a riadenia video streamu, dátového objemu či synchronizácie času.

2.3 Rozsah a topológia

Kamerové systémy od svojho uvedenia do praxe prešli dlhú cestu, táto kapitola preberie rôzne topológi nie od ich počiatku, ale zameria sa len aktuálne možnosti. Vynechá zastaralé možnosti s využitím VCR ((video cassete recorder). Zameria sa na využitie sieťových topológií.

2.3.1 Analógové VDS založené na sieťovanej DVR technológií

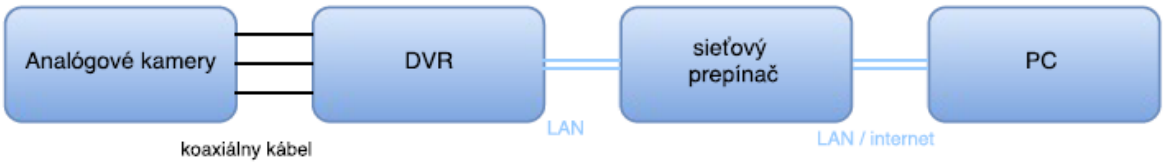
Pripojenie k sieti je pre DVR výhodou, preto bol systém vybavený ethernet portom, čo umožnilo spravovať vzdialenú video cez počítače Obr.17. Aby to bolo možné, je nutné mať v počítači nainštalované špeciálne programy, ktoré umožňujú ovládanie kamier a sledovanie videa. Tieto programy však existujú aj ako rozhranie vo webových prehliadačoch, čo robí VDS flexibilnejšími. [25]

Výhody

- vzdialené ovládanie
- diaľkové ovládanie systému

Nevýhody

- údržba a náhradné diely boli drahé
- žiadna antivírusová ochrana
- škálovateľnosť. [25]



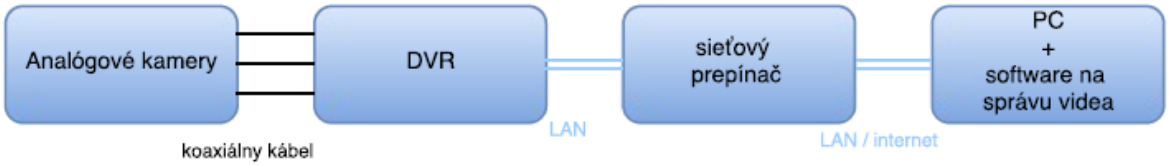
Obr. 15 Diagram sieťového DVR VDS [25]

2.3.2 Sieťové video systémy založené na video-encoderi

Významným krokom bolo zavedenie video-encoderu (video serveru), ktorý bol pripojený na kamery a dokázal zdigitalizovať, skomprimovať a následne poslať dáta cez IP sieť až k serveru, kde bežal software pre správu videa. Úlohy DVR sú v tomto prípade rozdelené tak, že digitalizáciu a komprimáciu vykonáva encoder a nahrávanie prebieha až v PC na serveri, čo zaručuje lepšiu škálovanosť [24]

Výhody sú:

- využitie štandardných sietí.
- lepšia škálovanosť.
- záznam na web.
- rozšíriteľnosť o sieťové kamery. [25]



Obr. 16 Diagram sieťového VDS s video-encoderom [25]

2.3.3 Sieťové VDS založené na IP kamerách

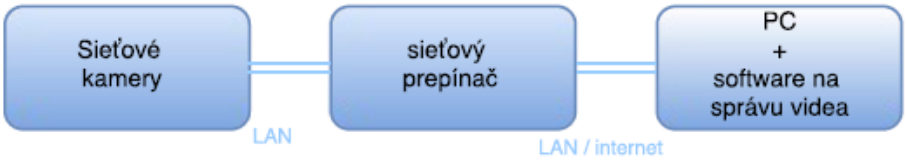
IP kamery posielajú video cez IP sieťové prepínače k PC serveru so správou videa. Tento systém nepoužíva žiadne analógové komponenty takže je plno digitálny. Najväčšou výhodou IP kamier je, že video je po celú dobu v systéme digitálne, čo zaručuje vysokú kvalitu. V rámci tejto technológie je možné vybudovať dohľadový systém so stovkami alebo tisícami kamier. *[24]*

Výhody:

- možnosť používať kamery s vysokým rozlíšením (high-resolution),
- možnosť využívania PoE.

- prístup k funkciám: snímať (pan), otočiť (tilt), priblížiť (zoom),
- audio a digitálne vstupy a výstupy cez IP spoločne s videom.
- Konfigurácia kamier a systému cez IP sieť.
- Flexibilita a škálovanosť. *[25]*

Vďaka tomu, že IP kamery majú vyšší vypočítaný výkon, vytvárajú možnosť video-inteligencie alebo videoanalýz. Dnes je videoanalýza veľkým trendom, pretože video je nutné riadiť a analyzovať efektívne, a to hlavne vo veľkých firmách.



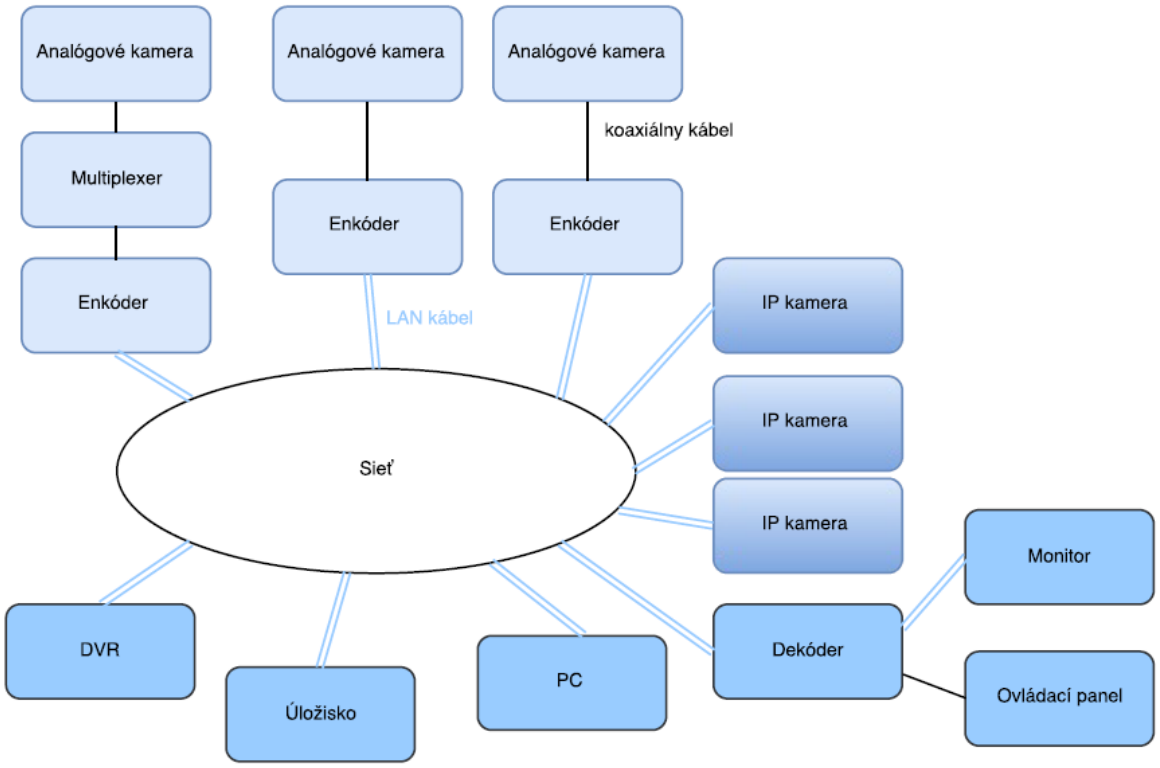
Obr. 17 Diagram sieťového VDS s IP kamerami [25]

2.3.4 Video prenosová sieť (VTD)

Video prenosové štandardy určujú rozdielne požiadavky na zariadenia s rozdielnymi charaktermi. Táto konfigurácia poskytuje model zariadení s konzistentnými podmienkami a použitím pre funkcionalitu týchto zariadení. Pre podporu interoperability medzi VDS sieťovými zariadeniami je pre klienta nevyhnutné splnenie všetkých požiadaviek odpovedajúceho dekódovacieho zariadenia VDS siete. Tiež je pre nahrávanie DVR nevyhnutné NVR alebo sieťové úložisko, ktoré spĺňa všetky požiadavky. Hybridný systém ponúka tieto funkcionality:

- enkódovanie streamu,
- prijímanie a dekódovanie streamu,
- nahrávanie streamu,
- zobrazenie streamu,
- prehrávanie streamu,
- ovládanie kamier,
- monitorovanie stavu zdravia,
- analýza video dosahu,
- vytvorenie a streamovanie metadát,
- pomocné zariadenia. [25]

Kľúčovým bodom rôznych funkcionalít je možná optimalizácia na požiadavky aplikácie. VTD štandard je zameraný na interoperabilitu zariadení s rovnakými odpovedajúcimi funkciami. [25]



Obr. 18 Video prenosová sieť [25]

2.4 Rozhranie s inými systémami

Pri prepájaní s iným systémom je nutné brať do úvahy, že oba systémy musia mať presne definované formáty príkazov a dát. Pri správnej konfigurácií rozhranie systému umožní vzájomný komfortný prístup k funkciám a dátumom. [26]

VDS môže byť prepojený s týmito systémami:

- Bezpečnostné systémy:
  - iné VDS
  - poplachové tiesňové a zabezpečovacie systémy (PZTS)
  - systémy kontroly vstupu
  - systémy požiarneho poplachu
- Systémy správy bezpečnosti:
  - systémy správy poplachu

    - dohľadové poplachové a prijímacie centrum
    - vzdialené centrum video dohľadu
- Systémy nesúvisiace so zabezpečením:
    - systémy správy budov
    - bankomaty
    - vybavenie na dohľad predajne
    - systémy pre automatické rozpoznávanie ŠPZ[26]

Prepojenie medzi systémami môže riadiť dátovú komunikáciu, vzájomné riadenie systému, spoločné databázy, užívateľské rozhrania alebo iné typy systémovej integrácie. Všeobecne je možné rozlíšiť dva typy prenosu fyzická prenosová cesta s VDS alebo poskytnutá treťou stranou. [26]

2.5 Čiastkový záver

Dohľadové videosystémy ako aj systémy kontroly vstupu sa stále inovujú, preto aj technický rámec prostredníctvom technických noriem sa mení. Táto kapitola je zameraná na funkčné vlastnosti video dohľadových kamerových systémov, ktoré sú uvedené v normách ČSN EN 62676-1-1, ČSN EN 62676-1-2 a ČSN EN 62676-2-1. Pre zameranie práce je dôležitým faktom, že VDS sú kompatibilné s inými poplachovými a neoplachovými systémami, tento fakt je podrobnejšie uvedený aj v norme ČSN EN CLC/TS 50398 v nasledujúcej kapitole.

Vybraná spoločnosť momentálne využíva dva VDS ktoré pracujú pod softwarmi DEDICATED-MICROS a ATEAS 4.4.0. DEDICATED-MICROS je zastaralý systém, ktorý spolupracuje s analógovými kamerami. V dnešnej dobe sú vypracované projekty na jeho aktualizáciu na ATEAS. ATEAS 4.4.0 je komplexný VDS, ktorý v dnešnej dobe, už v objekte spolupracuje s veľkým množstvom kamier. Tento software sa vyznačuje najmä technológiou inteligentného systému a je možné ho jednoducho integrovať.

3 SPÔSOBY INTEGRÁCIE

Integrácia ponúka niekoľko foriem prevedenia, ktoré vždy vychádzajú z technického riešenia vzájomného prepojenia systémov. S ohľadom na množstvo a odlišnosti dnešných elektronických zariadení je vždy možné previesť niekoľko variánt pre konkrétny objekt. Projekt závisí hlavne na zadaní investora a na návrhu poplachového integrovaného systému. Klasifikácia technických spôsobov integrácie vychádza z analýzy nasledujúcich dokumentov:

- technické normy- oblasť integrovaných poplachových systémov,
- technické normy- oblasť poplachových systémov (PZTS, VDS, SKV, SAS),
- technické špecifikácie výrobcu,
- inštalačné manuály relevantných systémov a ich prvkov,
- právne predpisy- legislatívne vymedzenie technických požiadaviek na komponenty integrovaných poplachových systémov. [27]

Technické spôsoby prepojenia jednotlivých aplikácií sú rozdelené na dve základné skupiny:

- hardwarové spôsoby integrácie,
- softwarové systémy integrácie. [27]

3.1 Technické požiadavky pre integráciu

Pri návrhu integrovaného systému je nutné vypracovať súbor požiadaviek, v ktorom bude špecifikovaná celistvosť systému. Návrh zároveň musí obsahovať aspoň tieto informácie:

- druhy použitých požiadaviek aplikácií,
- ciele, ktoré integráciou dosiahneme,
- charakteristika objektu, v ktorom bude systém integrovaný.

V integrovaných poplachových systémoch musia všetky zariadenia odpovedať normám pre ich aplikáciu. Ak je zariadenie spoločné pre viacero aplikácií, musí vyhovovať normám pre každú aplikáciu. To platí aj pre súvisiace prvky integrovaného systému napr. kabeláž a napájacie zdroje. [27]

3.1.1 Všeobecná klasifikácia

Norma ČSN EN CLC/TS 50398 rozdeľuje integrované poplachové systémy do troch základných skupín uvedených v tabuľke Tab, 4

Tab. 4 rozdelenie integrovaných poplachových systomv [27]

Typ 1	Ide o kombináciu a integráciu jednoúčelových poplachových systémov s jednoúčelovým systémom nepoplachového typu.
Typ 2A	Kombinácia integrácia poplachových a nepoplachových systémov využívajúcich spoločné zariadenia, vybavenie a prenosové cesty. Porucha jedného systému nemôže spôsobiť poruchu na druhom systéme.
Typ 2B	Rovnako ako pri type 2A sa jedná o integráciu poplachových a nepoplachových systémov využívajúcich spoločné zariadenia, vybavenie a prenosové cesty. Rozdielom je, že porucha jednej aplikácie môže ovplyvniť chod ostatných.

Jednoúčelový systém je zariadenie využívané pre špecifické účely alebo jeden účel napr. VDS a SKV. Spoločným zariadením je zabezpečená jedna alebo viacero aplikácií. (VDS dáva povolenie otvorenia brány pri skontrolovaní ŠPZ).

3.1.2 Systémové požiadavky

V kľudovom stave integrovaného systému nesmie žiadna aplikácia negatívne ovplyvňovať funkciu inej aplikácie. Signály môžu byť prenášané z jedenej aplikácie do druhej, alebo z ústredného ovládacieho zariadenia do aplikácie.

Ak systémy využívajú spoločné ovládacie a signalizačné zariadenia, musia mať jednoduché ovládanie a signalizácia musí spĺňať najprísnejšie požiadavky definované normami. Pri signalizácii by mali byť priority zoradené následne:

- Priorita 1- Poplachové signály vzťahujúce sa k ochrane života pri požiarnom poplachu alebo napadnutí.
- Priorita 2- Poplachové signály vzťahujúce sa k ochrane majetku a proti nedovolenému vniknutiu
- Priorita 3- Poplachové signály ostatných poplachových systémov.
- Priorita 4- Poplachové signály zo systémov ochrany života a majetku.
- Priorita 5- Poplachové signály z ostatných poruchových signálov.
- Priorita 6- Poplachové signály nepoplachových systémov.

Ak sa jedná o software jednotlivých poplachových a nepoplachových aplikácií odporúča sa, aby jeho dokumentácia bola oddelená od návrhu. Ak je možnosť pôsobenia softwarov negatívne, malo by to byť popísané v zvláštnej dokumentácií. [27]

3.1.3 Požiadavky na centrálne ovládacie zariadenie

Centrálne ovládacie zariadenie je rozdelené do dvoch základných tried uvedených v tabuľke

Tab. 5 Triedy centrálnych ovládacích zariadeni [27]

Trieda 1	Pre zobrazovanie informácií, nepretržitá obsluha, signalizačné zariadenie umiestnené na rovnakom mieste ako centrálne ovládacie zariadenie
Trieda 2	Okrem zobrazovania informácií môže byť pre všetky ostatné činnosti, neustála obsluha.

Centrálne ovládacie zariadenie musí spĺňať tieto funkcie:

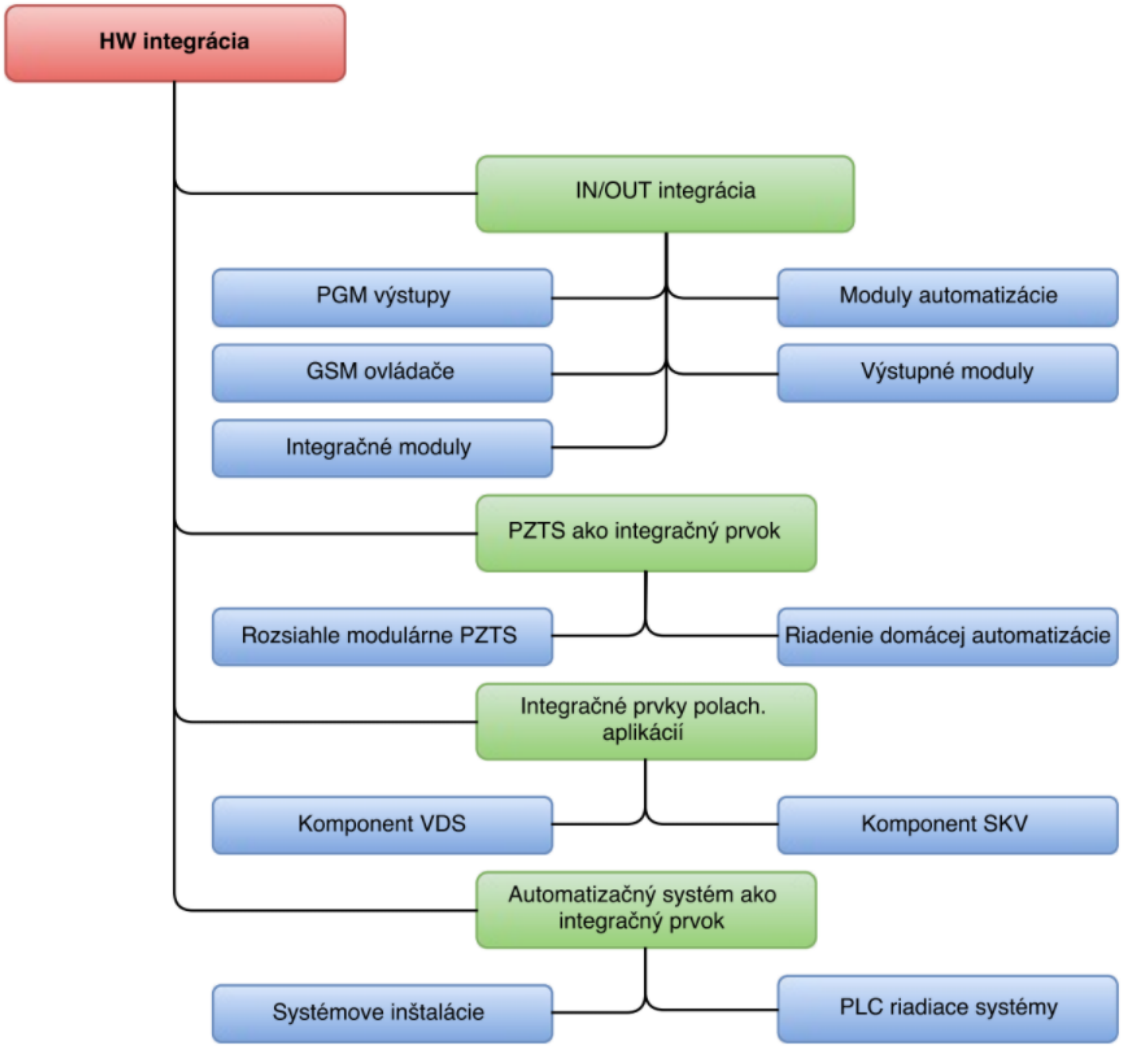
- zodpovedať správnej triede prostredia,
- byť správne umiestnený (podľa triedy),
- vyčlenený iba pre integrovaný poplachový systém
- opticky a akusticky signalizovať poruchy,
- monitorovať sieťové pripojenie,
- signalizovať výpadok komunikácie
- obsahovať záložný zdroj. [27]

3.2 Hardwarová integrácia

Hardwarová integrácia je založená na:

- vzájomnom prepojení vstupov a výstupov,
- technických parametroch.

Technické parametre môžu zahŕňať okrem základných bezpečnostných funkcií aj špeciálne rozširovacie prvky (moduly), ktoré zabezpečujú ovládanie ďalších poplachových alebo nepoplachových aplikácií. Medzi hardwarové spôsoby integrácie sú zaradené aj automatizačné systémy (napr. systémová elektroinštalácia), ktoré okrem ovládania štandardných technológií v budovách ponúkajú možnosť pripojenia zabezpečovacích prvkov (prvky PZTS, SKV, VDS atď.) [28]



Obr. 19 Hardwarová integrácia možnosti integrácie [26]

3.2.1 Integrácia IN/OUT

Technické riešenie integrácie IN/OUT predstavuje spôsob prepojení prostredníctvom vstupov (IN) a výstupov(OUT). Na základe parametrov jednotlivých komponentov je možné realizovať integráciu heterogénnych systémov, ktoré zaisťujú vzájomný prenos informácií o ďalších systémoch. Tieto informácie sú využité k ovládaniu prepojených systémov v súlade s vopred nastavenou konfiguráciou (nastavenie vzájomných väzieb medzi aktivačnými udalosťami a reakčnými udalosťami). [26]

Integrácia IN/OUT je prevažne využívaná v menej rozsiahlych aplikáciách, čo samozrejme nevylučuje použitie v rozsiahlejších projektoch. Tieto riešenia sú ale technologický náročnejšie a môžu byť limitované napr. počtom programovateľných výstupov alebo pripojených modulov. V porovnaní s nasledujúcimi integráciami, z hľadiska riešenia systému

s ohľadom na jeho správu, vizualizácie a ovládania je práve integrácia IN/OUT najslabšou variantnou. Napriek tomu sa však jedná o často využívané riešenie, a to vďaka širokým možnostiam vytvárania realizácie konkrétnych, zákazníkom požadovaných funkcií. [26]

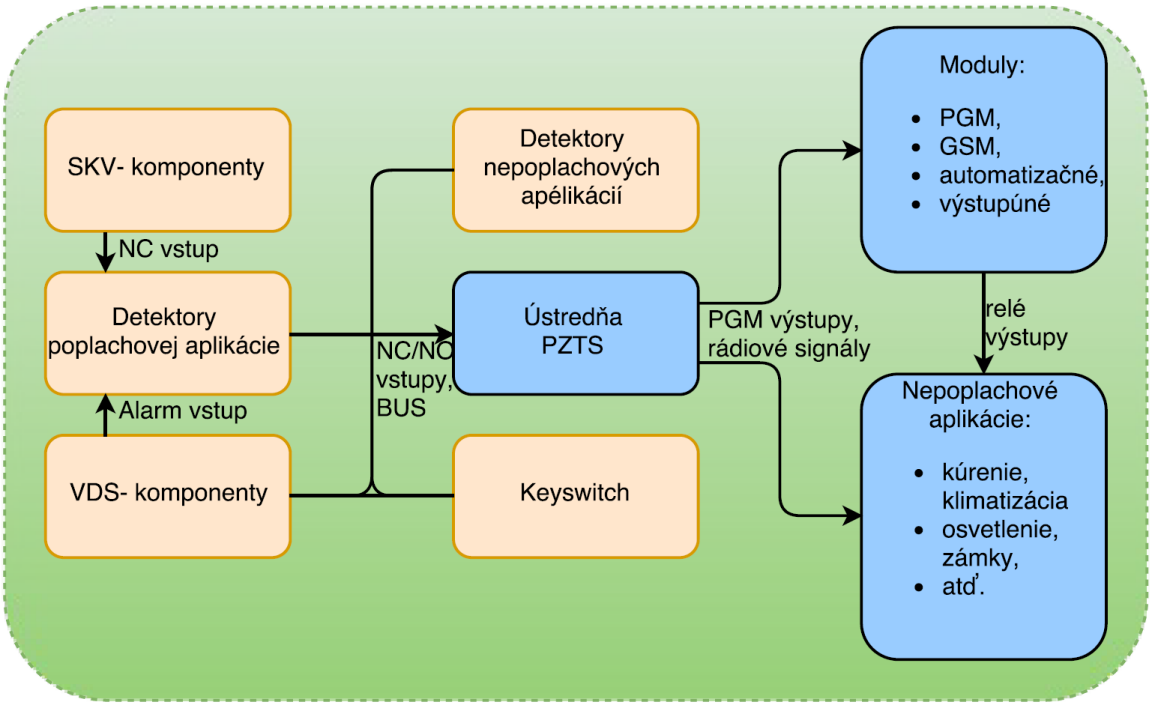
Výhody

- systémy sa vzájomne negatívne ovplyvňujú.
- jedna porucha nemusí mať vplyv na ostatné aplikácie
- prepojenie systémov realizovaných bez ohľadu na výrobcu a komunikačné protokoly. [26]

Nevýhody

- hardwarová náročnosť na počet vstupov a výstupov.
- decentralizovaná správa systémov.
- problematická centrálna vizualizácia v reálnom čase.
- nižšia transparentnosť systému. [26]

Na Obr. 20 je schematicky znázornená IN/OUT integrácia v prípade, že základný integračný prvok tvorí ústredná riadiaca jednotka.



Obr. 20 Schéma znázorňujúca možnosti integrácie IN/OUT [26]

Integračný prvok môže byť pripojený pomocou NC/NO vstupov, zbernice alebo využitím rádiového modulu (pre bezdrôtovú komunikáciu) s rôznymi detektormi, hlásičmi, ovládacími tlačidlami, prostriedkami úmyselného vyvolania poplachu ako súčasť poplachového tiesňového systému, alarmovými výstupmi atď. Na základe stavu ústrednej riadiacej jednotky je možné určiť napr. poplach, poruchu, sabotáž, aktiváciu príchodového a odchodového času, aktiváciu výstražného zariadenia, stisk tlačidla programovateľných výstupov atď.

Integráciu IN/OUT je možné rozdeliť podľa spôsobu realizácie vzájomného prepojenia systému na:

- integrácia s využitím programovateľných výstupov,
- integrácia s využitím GSM ovládačov,
- integrácia využitím modulu automatizácie,
- integrácia s využitím výstupných modulov,
- integrácia s využitím integračných modulov,
- integrácia s využitím rádiových relé modulov. [26]

3.2.2 Poplachový zabezpečovací a tiesňový systém ako integračný prvok

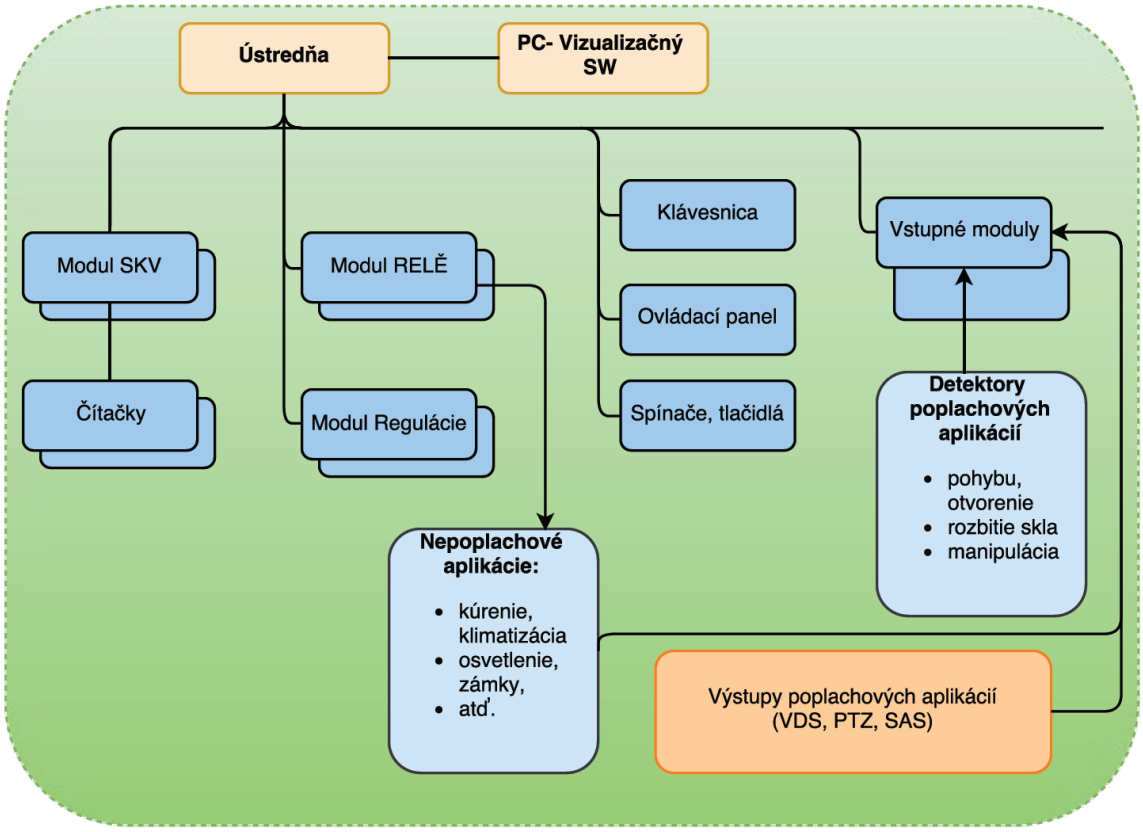
Rozsiahle poplachové zabezpečovacie a tiesňové systémy (PZTS) so zapojením cez zbernicu môžu okrem zabezpečovacích komponentov obsahovať a riadiť aj prvky kontroly vstupu či automatizácie. Umožňujú aj ovládanie pripojenia nepoplachových technológií budov. [26]

Možnosťou spôsobu integrácie s využitím ústredni je využitie funkcií výstupov ústredni poplachového zabezpečovacieho a tiesňového systému. Tento princíp je založený na generovaní signálov pre potreby ovládania automatizácie. [26]

Na základe spomenutých faktov je možné integráciu s využitím ústredni PZTS klasifikovať na:

- integráciu s využitím modulárneho systému PZTS,
- integráciu s využitím PZTS ako riadiaceho prvku systému. [26]

Na Obr. 21 je zobrazená schéma možnej varianty integrácie s nadriadeným PZTS



Obr. 21 Schéma možnej varianty integrácie s nadriadeným PZTS [26]

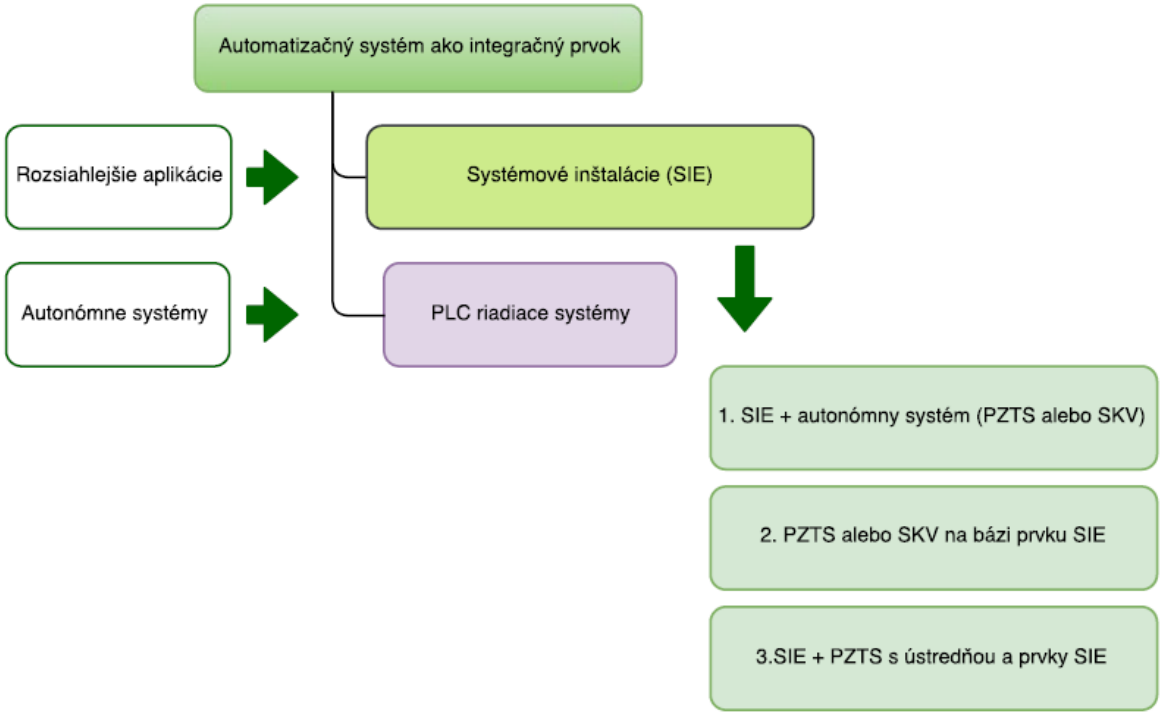
Hlavným rozdielom od integrácií IN/OUT je v smere komunikácie. V prípade IN/OUT integrácií kamera prijíma signál od ústredného riadiaceho prvku (napr. ústredňa) a reaguje na jej podnet zapnutím nahrávania. V prípade integrácie s využitím ústredni PZTS ako integračného prvku reaguje ústredňa na podnety kamery následnou vopred nastavenou funkciou. V tomto prípade však systémy nie sú od seba nezávisle. To znamená, že v prípade nefunkčnosti VDS stráca ústredňa PZTS schopnosť sledovania daného priestoru.

3.2.3 Automatizačné systém ako integračný prvok

Integrácia poplachových a nepoplachových aplikácií s využitím automatizačného systému ako integračného prvku môže byť realizovaná dvomi základnými spôsobmi:

- aplikácia systémovej inštalácie (SIE),
- aplikácia s využitím programovateľného logického automatu (PLC) riadiacim systémom.

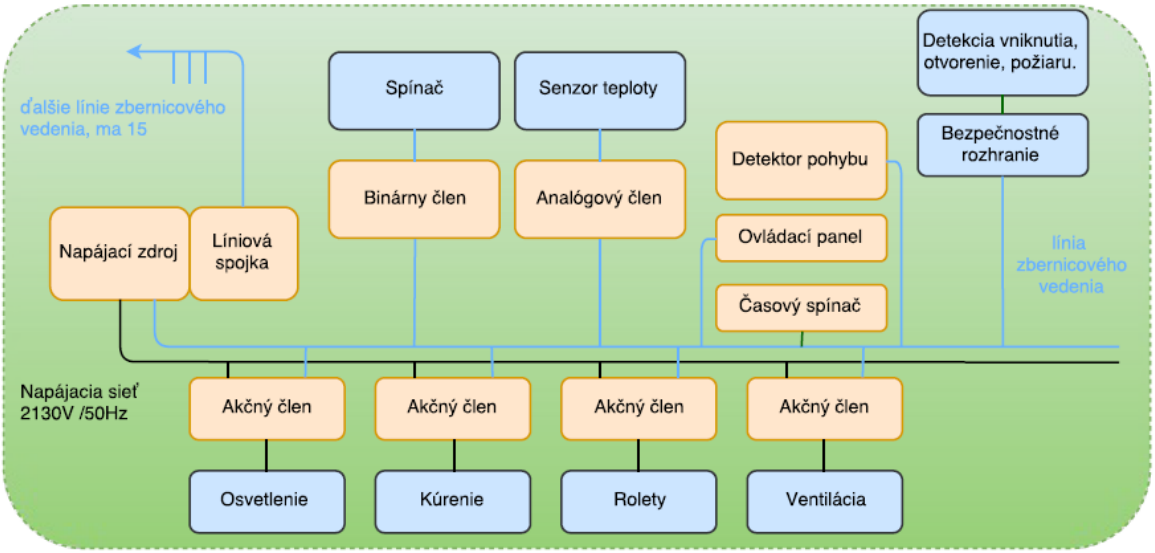
Na Obr. 22 je zobrazená základná klasifikácia možností využitia automatizačných systémov ako integračného prvku prepojenia poplachových a neoplachových aplikácií. [26]



Obr. 22 Klasifikácia spôsobu integrácie s využitím automatizačných systémov [26]

Moderné automatizačné systémy využívajú technológiu SIE. Tento spôsob integrácie je vhodný najmä pre PZTS alebo SKV. Pre VDS nie je tento spôsob až natoľko vhodný vzhľadom na fakt, že podnety, na ktoré reagujú akčné členy inteligentnej elektroinštalácie (teplota, svetlo, prednastavený čas a pod.), nie sú až tak podstatné. Samozrejme aj v tomto prípade si VDS môže nájsť uplatnenie. Hlavne ak kamery podporujú inteligentnú analýzu obrazu alebo detekciu pohybu. [26]

SIE fungujú na platforme zbernice, ku ktorej sú pripájané snímacie a akčné prvky. Jednotlivé prvky technológie je potom možné ovládať lokálne alebo diaľkovo (GSM, web) alebo nastavovať centrálne časové plány ich aktivácie a vzájomne väzby. [26]



Obr. 23 Schéma princípu zapojenia elektroinštalácie [26]

3.2.4 Integrácia s využitím prvkov poplachových aplikácií

Hardwarová integrácia poplachových a nepoplachových aplikácií môže byť zrealizovaná aj bez prvkov PZTS. Integračné prvky môžu predstavovať komponenty:

- VDS pri použití v bezpečnostných aplikáciách,
- SKV pri použití v bezpečnostných aplikáciách.

Tieto integrácie sú využívané v prípadoch, kde objekt nevyžaduje veľký rozsah integrovaného bezpečnostného systému. [26]

Prvok VDS ako integračný prvok

Pri zabezpečení hardwarovej integrácie prvkami VDS, je nutné, aby prvok obsahoval potrebné digitálne vstupy a výstupy. Tým pádom môžu byť integračným prvkom IP kamery, DVR alebo NVR

Zapojenie systému s využitím sieťovej kamery resp. jej digitálnych vstupov a výstupov umožňuje:

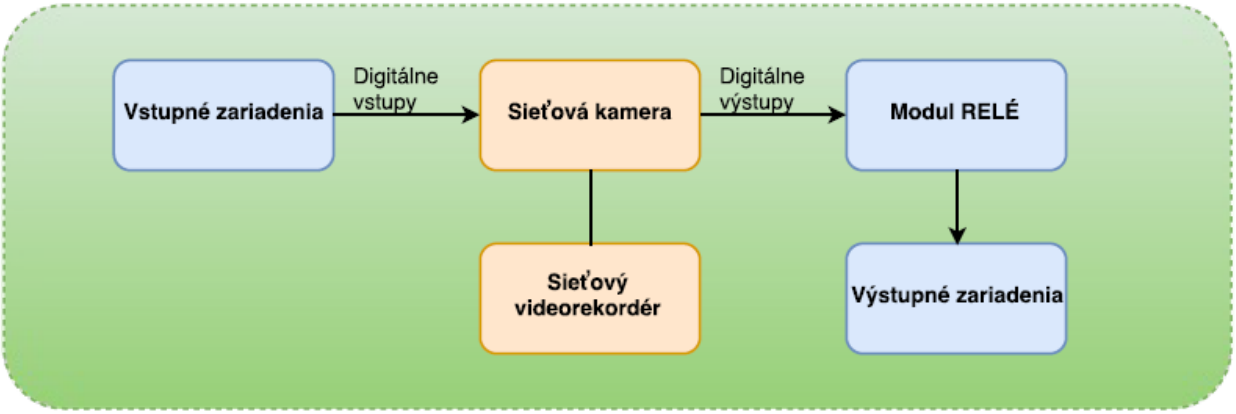
- nastaviť väzby medzi vstupnými zariadeniami a odozvu výstupných zariadení,
- nastaviť väzby medzi vstupnými zariadeniami a činnosťou kamery.

Tento spôsob v praxi zahŕňa tieto činnosti:

- zábery sú odosielané až po aktivácii vstupu,
- ukladané zábery s časom detekcie môžu byť ukladané na akékoľvek miesto v sieti,

- detekcia poplachu vniknutia je signalizovaná na ústredni PZTS,
- priama signalizácia poplachu prostredníctvom výstražného zariadenia pripojeného priamo na výstup kamery,
- ovládanie kúrenia, osvetlenia a ďalších prídavných technológií,
- nastavenie výstupných reakčných udalostí na základe úrovni zvuku,
- zamykanie a odomykanie vstupov na základe vstupných zariadení,
- zamykanie a odomykanie vstupov operátorom po sieti. [26]

Nasledujúci obrázok (Obr. 24) znázorňuje princíp integrácie s využitím sieťovej kamery ako prvku VDS dohľadového systému pre použitie v bezpečnostných alokáciách.



Obr. 24 Integrácia systému s využitím sieťovej kamery [26]

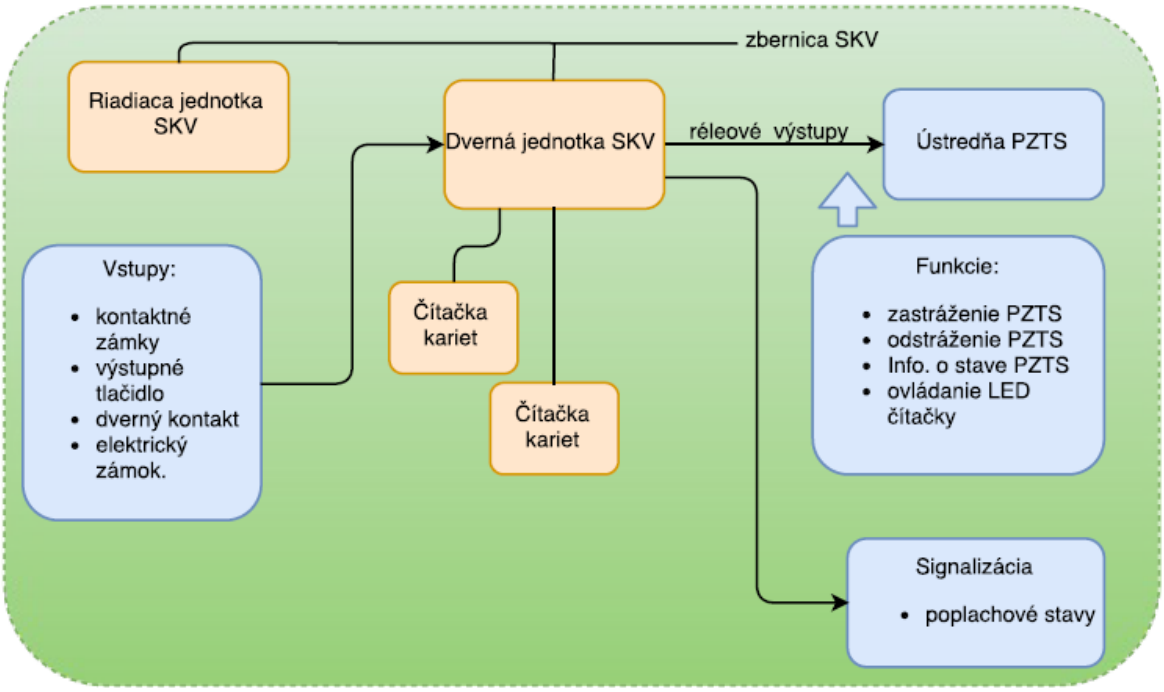
Prvok SKV ako integračný prvok

Dverné jednotky sú v SKV pripojené na riadiacu jednotku, ktorá môže obsahovať vstupy pre monitorovanie stavu a výstupy pre ovládanie. Prepojenie dvernej jednotky s ústredňou PZTS umožňuje:

- uvedenie PZTS do stavu „v kľude“,
- uvedenie PZTS do stavu „zastrážené“
- indikácia stavu PZTS na čítačke pripojenej ku dvernej jednotke,
- uvedenie PZTS do stavu „zastrážené“ na základe časového programu,
- predaktivačné upozornenia čítačky,
- premostenie vstupného zariadenia s PZTS počas doby otvorenia dverí. [26]

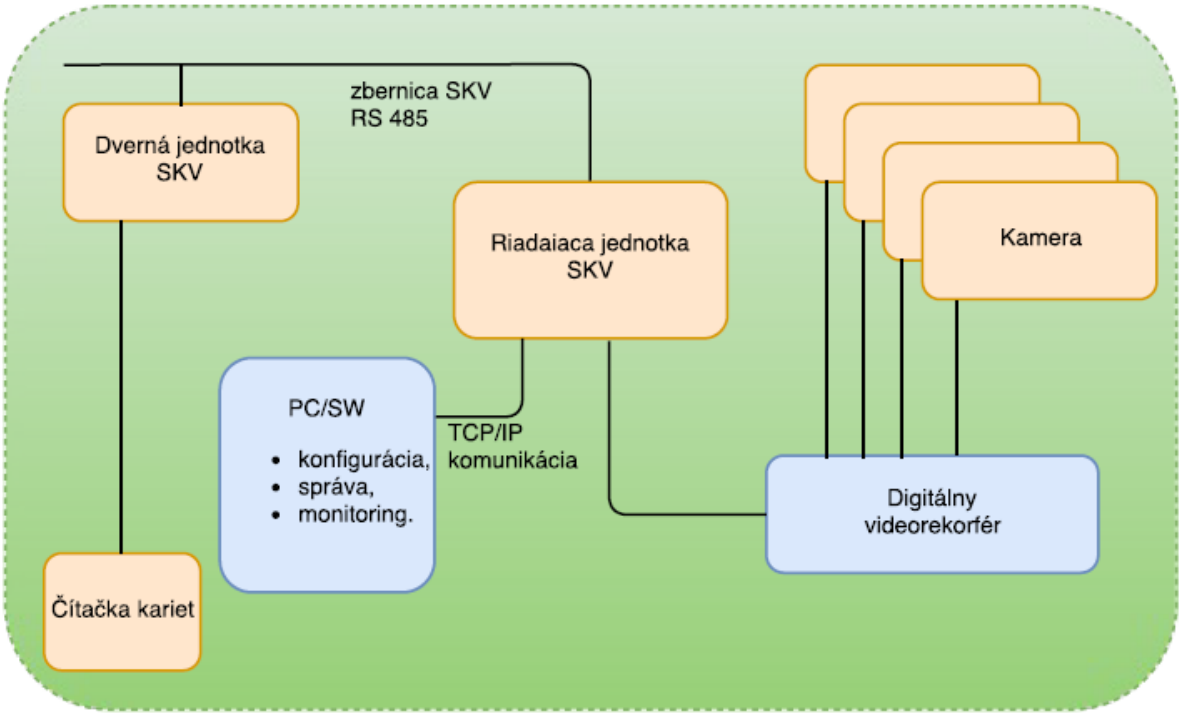
Na Obr. 25 je znázornené schematické prepojenie SKV a PZTS s využitím dvernej jednotky ako integračného prvku. Výstupy dvernej jednotky sú vybavené formou relé, ktoré okrem

vyššie spomenutých funkcií môžu aj spínať výstražné zariadenia, alebo ovládať elektronické zariadenia (elektronické zámky, IP kamery atď.)



Obr. 25 Integrácia poplachových systémov s využitím dverných jednotiek SKV [26]

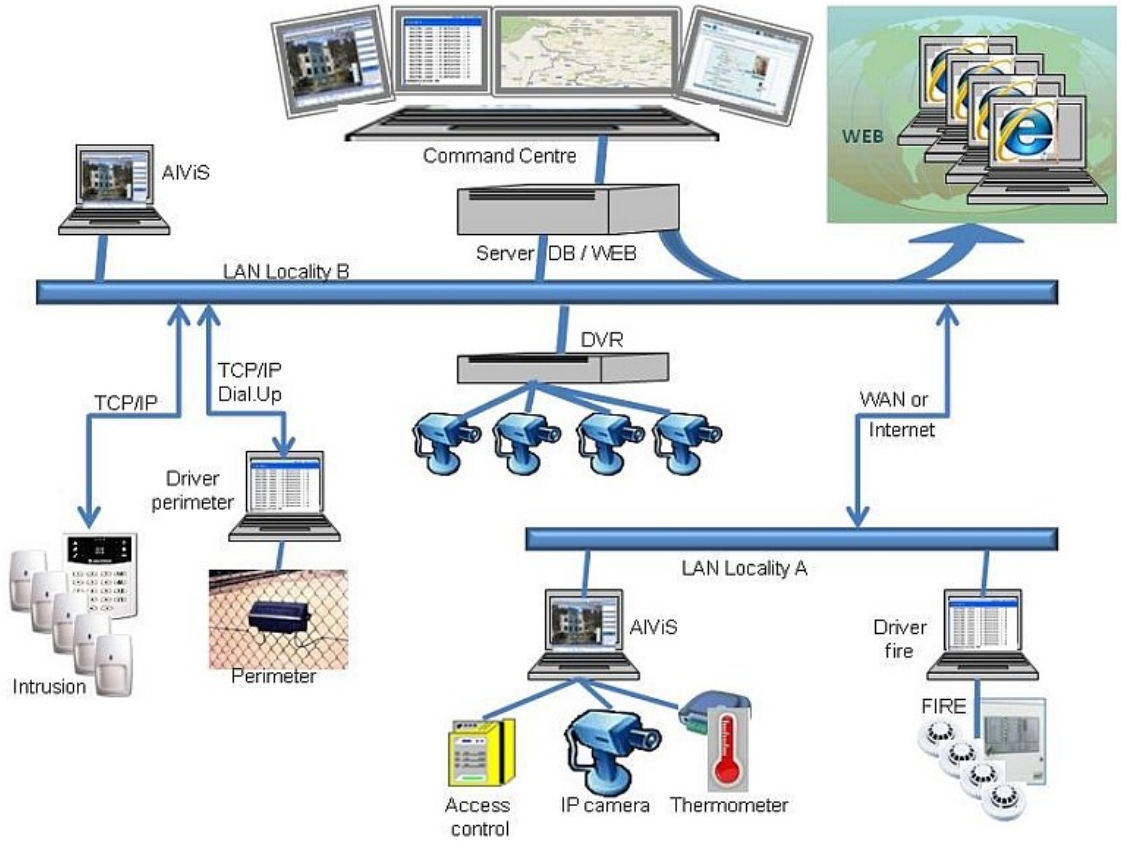
SKV umožňujú okrem integrácie SKV/PZTS aj integráciu SKV/VDS. SKV komunikuje na základe využitia protokolu TCP/IP s prvkom VDS(DVR). Toto riešenie umožňuje nastaviť udalosti v SKV, na základe ktorých je aktivovaný záznam na DVR. [29]



Obr. 26 Integrácia poplachových systémov s využitím riadiacej jednotky SKV [*26]*

3.3 Softwarová integrácia

Softwarová integrácia je využívaná najmä v prípadoch, kde sú vysoké požiadavky na obsluhu, čo je zapríčinené zložitosťou objektu či vysokým počtom zariadení. V takomto prípade nie je možné dosiahnuť prehľadné monitorovanie a riadenie objektu bez počítačovej nadstavby. Z dôvodu zjednodušenia, sprehľadnenia a zároveň zníženia prevádzkových nákladov pre jednotlivé systémové softwary je možné použiť tzv. „integračné softwary“, ktoré vzájomne integrujú SKV, EPS, PZTS, CCTV a systémy merania a regulácie. Integračné softwary ponúkajú funkcie ako vizualizácia centrálneho managementu, analýza udalostí, automatizácia bezpečnostných procesov, správa identít, riešenie krízových situácií atď. Môžu pracovať v rôznych softwarových platformách. Spolupracujú s SQL-databázami. Integrovať systémy je možné len vtedy, pokiaľ majú podporu integračných softwarov. Väčšina veľkých dodávateľov bezpečnostných systémov poskytuje podporu v aspoň jednom integračnom software. Samozrejme môže nastať prípad, že všetky technológie nebudú mať podporu pre ten istý integračný software. [2]



Obr. 27 Príklad architektúry integračného softwaru AlViS [2]

Softwarové spôsoby integrácie sú postavené na základe prepojenia pomocou komunikačnej zbernice a softwarových produktov nainštalovaných v externom PC (servery, klientskom PC) alebo autonómnej bezobslužnej centrály s potrebným SW vybavením. [30]

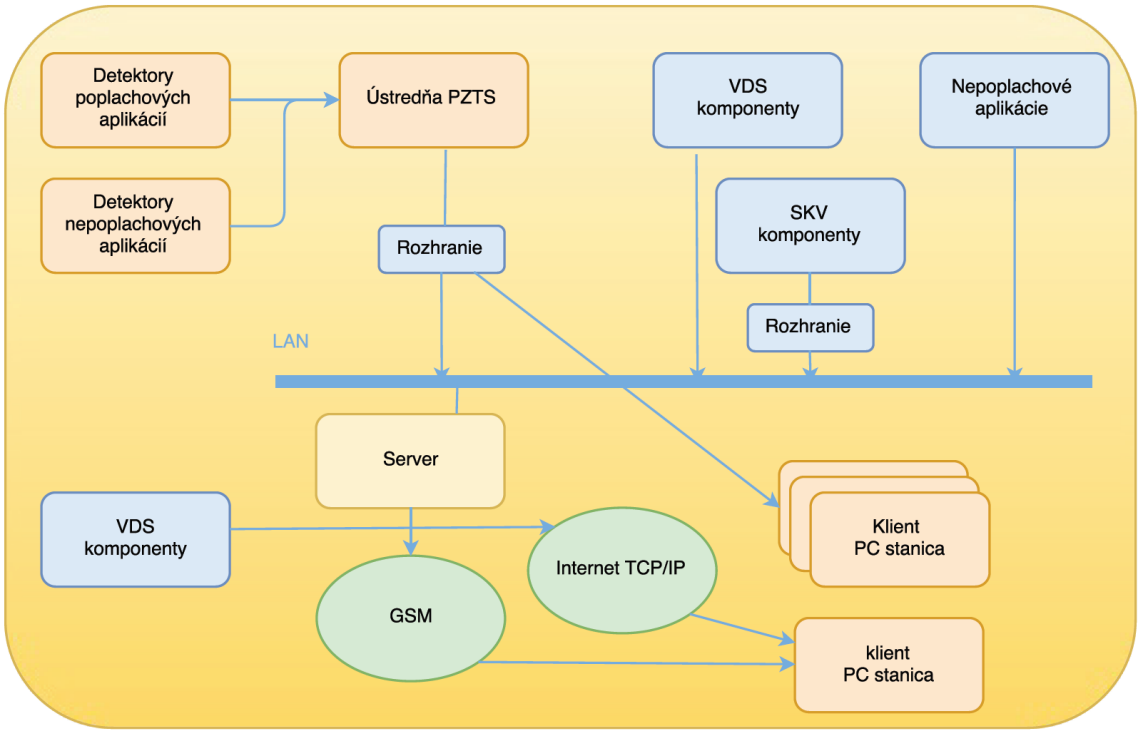
SW produkty poskytujú 3 základné funkcie:

- riadenie,
- správu,
- vizualizáciu. [30]

Jednotlivé aplikácie sú spravidla prepojené prostredníctvom Ethernetu (LAN, WAN) k hardwarovým komponentom (servery, klientske PC), v ktorých sú nainštalované potrebné SW.

Menej rozsiahle aplikácie využívajú prepojenie klienta s jednotlivými aplikáciami pomocou rozhrania RS232 alebo USB portu, kde spoločným prvkom je prístup užívateľa k jednotlivým funkciám cez PC alebo mobilné zariadenie. [31]

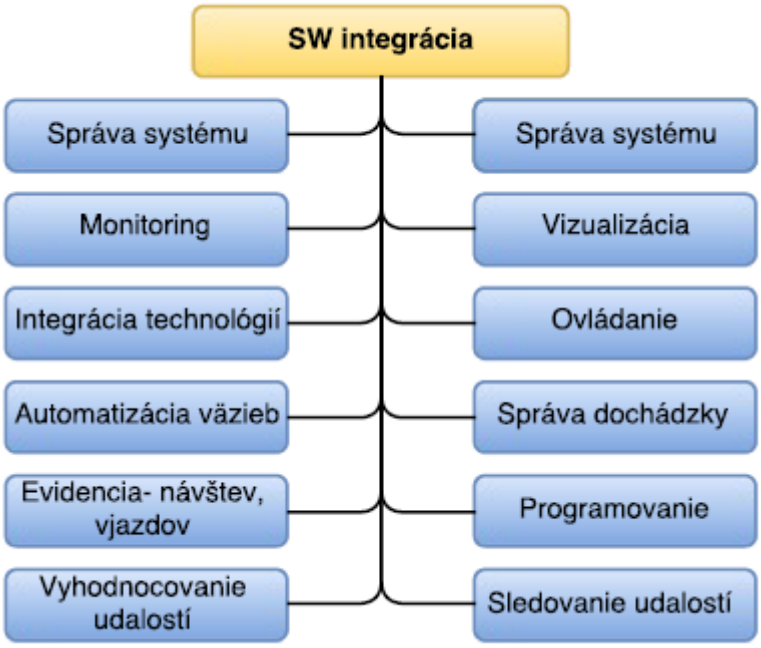
Na Obr. 28 je znázornená schéma zapojenia komponentov poplachových a nepoplachových aplikácií s využitím softwarového produktu ako integračného prvku.



Obr. 28 Schéma poplachových a nepoplachových aplikácií s využitím softwarového produktu a integračného prvku [30]

Všetky systémy sú jednotlivo pripojené k serveru, v ktorom je nainštalovaný nadstavbový SW prostredníctvom rozhrania a s využitím LAN. Čiarkovanou čiarou sú načrtnuté možnosti prepojenia ústredni PZTS alebo komponentov VDS, kde komunikujú priamo so sieťovými prvkami. Pomocou prístupových bodov sú pripojené k serveru. Klientske PC môžu byť pripojené cez LAN alebo vzdialene cez GSM a internetu. [30]

Funkcie SW produktov môžu zahŕňať integráciu vybraných činností alebo technológií (databázy, správy užívateľov, vizualizácie alebo nastavenie automatických väzieb). Na nasledujúcom obrázku (Obr. 29.) sú uvedené funkcie, ktoré môže poskytnúť integrácia. [30]



Obr. 29 Funkcie softwarových produktov v rámci integrácie poplachových systémov [30]

SW produkty pre podporu integrácie je možné rozdeliť na nasledujúce typy:

- **software ústrední**
- **software pre užívateľskú správu**
- **vizualizačné softwary**
- **integračný software systému budov** [30]

3.3.1 Software ústrední poplachových systémov

Ústredne (riadiace jednotky) môžu byť prepojené k PC diaľkovo alebo miestne za účelom naplnenia týchto základných funkcií:

- programovanie,
- sledovanie,
- vyhodnocovanie,
- archivácia udalostí. [30]

Doplnkové programy slúžia pre potrebu inštalačných a servisných spoločností. V tomto prípade je možné hovoriť o integrácii z pohľadu centrálneho vyhodnocovania archivácií udalostí ústrední, ktorá môže byť HW prepojená s inými systémami. Prepojenie ústrední môže byť prostredníctvom:

- modemu, telefónnej linky,
- rozhrania LAN/WAN,
- GPRS,
- sériového rozhrania. [30]

3.3.2 Software pre užívateľskú správu

SW pre užívateľskú správu umožňuje vytvorenie užívateľských nastavení riadiacej jednotky (ústredne alebo centrály) pripojenej k systému. Tieto programy sú najčastejšie využívane pri prepojení PZTS s SKV. Dokážu obohatiť základné funkcie (vyhodnocovanie, sledovanie, archivácia) o radu možností ako:

- nastavenie užívateľských profilov,
- vytvorenie popisov subsystémov, zón a terminálov,
- vytvorenie časových rozvrhov prístupu,
- pridelenie a evidenciou identifikačných prvkov,
- filtrovanie histórie udalostí. [30]

Tieto SW nie sú dodávané len pre PC rozhranie, ale aj pre komunikačné prostredie telefónov a tabletov. Umožňujú:

- zobrazenie stavu PZTS,
- stav zón,
- signalizáciu poplachov a porúch,
- ovládanie systému,
- ovládanie programovateľných výstupov. [30]

3.3.3 Vizualizačné softwary

Vizualizačný SW je druh integrácie, ktorý má oproti už spomínaným typom, možnosť vytvárať vizualizáciu stavu v reálnom čase, priestore (v závislosti od pôdorysu) a komponentov. Operátor, ktorý riadi tento systém je schopný sledovať a riadiť všetky procesy v danom užívateľskom prostredí. V tomto prostredí je možné previesť nasledujúce možnosti:

- zapnutie/vypnutie strážených subsystémov alebo zón,
- otvorenie dverí,
- zamknutie dverí,

- zapnutie kamier sledovaného priestoru,
- otáčanie kamier,
- aktiváciu inteligentných funkcií kamier (napr. sledovanie objektu),
- ovládanie PGM výstupov.
- spúšťanie externých aplikácií
- manipulácia s históriou udalostí (vyhľadávať, filtrovať, exportovať logy udalostí, atď.). [32]

Tento typ je ideálny pre VDS a to z dôvodu výbornej prehľadnosti, čo je výhodné v mnohých možnostiach využitia nadštandardných kamier a intuitívneho systému.

3.3.4 Integračný software systému budov

Bezpečnostné systémy môžu byť prepojené s ostatnými systémami prostredníctvom nadstavbových SW produktov nainštalovaných na serveri. Táto integrácia je ovládaná pomocou klientskeho PC cez webový prehliadač. Systémy sú najčastejšie prepojené v rámci LAN. Integračný SW určuje nadstavbová doplnková služba umožňujúca:

- nastavenie automatických väzieb medzi systémami,
- vizualizácia systému,
- lokálne a vizuálne ovládanie,
- správa systému a užívateľov,
- kontrola činnosti operátorov,
- správa dochádzky s nevážnosťou na mzdový systém,
- definícia role a prác užívateľa. [32]

Pri výpadku integračného SW nesmie dôjsť k negatívnemu ovplyvneniu poplachových a nepoplachových systémov. Pre zabezpečenie tejto situácie je vhodné systémové väzby zabezpečiť už na HW úrovni. Integračný SW je väčšinou zložený zo samostatných modulov(PZTS, VDS, SKV, atď.), ktoré je možné kombinovať. Tento SW môže spĺňať väčšinu funkcií SW produktov v rámci integrácie poplachových systémov, čo je zobrazené na Obr. 29. Medzi užívateľov integračného je možné na základe práv klasifikovať funkcie:

- užívateľ,
- recepčný,
- operátor,
- spracovateľ,

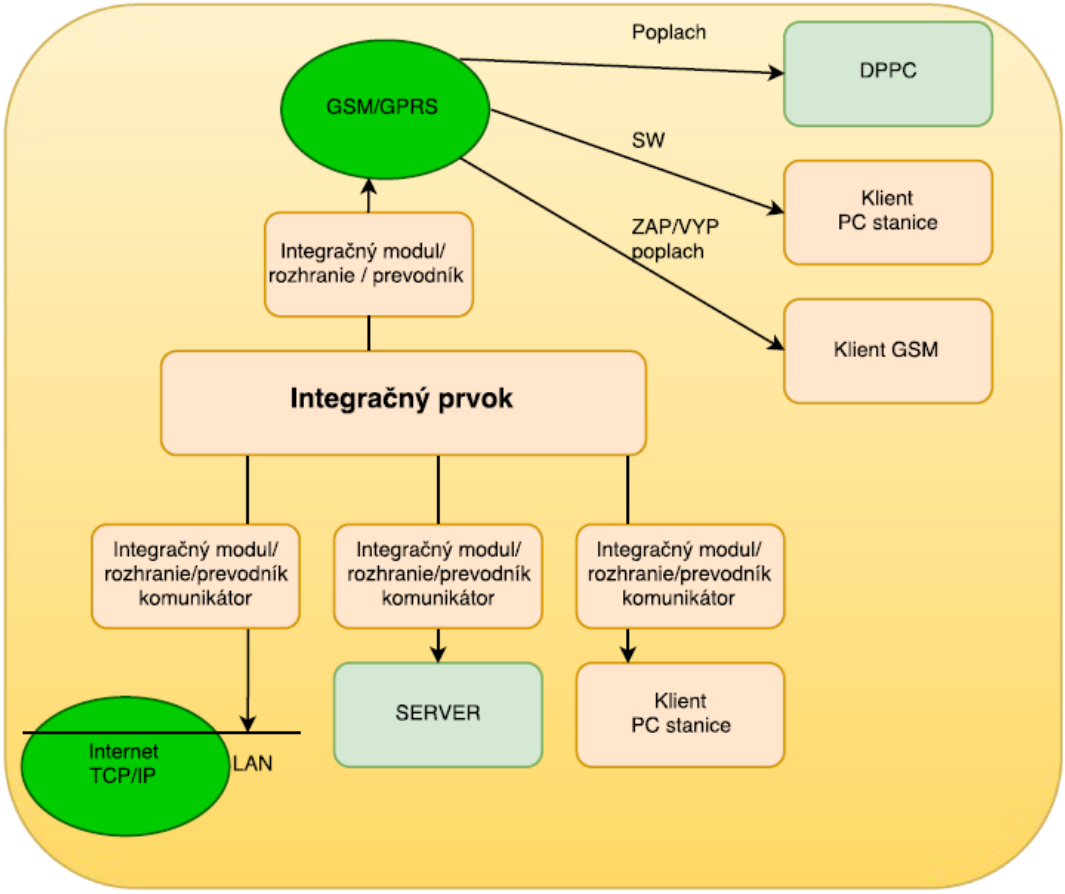
- schvaľovateľ,
- správca. [32]

3.3.5 Integračné moduly pre podporu softwarovej integrácie

Integračné moduly ako súčasti integrovaného systému slúžia k zabezpečeniu technického prepojenia poplachových systémov v rámci:

- vzájomnej integrácie poplachových systémov,
- integrácie nepoplachovými aplikáciami,
- pripojenie k centrálnej riadiacej jednotke. [30]

Realizácia integračného modulu je využívaná medzi internou zbernicou a štandardným rozhraním komunikačného prvku (RS232, LAN, GSM). Na Obr. 30 sú znázornené možnosti aplikácie integračných modulov. [30]



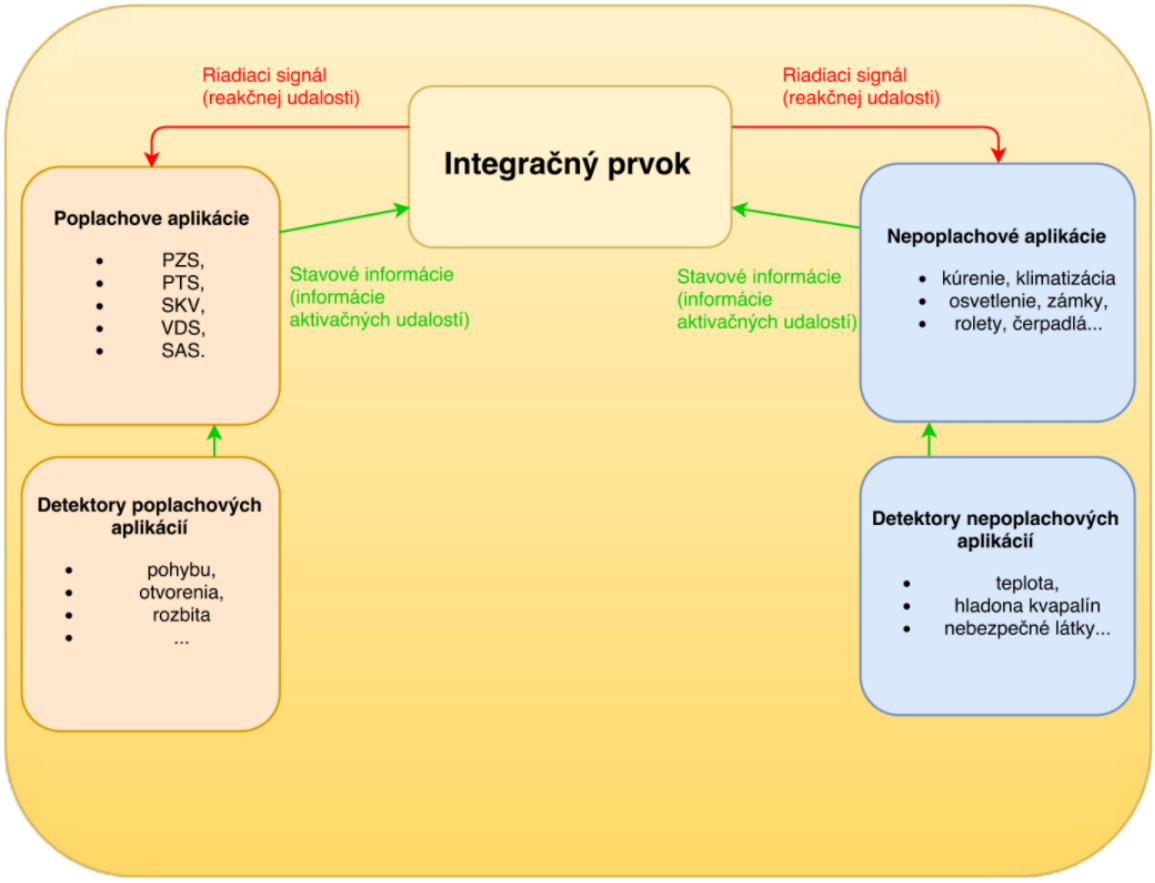
Obr. 30 Možnosti aplikácie integračného modulu v spolupráci s ústredňou PZTS [30]

3.3.6 Návrh funkcií integrovaných poplachových systémov

Hlavnou funkciou hardwarovej a softwarovej integrácie je nastavenie vzájomných väzieb medzi jednotlivým integrovanými aplikáciami. Podstatou je stanovenie prehľadu:

- aktivačných udalostí (na základe udalostí vyvolávajú reakčné udalosti),
- reakčné udalosti (napr. poplach vniknutia vyvoláva zapnutie osvetlenia).

Na Obr. 31 je znázornená schéma základných väzieb v rámci integrácie, kde prenos stanovených informácii medzi jednotlivými aplikáciami a riadiacim prvkom pôsobí ako odozva generovaného signálu a odoslanie riadiaceho signálu, ktorého následkom je reakčná udalosť v ovládanom zariadení. [30]



Obr. 31 Schéma základných väzieb v rámci integrácie poplachových a nepoplachových aplikácií [30]

3.4 Čiastkový záver

Táto kapitola sa zaoberá technickou normou ČSN EN CLC/TS 50398 cez technické a systémové požiadavky pre integráciu. Spomína všetky možné technicko-technologické možnosti synergie VDS a SKV. Technické spôsoby prepojenia jednotlivých aplikácií sú rozdelené na dve základné skupiny hardwarové spôsoby integrácie a softwarové systémy integrácie. Efektívnosť jednotlivých druhov riešení závisí na tom, aké predstavy má užívateľ, a o akú veľkosť objektu sa jedná.

Na základe zistených informácií je najlepšou možnou alternatívou softwarová integrácia, keďže SKV a aj VDS využívajú svoje vizualizácie platformy na osobitnú správu. Ideálnou možnosťou je softwarová integrácia cez integračný software systémov budov, ktorá funguje na základe softwarových produktov nainštalovaných na serveri a je ovládaná cez klientsky PC. Použitý integračný software vytvorí veľké množstvo nových výhod pre danú výrobnú spoločnosť.

II. PRAKTICKÁ ČASŤ

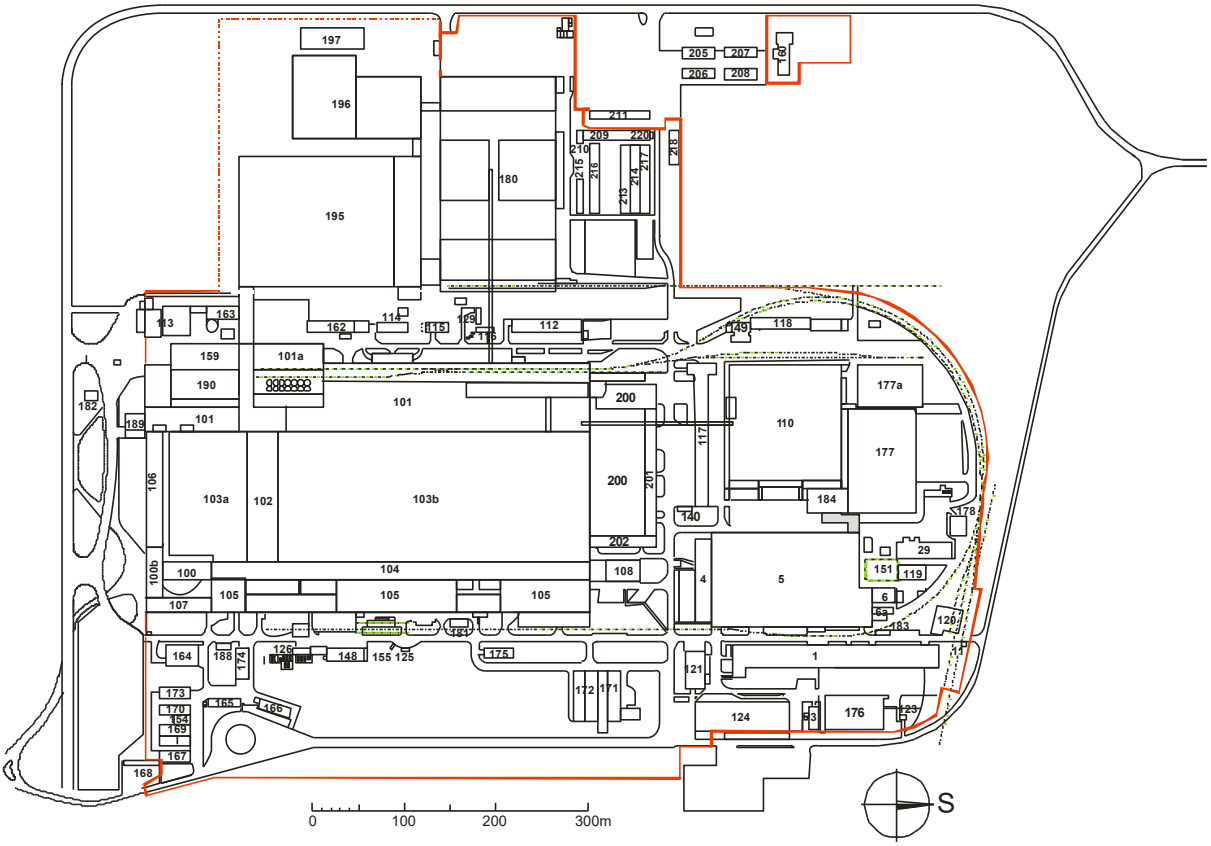
4 SYSTÉM KONTROLY VSTUPU A DOHĽADOVÝ SYSTÉM VÝROBNEJ SPOLOČNOSTI

Hlavným účelom tejto kapitoly je zhrnúť súčasné informácie o spoločnosti, s primárnym zameraním na systém kontroly vstupu a videodohľadového systému, a zároveň určiť možné prepojenie týchto systémov. Prepojenie predstavuje skvalitnenie zabezpečenia areálu prostredníctvom synergie súčasného SKV so súčasným VDS, ktoré spolu vytvoria tzv. videodohľadový prístupový systém. Využitie systému bude primárne zamerané na vstupy a výstupy do objektu a zlepší:

- evidenciu osôb pri vstupe/výstupe,
- evidenciu vozidiel pri vjazde/výjazde do objektu.

4.1 Súčasné informácie o spoločnosti

Práca reálne rieši integráciu SKV a VDS rozsiahlej výrobnej spoločnosti medzinárodného výrobcu, ktorý je zameraný na výrobu automobilových komponentov. Výrobná spoločnosť sa nachádza na území moravského kraja v Českej republike. Uvedená spoločnosť má dobrú taktickú polohu a disponuje železničnou traťou, cestnou dopravou obohatenou o blízkosť diaľnice a malým letiskom. Rozmanitosť typov dopravy hovorí o príslušných opatreniach vstupov, ktoré sú pre danú spoločnosť nevyhnutné. Areál sa rozlieha na ploche 738 m^2. Tu je možné nájsť výrobné haly, sklady, vrátnice, administratívne budovy a mnoho ďalších budov súvisiacich s výrobou. Veľký obrat osôb spôsobujú okrem 4500 aktívnych zamestnancov výrobnej spoločnosti aj iné nájomné spoločnosti, ktoré v súčasnej dobe pracujú na budovaní a rekonštrukcií budov v areáli.



Obr. 32 Pôdorys celého areálu výrobnej spoločnosti

Tým, že sa jedná o rozsiahlu výrobnú spoločnosť je kladený veľký dôraz na bezpečnosť. Pri veľkom množstve zamestnancov je náročné mať prehľad a monitorovať dochádzku. Preto výrobná spoločnosť využíva ako systém kontroly vstupu systém AKTION a ako video - dohľadový systém ATEAS. Tieto software samostatne fungujú spoľahlivo, ale je možné z nich vytvoriť efektívny integrovaný systém, ktorého návrh je hlavnou podstatou diplomovej práce.

4.1.1 Prístupové práva

Výrobná spoločnosť má prístupové práva ošetrené v internej smernici o evidencií osôb a pracovnej doby pre vjazdy a výjazdy do objektu. Pre získanie vstupu do areálu, musí byť príslušníkom bezpečnostnej divízie vyhotovená identifikačná čipová karta. V danom objekte sú identifikačné karty rozdelené podľa druhu použitia na:

- Osobná karta zamestnanca,
- Karta kontraktor,
- Krátkodobá osobná karta pre zamestnancov externých spoločností,

- Karta agentúrneho zamestnanca,
- Návštevná osobná karta,
- Karta osobného vozidla,
- Karta nákladného vozidla.

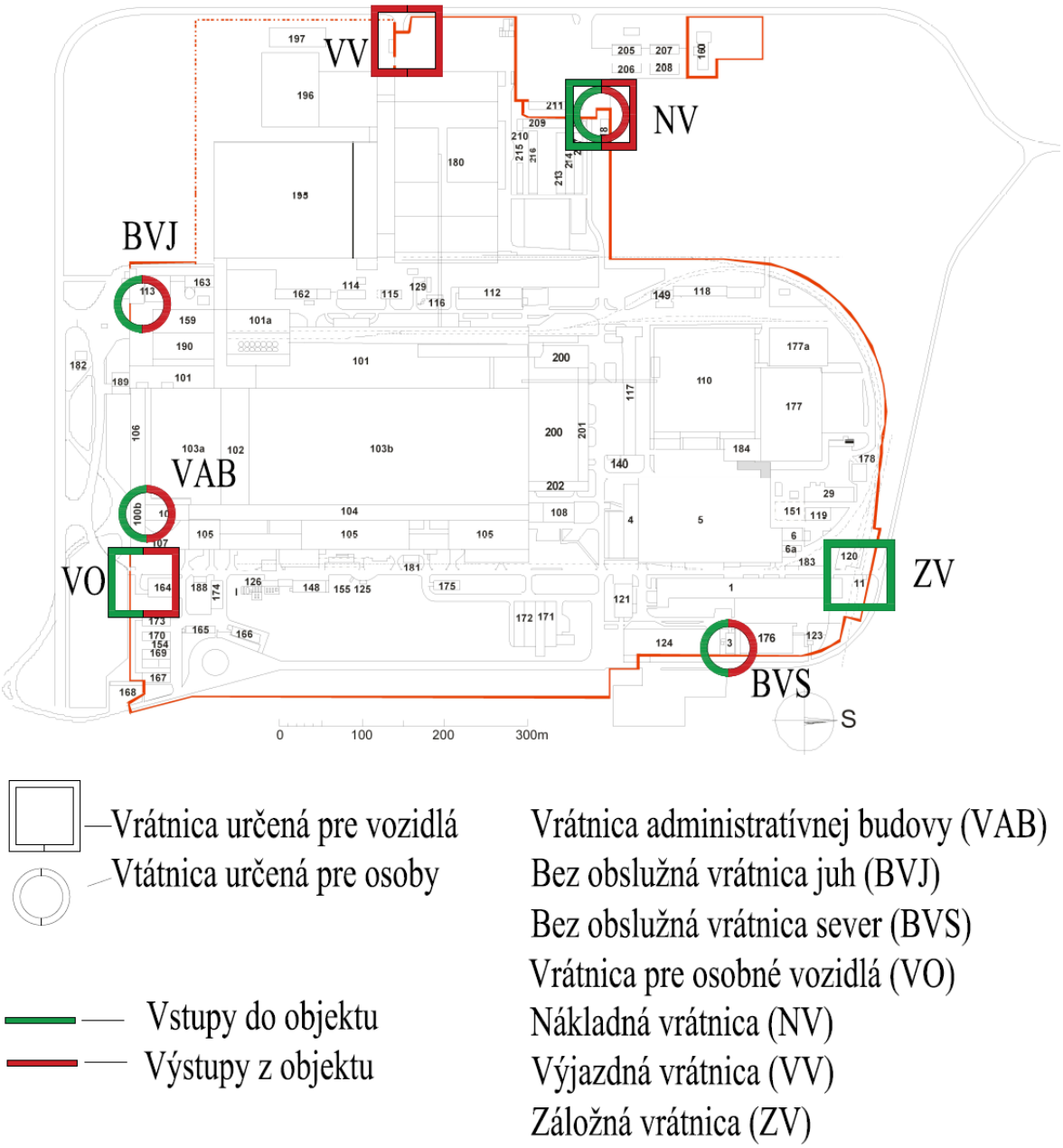
Každá z uvedených typov kariet má príslušné prístupové práva, ktoré sú nastavené administrátorom bezpečnostnej divízie. Prístupové práva sú vytvorené na základe účelu pôsobenia osoby v objekte. Každá osoba v objekte je povinná zaznamenať svoj vstup/ výstup z objektu prostredníctvom identifikačnej karty. Vstup a výstup je zaznamenaný jednoduchým priložením identifikačnej karty k terminálu. Pri opustení objektu je nutné na termináli zvoliť jeden z uvedených dôvodov. Identifikačné karty sú neprenosné a je prísny zákaz ich požičiavania. Tieto pravidlá platia aj pre zamestnancov externých firiem, ktoré sídlia v areáli spoločnosti, ale neplatia pre: Hasičský záchranný zbor (HZS), Pracovníkov HZSp, Pracovníkov energetiky, políciu ČR, Zdravotnú záchrannú službu (ZZS), Krajské hygienické stanice a Kontrolné orgány štátnej správy.

4.1.2 Prístupové body

Prístupovým bodom je charakterizované akékoľvek usporiadanie prvkov, ktoré spolupracujú pri vstupe/výstupe do objektu. Výrobná spoločnosť disponuje ôsmimi prístupovými bodmi, ktoré je možné rozdeliť do dvoch skupín:

- vstupy/výstupy určené pre osoby:
    - Vrátnica administratívnej budovy (VAB)
    - Bezobslužná vrátnica juh (BVJ)
    - Bezobslužná vrátnica sever (BVS)
- Vstupy/výstupy určené pre dopravné vozidlá
    - Vrátnica pre osobné vozidlá (VO)
    - Nákladná vrátnica západ s bezobslužným turniketom pre osoby (NV)
    - Výjazdná vrátnica (VV)
    - Záložná vrátnica (ZV)

Všetky uvedené miesta prístupu sú vyznačenie na obrázku č. 33 , kde zeleno sú vyznačené vrátnice pre osoby a červenou pre dopravné vozidlá.



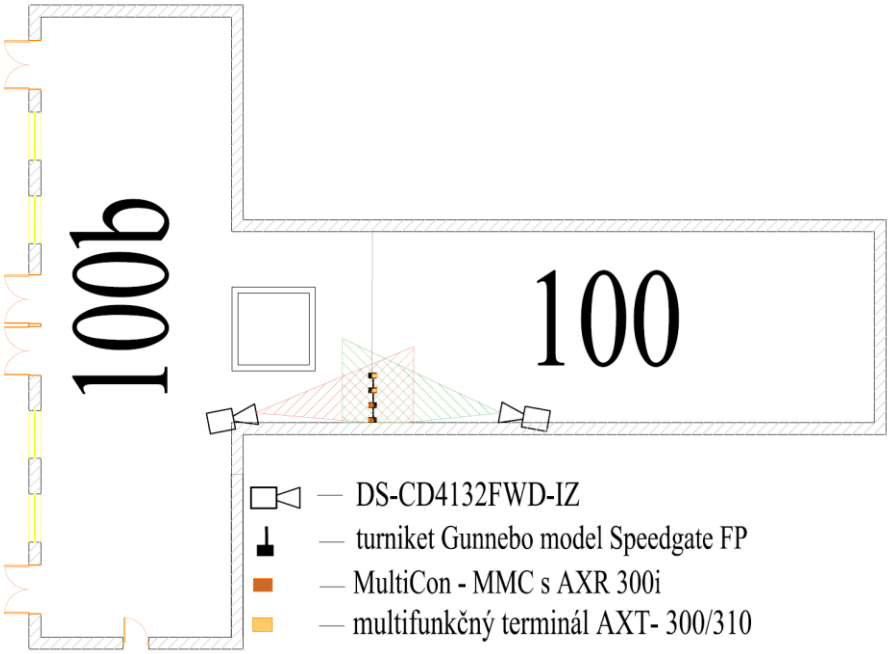
Obr. 33 Pôdorys v vyznačenými vrátnicami

4.1.2.1 Vrátnica administratívnej budovy (VAB)

Vrátnica administratívnej budovy je umiestnená priamo vo vnútri administratívnej budovy (označená č.100). Tento vstup je využívaný najmä pre zamestnancov a návštevníkov spoločnosti. Táto vrátnica je najvyužívanejšou. Denne zaznamenáva okolo 5000 priechodov osôb.

Prístupový bod je vybavený týmto hardwarom:

- Systém kontroly vstupu
  - 4x Mul
  - tiCon (MMC) s AXR 300i -(vstupy)
  - multifunkčný terminál AXT- 300/310-(výstupy)
- Dohľadový videosystém
  - 2x Hikvison DS-CD4132FwD-IZ



Obr. 34 vrátnica administratívnej budovy

Súčasťou prístupového bodu je aj informačný pult so zamestnancami bezpečnostnej divízie. Títo zamestnanci sú k dispozícii 24 hodín denne.

4.1.2.2 Bezobslužná vrátnica juh (BVJ)

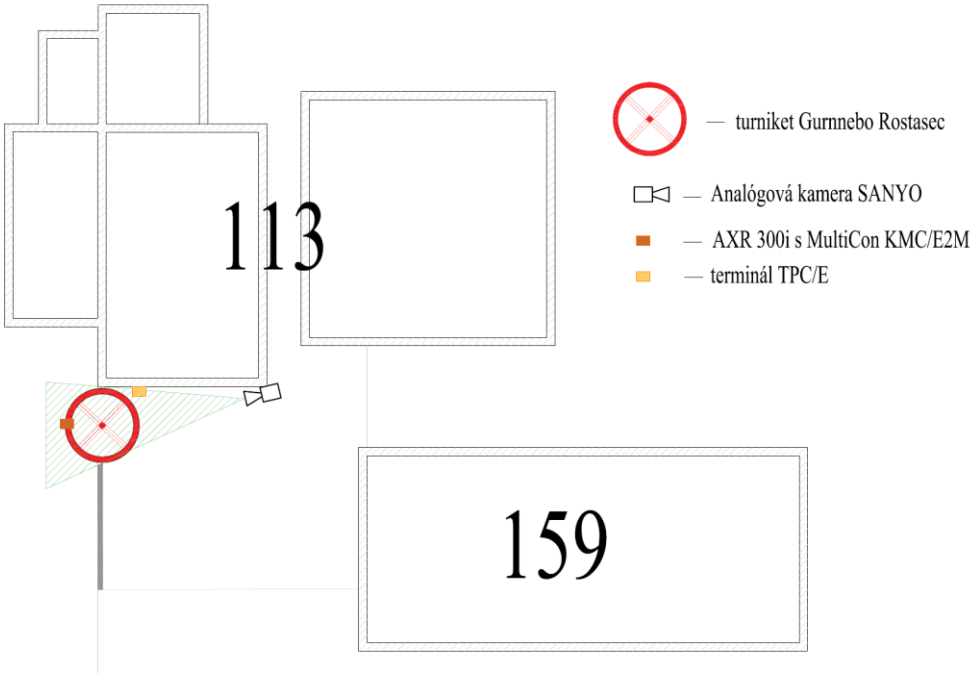
Vrátnica je umiestnená v južnej časti objektu. konkrétne medzi podnikovou predajňou a výrobnou halou. Využívaná je na príchody a odchody zamestnancov výrobnej spoločnosti a externých firiem v objekte. Vrátnica je určená len na prechod osôb a disponuje:

- Systémom kontroly vstupu:
  - turniket Gurnnebo Rostasec
  - MultiCon KMC/E2M (vstupy)
  - AXR 300i (vstupy)

- terminál TPC/E (výstup).

- Dohľadovým videosystémom:
  - Analógova kamera SANYO

Analógová kamera SANYO disponuje rozlíšením 640x 480p a spolupracuje so softwarom DEDICATED-MICROS. Jedná sa o zastaralý systém, ktorý nie je za integrovateľný. Dnes sa už pracuje na projekte o inovácií tohto systém s prechodom na IP kamery so softwarom ATEAS.



Obr. 35 Bezobslužná vrátnica juh

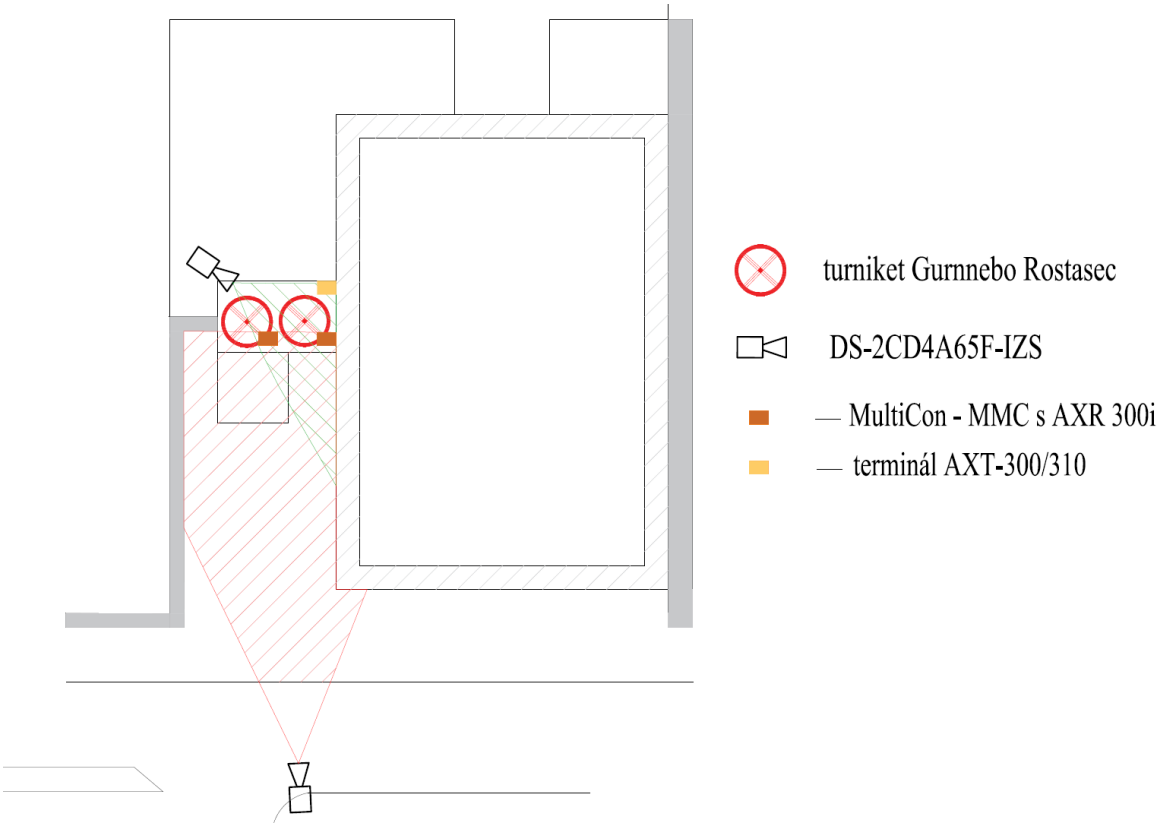
Pred vstupom sú vybudované dve pomerne nové zamestnanecké parkoviská, ktoré sú tiež dostatočne zabezpečené VDS (ATEAS). Priemerný denný prechod vrátnice je niečo okolo 1300 osôb.

4.1.2.3 Bezobslužná vrátnica sever (BVS)

Vrátnica je umiestnená v severovýchodnej časti objektu. Tak ako predošlá vrátnica je aj táto určená pre príchody a odchody zamestnancov výrobnej spoločnosti a externých zamestnancov. Táto vrátnica sa vyznačuje tým, že okrem parkoviska je vedľa umiestnená aj úschovňa bicyklov. Denná priechodnosť vrátnice je 1600 osôb, čo výrazne ovplyvňuje to, že vrátnica je v blízkosti autobusového nádražia a vlakovej stanice.

Vrátnica je zabezpečená:

- Systémom kontroly vstupu:
  - 2x turniket Gurnnebo Rostasec
  - AXR 300i,
  - MultiCon- MMC, (vstupy)
  - terminál AXT- 300/310 (výstupy).
- Dohľadovým videosystémom:
  - DS-2CD4232FWD-IS
  - DS-2CD4A65FIZS



Obr. 36 Bezobslužná vrátnica sever

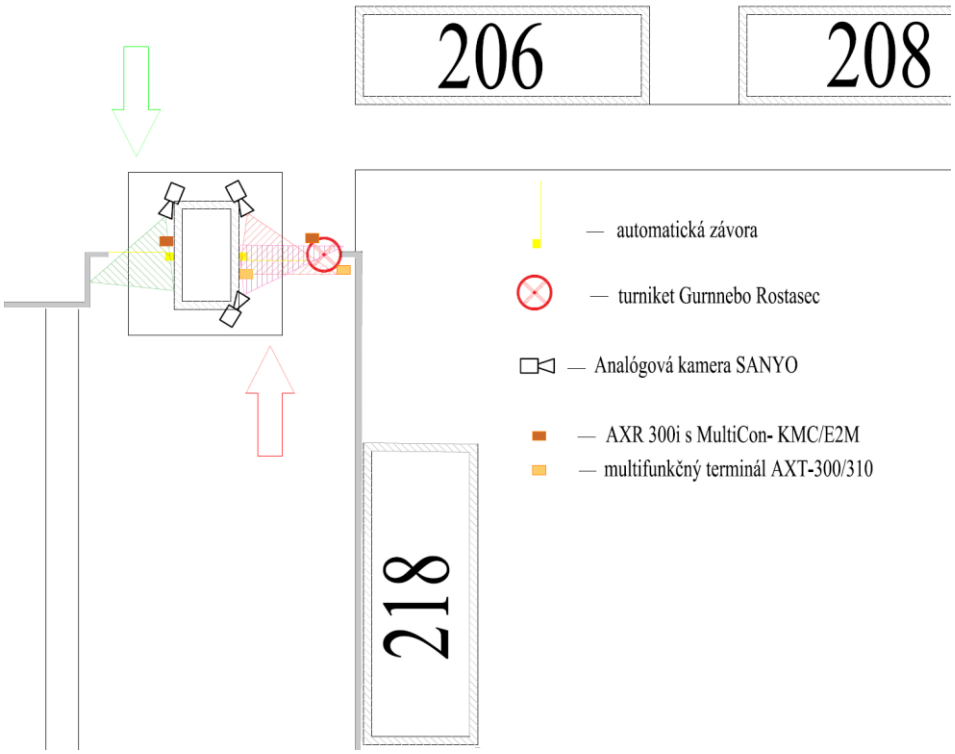
Súčasťou vrátnice je aj obytná bunka, v ktorej však nie je nutná 24 hodinový fyzická ostraha. Turnikety fungujú autonómne a skúsenosti firmy hovoria o ich spoľahlivosti s nízkymi nákladmi na údržbu.

4.1.2.4 Nákladná vrátnica s bezobslužným turniketom západ (NV)

Vrátnica sa nachádza v západnej časti objektu primárne určená pre vozidlá, ale jej súčasťou je aj jeden bezobslužný turniket. Ako už vyplýva z názvu, táto vrátnica je využívaná

nákladnými vozidlami, a to hlavne na ich nakladanie a vykladanie. Súčasťou vrátnice je aj budova, v ktorej sa nachádzajú príslušní zamestnanci, ktorí vydávajú karty a kontrolujú evidenciu vozidiel. Vrátnica funguje 24 hodín denne. Turniket denne zaznamená okolo 340 prechodov, nízky počet prechodov spôsobuje lokalita a fakt, že slúži ako doplnok nákladnej vrátnici. Vrátnica je vybavená:

- Systémom kontroly vstupov:
  - 2x automatická závora
  - turniket Gurnnebo Rostasec
  - AXR 300i,
  - kontrolér MultiCon- KMC/E/2M
  - multifunkčný terminál AXT- 300/310
- Dohľadovým videosystémom:
  - 3x AXIS P1435-LE



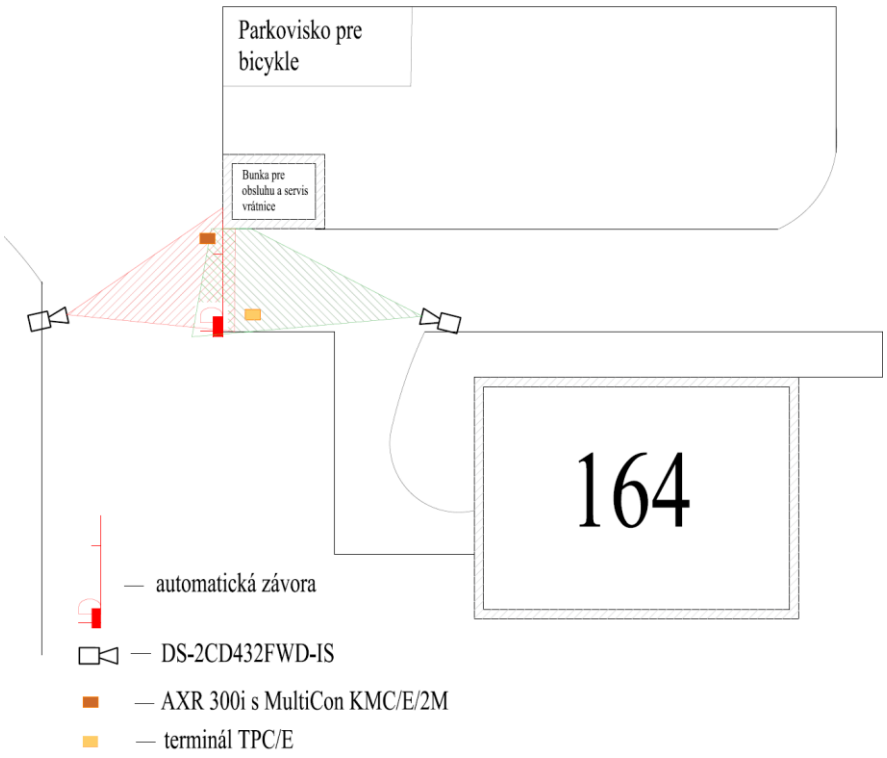
Obr. 37 Nákladná vrátnica s bezobslužným turniketom západ

4.1.2.5 Vrátnica pre osobné vozidlá (VO)

Vrátnica je situovaná v juhovýchodnej časti areálu vedľa administratívnej budovy. Táto vrátnica je určená pre vjazd a výjazd osobných vozidiel, jedná sa hlavne o automobily

managementu výrobnej spoločnosti. Identifikácia prebieha prostredníctvom čipovej karty vozidla a priradených prístupových práv. Vrátnica je zložená zo:

- Systému kontroly vstupov:
  - automatickej závory
  - AXR 300i
  - kontrolér MultiCon- KMCE//2M (vstup)
  - terminál TPC/E (výstup).
- Dohľadovým videosystémom:
  - DS-2CD432FWD-IS



Obr. 38 Vrátnica pre osobné vozidlá

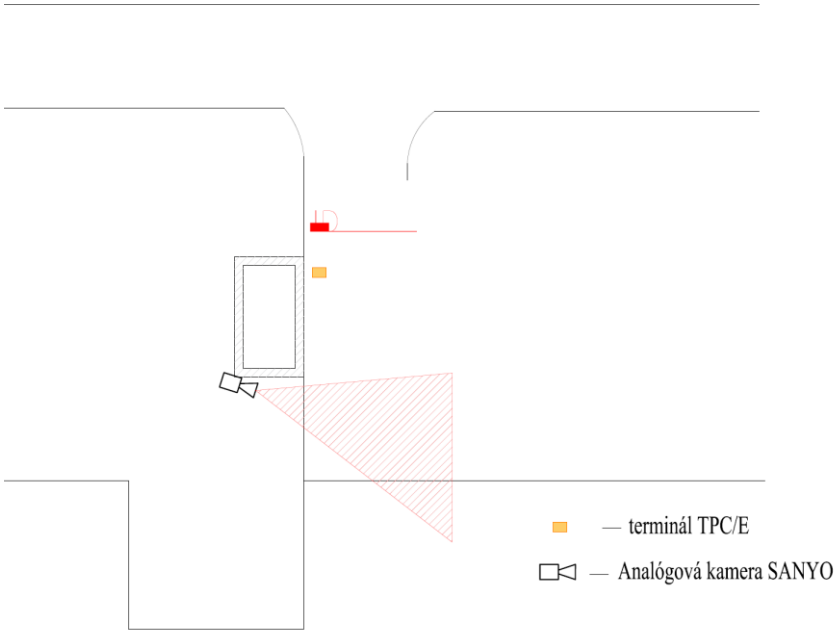
Súčasťou vrátnice je aj bunka, ktorá slúži na ručnú obsluhu a servis. Vrátnica je bezobslužná a funguje plne automaticky. Nie je nutný žiadny zamestnanec fyzickej stráže na obsluhu.

4.1.2.6 Výjazdná vrátnica (VV)

Vrátnica sa nachádza v západnej časti objektu, kde je situovaná v blízkosti stanovišťa určeného na nakládku a parkoviska pre nákladné vozidlá. Jej hlavnou funkciou je odľahčenie premávky nákladnej vrátnice, pričom je určená iba na výjazd nákladných vozidiel

s obmedzenou dobou chodu (od 7:00 do 15:00). Na vrátnici v bunke sa nachádza príslušník bezpečnostnej divízie, ktorý dohliada na prevoz vrátnice. Vrátnica obsahuje tento hardware:

- Systém kontroly vstupu:
  - automatickej závora
  - kontrolér MultiCon- KMC/2M
  - terminál TPC/E
- Dohľadový videosystém:
  - Analógová kamera SANYO



Obr. 39 Výjazdná vrátnica

Ako už bolo spomenuté analógová kamera SANYO disponuje srozlíšením 640x 480p a spolupracuje so softwarom DEDICATED-MICROS. Jedná sa o zastaralý systém, ktorý nie je za integrovateľný. Aj v tomto prípade je plánovaná inovácia na IP kameru, ktorá bude pracovať pod softwarom ATEAS ako väčšina kamier v objekte.

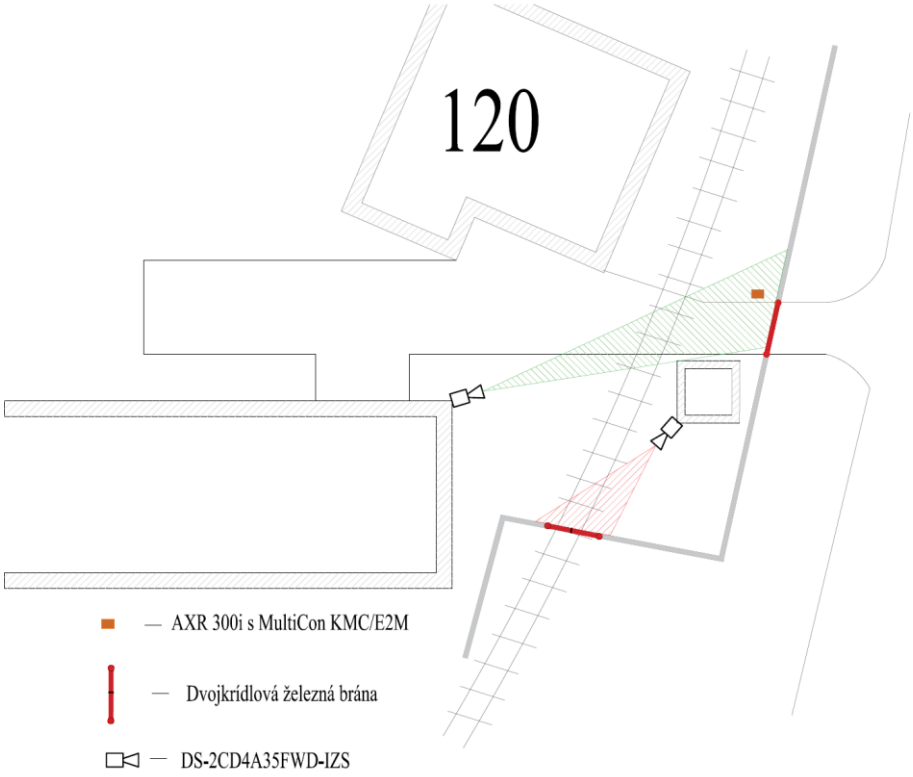
4.1.2.7 Záložná vrátnica (ZV)

Vrátnica je situovaná v severnej časti objektu a je vytvorená iba pre vstup do objektu. Slúži ako záložná vrátnica pri preťažení nákladnej vrátnice. Súčasťou tejto vrátnice je aj železničný prechod objektom, ktorý je tiež monitorovaný prostredníctvom VDS: Vrátnica obsahuje tento hardware:

- Systém kontroly vstupu:

- dvojkrídlová železná brána
- AXR 300i
- kontrolér MultiCon- KMC/2M

- Dohľadový videosystém:
  - DS-2CD4A35FWD-IZS



Obr. 40 Záložná vrátnica

4.2 AKTION

Aktion je obchodnou značkou českej spoločnosti EFG CZ spol. s. r. o., ktorá sa zaoberá výrobou a implementáciou dochádzkových, prístupových a ďalších elektronických systémov. V Európe je zaradený medzi špičku v riešení dochádzkových a prístupových systémov. Jeho primárnou funkciou je fyzické zabezpečenie objektu prostredníctvom nastavenia oprávnení miest prístupu a evidenciou pohybu osôb v objekte. Výhodou tohto systému je:

- modulárne riešenie,
- neobmedzenosť počtu prístupových bodov,
- integrácia s inými systémami,
- vizuálne rozhranie,

- funkcia antipassback,
- prepojenie so serverom.

Systém Aktion umožňuje ovládanie dverí , zámkov, závor, turniketov a automatických dverí na základe vopred stanovených oprávnení. Oprávnenia sú v danej spoločnosti overované prostredníctvom čipových kariet. [33]

4.2.1 Aktion 5.1

Aktion 5.1 je jeden z viacerých produktov spoločnosti Aktion. Pre evidenciu prístupu a dochádzky využíva bezkontaktné a biometrické technológie, ktoré zaručujú maximálnu spoľahlivosť a bezpečnosť. Evidencia kontroly prístupu je zaistená sieťovým prepojením bezkontaktnými a biometrickými snímačmi a umožňuje elimináciu vstupov nepovolaných osôb, monitorovanie pohybu ľudí, poprípade príjazdy a odjazdy vozidiel. Snímače pracujú on/off-line a sú prepojené s riadiacim PC, ktorý vyhodnocuje načítané údaje. Tento systém vyhodnocuje záznamy , ktoré zamestnanci zadajú pomocou klávesníc terminálov alebo priložených kariet, či odtlačkov prstov. Tým uľahčuje a urýchľuje prácu pracovníkom mzdových ústredí, vedúcim prevádzky, a aj všetkým ostatným zamestnancom. [33]

Funkcie:

- jedna karta/odtlačok nahradia všetky kľúče,
- prehľad osôb v objekte,
- urýchlenie chodu vrátnic,
- určenie prístupových práv (v čase a priestore),
- ovládanie turniketov a závor,
- blokácia v prípade strát,
- ovládanie 250 dverí súčasne,
- sledovanie dochádzky,
- import dát (DBF, XLS, TXT),
- možnosť zadania dôvodu odchodu,
- úprava systému podľa požiadaviek zákazníka [33]

4.2.2 Hardwarová časť

Výrobná spoločnosť disponuje ôsmimi miestami prístupu, ktoré sú zabezpečené týmto hardwarom:

- Terminál ProfiCon/Ethernet,
- Multifunkční terminál AXT-300/310,
- Kontrolér MultiCon – KMC/E/2M,
- Modul MultiCon – MMC.

4.2.2.1 Terminál ProfiCon/Ethernet

Terminál ProfiCon/Ethernet je možné využiť aj ako samostatnú riadiacu jednotku. V termináli je integrovaný bezkontaktný snímač typu APR-P20/USB s dosahom v rozmedzí 5 až 10 cm. Súčasťou zariadenia je aj sedempalcový dotykový display s rozlíšením 800 x 480. Pre komunikáciu poskytuje 2x Ethernet port, 2x DB9 a RS232. [34]

Obr. 41 Terminál ProfiCon/Ethernet [34]

4.2.2.2 Multifunkční terminál AXT-300/310

Multifunkční terminál AXT-300/310 má integrovanú 1,3 Megapixelovú kameru a je založený na platforme priemyslového PC (86). V termináli môžu byť integrované dva typy snímačov a to buď Unique/HS (AXT-300) alebo Mifare (AXT-300). Tento je možné použiť aj ako

samostatnú riadiacu jednotku. Zariadenie je vybavené osempalcovým dotykovým displejom a ponúka tieto typy komunikačného rozhrania: 2x Ethernet, RS 485, a 4x USB a RS 232. [35]

Obr. 42 Multifunkční terminál AXT-300/310 [35]

4.2.2.3 AXR 300i

Autonómny bezkontaktný snímač identifikačných kariet. S využitím Aktion NEXT je možné prístupové oprávnenie kariet programovať z čelného panelu bez nutnosti pripojenia.

- Kapacita 255 identifikátorov.
- Pamäť pre 4000 udalostí.
- 125 KHz Frekvencia čítania (jedinečná H4100).
- Odčítacia vzdialenosť 3 cm.
- 4 programovacie tlačidlá.
- Rozhranie USB na čítanie pamäti udalostí
- Predné kryty v piatich farebných odtieňoch
- Možnosť pripojenia externých snímačov Wiegand
- Trojfarebná LED a zvukový á signalizácia. [36]

Obr. 43 AXR 300i [36]

4.2.2.4 Kontrolér MultiCon – KMC/E/2M

KMC/E/2M je samostatná riadiaca jednotka s rozšírenou pamäťou pre rozsiahle inštalácie. V spolupráci s MMC je využiteľná aj pre najnáročnejšie aplikácie. Na sekundárnu linku RS 232 je možné pripojiť až 15 modulov MultiCon (MMC) alebo terminálov MultiCon (TMC/L). Kontrolér je ešte možné obohatiť o dva bezkontaktné snímače alebo 2 terminály s dotykovým displejom (TPC/L). Kapacita pamäti udalostí závisí na pripojených podriadených moduloch, počte nahraných osôb alebo bázach mien a počte podmienených kariet. Pre komunikáciu môžu byť využité rozhrania ethernet so sekundárnou linkou RS 485. [37]

Obr. 44 Kontrolér MultiCon – KMC/E/2M [37]

4.2.2.5 Modul MultiCon – MMC [38]

MMC je rozširujúci modul I/O pre kontrolér KMC/E. Tento modul nie je možné použiť ako samostatnú riadiacu jednotku. Iba v kombinácií s KMC. Zariadenie je vyvážené vstupmi pre dverný kontakt, tlačidlo či tamper. Vďaka funkcií Massanger dokáže definovať rozdiel medzi vstupmi a výstupmi, a zároveň informovať tak o rôznych situáciách. Samozrejmosťou je funkcia Antipassback. Ako komunikačné rozhranie využíva RS 485.

Obr. 45 Modul MultiCon – MMC [38]

4.3 ATEAS

ATEAS Security je komplexný videodohľadový systém, zameraný na profesionálne využitie potenciálu kamier. Otvorené štandardy umožňujú extrémny výkon, jednoduchosť a pokročilé funkcie. Tento software slúži ako:

- intuitívny dohľadový nástroj,
- správca aplikácií pre vzdialenú správu serveru,
- bezobslužný klient video steny. [39]

ATEAS patri medzi najvýkonnejšie videodohľadové systémy na trhu. Hlavne prostredníctvom jeho technológii ako sú grafické akcelerácie pre dohľadové stanice i mobilné zariadenia a rozpoznávanie ŠPZ vozidiel. Pod pojmom pokročilé funkcie ATAES rozumieme špecifické potreby zákazníka, a to od oblasti bezpečnosti a užívateľských funkcií až po multifunkčné scenáre udalostí. Platforma je otvorená všetkým výrobcom podporujúcich štandardov ONVIF, s ktorými je ATEAS oficiálne kompatibilný. Systém je ľahko integrovateľný so systémami v oblasti prístupových systémov a podnikových informačných systémov. [39]

4.3.1 Ateas 4.4.0

Edícia Ateas 4.4.0 je maximálne flexibilná. Má možnosť prepojenia ľubovoľného počtu kamier do systému podporovaného ľubovoľným počtom serverov. Vďaka technológií inteligentného záznamu a využitia inteligencie kamerových bodov je možné zaistiť efektivitu celého systému i pre veľmi vysokom počte kamier:

Funkcie:

- správa pohľadov kamier,
- určovanie funkcií jednej kamery (zobrazenie detailov, ukladanie snímok..),
- aktivácia externých zariadení,
- spolupráce s mapovým oknom,
- práca s videostenou,
- práca s užívateľskými tlačidlami,
- vyhľadávanie záznamu,
- denník poplachov,
- lokálna správa sekvencií,
- prehľad sekvencií. [39]

4.3.2 Hardwarová časť

4.3.2.1 Hikvison DS-CD4132FWD-IZ

Táto 3 megapixelová interiérová kamera od firmy Hikvison má rozlíšenie 2048 x 1536. Inteligentné LED diódy jej umožňujú viditeľnosť v noci až do 30m. Zariadenie je tiež vybavené vlastným úložným priestorom až 64GB (karta SD). [40]

Obr. 46 Hikvison DS-CD4132FWD-IZ [40]

Vlastnosti produktu:

- CMOS s progresívnym skenovaním 1/3 "
- Smart kodek
- 120 dB široký dynamický rozsah
- 3D digitálna redukcia šumu
- kompresia videa H.264/ MPEG4/ MJPEG
- Vstavaný slot micro SD/ SDHC/ SDXC až 64 GB
- Objektív s motorovým zoomom 2,8-12 mm
- Smart VQD/ inteligentná detekcia tváre/ inteligentná detekcia zvuku/ detekcia narušenia
- Dvojcestný zvuk
- 12VDC/ PoE [40]

4.3.2.2 Hikvison DS-2CD432FWD-IS

Táto 3 megapixlová IP kamera od firmy Hikvison je určená pre vonkajšie použitie a má rozlíšenie 2048x1536. IR LED ako pri predošlej kamere umožňuje vidieť v noci až do dĺžky 30 m. Takisto je vybavená pamäťovým slotom pre 64 GB SD kartu. Vstavaný ohrievač umožňuje používať kameru aj pri teplote – 40 stupňoch Celzia. [40]

Obr. 47 Hikvison DS-2CD432FWD-IS [40]

Vlastnosti produktu:

- CMOS s progresívnym skenovaním 1/3 "
- Smart kodek

- 120 dB široký dynamický rozsah
- 3D digitálna redukcia šumu
- kompresia videa H.264/ MPEG4/ MJPEG
- Vstavaný slot micro SD/ SDHC/ SDXC až 64 GB
- Objektív s motorovým zoomom 2,8-12 mm
- Smart VQD/ inteligentná detekcia tváre/ detekcia narušenia
- zabudovaný ohrievač (-40 ° C ~ 60 ° C (-40 ° F ~ 140 ° F)
- IP66 je určený na vonkajšie použitie
- 12VDC/ PoE [40]

4.3.2.3 Hikvison DS-2CD4A65F-IZS

Hikvison DS-2CD4A65F-IZS je 6 megapixlová s rozlíšením až 3072 x 2048p. Primárne je určená pre vonkajšie použitie. Vďaka IR LED diódy dokáže kamera vidieť do vzdialenosti až 50 m. Tak isto ako predošlé kamery obsahuje slot na micro SD/ SDHC/ SDXC kartu, ale s veľkosťou až 128 GB. [40]

Obr. 48 Hikvison DS-2CD4A65F-IZS [40]

Vlastnosti produktu

- 1/ 1,8 "CMOS s progresívnym skenovaním
- Funkcia deň/ noc s filtrom IR rezu
- Smart kodek
- digitálny širokouhlý dynamický rozsah
- 3D digitálna redukcia šumu
- Kompresia videa H.264 / MJPEG

- Vstavaný slot micro SD/ SDHC/ SDXC až 128 GB
- Objektív s motorovým zoomom 2,8-12 mm
- Inteligentná detekcia: detekcia narušenia, detekcia prieniku trate, vstup/ odchod oblasti, detekcia zmeny scény, detekcia prepätia zvuku, detekcia straty zvuku ,detekcia tváre,
- zabudovaný ohrievač (-40 ° C ~ 60 ° C (-40 ° F ~ 140 ° F)
- IP67 pre vonkajšie použitie
- 12VDC/ PoE [40]

4.3.2.4 Hikvison DS-2CD4A35FWD-IZS

Hikvison DS-2CD4A35FWD-IZS je 3 megapixelová a má rozlíšenie 2048 x 1536 HD video. Obsahuje IR LED diódu s rozsahom až 50 m. Kamera má vlastný úložný priestor 64GB.

Obr. 49 Hikvison DS-2CD4A35FWD-IZS [40]

Vlastnosti produktu

- CMOS s progresívnym skenovaním 1/ 2,8 "
- široký dynamický rozsah (120 dB)
- trojité prúdy
- 3D digitálna redukcia šumu
- objektív motorizovaného VF s inteligentným zaostrovaním (2,8 - 12 mm)
- inteligentná detekcia tváre
- detekcia narušenia
- vnútorný úložný priestor až do 64 GB
- zabudovaný inteligentný ohrievač

- IP67 pre vonkajšie použitie
- 24VAC [40]

4.3.2.5 AXIS P1435-LE

Kompaktná vonkajšia kamera pre denné a nočné sledovanie s skrytím IP-6 a verifikátorom objektívom P-iris. IR LED dióda umožňuje dohľad do vzdialenosti 30m. Kamera obsahuje slot na micro SD/ microSDHC/ microSDXC karty.

Obr. 50 AXIS P1435-LE

Vlastnosti produktu

- 2 MP, 1920x1080/ 60 fps
- Horizontálny uhol pohľadu: 95° – 35°
- Objektív 3–10.5 mm, F1.4
- WDR**:** Áno
- Režim Deň /Noc: Áno
- Min. svetelnosť 0,12 Lux
- Prostredie Exteriér, IP66, NEMA 4X
- Špeciálne funkcia Axis' Zipstream, Lightfinder

4.3.2.6 AXIS P3225-LVE

AXIS P3225-LVE je vonkajšia bezpečnostná 2 Megapixlová IP kamera s rozlíšením 1920 x 1080. Dosiahnuteľná viditeľná vzdialenosť je niečo okolo 30m. Obsahuje slot na microSD/ microSDHC/ microSDXC karty.

Obr. 51 AXIS P3225-LVE [41]

Vlastnosti produktu

- snímací senzor 1/3” CMOS s progresívnym skenovaním
- kompresia videa H.264 a MJPEG. WDR
- ohniskovou vzdialenosťou 3,0 až 10,5mm
- clonu P-iris a uhla záberu 34° až 92°
- ONVIF
- PoE [41]

4.4 Čiastkový záver

Kapitola zhrnula súčasné informácie o spoločnosti, a to:

- základné informácie o spoločnosti,
- uvedenie aktuálnych prístupových práv,
- prístupové bodov,
- súčasné SKV a VDS spoločnosti.

Hardwarové vybavenie jednotlivých bodov bolo v podstate dostačujúce. Až na prístupové body: bezobslužná vrátnica juh (BVJ) a záložná vrátnica (ZV). Na základe komunikácie so špecialistom divízie ESH bolo zistené, že tieto prístupové body sú v súčasnej dobe v štádiu riešenia a už sú aj vypracované projekty na ich inováciu. Jedná sa o prechod analógových kamier na IP kamery a inováciu VDS systému DEDICATED-MICROS na systém ATEAS, na ktorom pracujú všetky ostatné kamery v objekte. Všetky hardwarové komponenty prístupového systému Aktion a videodohľadového systému ATEAS sú dostačujúco prepojené so serverom prostredníctvom eternetového rozhrania alebo zbernice RS485 .

Pre softwarové prepojenie SKV a VDS, z hľadiska predstáv zákazníka, produktov nainštalovaných na serveri a ovládania na klientskom PC je najvhodnejšou variantou softwarová integrácia pomocou integračného softwaru systémov budov, ktorý spĺňa všetky podmienky na požadované funkcie zadané výrobnou spoločnosťou:.

- nastavenie automatických väzieb medzi systémami,
- vizualizácia systému,
- lokálne a vizuálne ovládanie,
- správa systému a užívateľov,
- kontrola činnosti operátorov,
- správa dochádzky s nadväznosťou na mzdový systém.

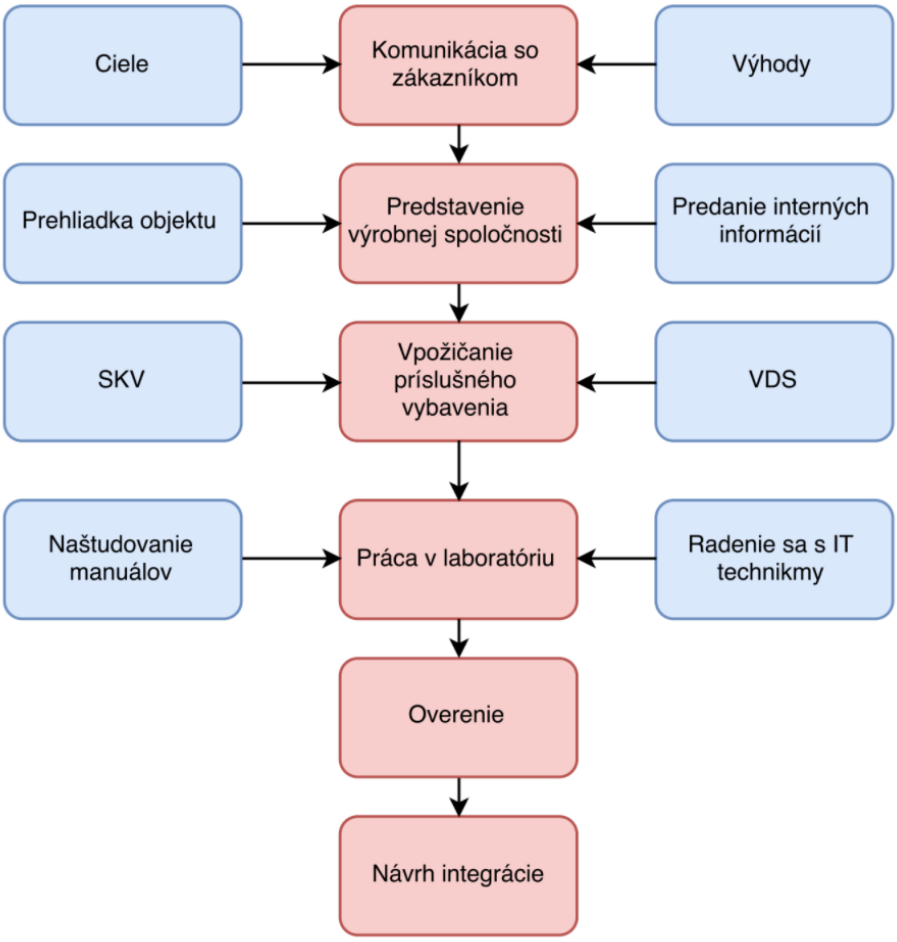
Dôležitou častou práce je zvolenie správneho integračného softwaru. Na základe získaných informácií a požiadaviek zákazníka, bude vhodnejšou alternatívou zvolenie systému SKV(Aktion), pretože jedna z podmienok zákazníka bola vyhľadávanie kamerových záznamov na základe ID užívateľa. SKV pracuje s databázami a s identifikačnými údajmi užívateľov a preto má aj prispôsobené prostredie pre priehľadný zoznam udalostí o jednotlivých vstupoch a výstupoch. K týmto udalostiam je možné priradiť záznam z ATEAS a následne si ho bude možné prehrať v prostredí systému Aktion.

5 BEZPEČNOSTNÝ PROJEKT VIDEODOHĽADOVÉHO PRÍSTUPOVÉHO SYSTÉMU

Táto kapitola bude zameraná na vytvorenie bezpečnostného projektu. Cieľom vytvoriť komplexný videodohľadový prístupový systém, VDPS, ktorý skvalitní a zefektívni bezpečnostný systém danej rozsiahlej výrobnej spoločnosti. Súčasný systém kontroly vstupu Aktion nekomunikuje so súčasným videodohľadovým systémom ATEASOM. Často vznikajú problémy, a to napr. pri do hľadávaní video záznamov zameraných na evidenciu osôb či vozidiel. Tieto softwary nie sú zosynchronizované, preto je nutné pracovať s istým časovým posunom, čo určite nie je pohodlné a práve takéto problémy, by mal navrhnutý VDPS zamedziť.

Pri tvorbe návrhu daného bezpečnostného projektu bola použitá metodika, v ktorej bol zvolený nasledovný postup:

- komunikácia so zákazníkom,
- predstavenie výrobnej spoločnosti,
- vypožičanie príslušného vybavenia,
- práca v laboratóriu,
- overenie konektivity.
- návrh integrácie



Obr. 52 Štruktúra metodiky

5.1 Komunikácia so zákazníkom

Prvým bodom vypracovania bola konzultácia so zákazníkom, kde boli vymedzené požiadavky a ciele zákazníka. Komunikácia prebehla v areáli výrobnej spoločnosti a zúčastnili sa jej: riaditeľ divízie ESH, vedúci diplomovej práce a študentom. Študent dostal potrebné informácie a kontakty na príslušné osoby, s ktorými v príbehu vypracovania práce spolupracoval.

5.1.1 Ciele

Vymedzené ciele bezpečnostného projektu:

- zjednodušenie práce obsluhy,
- zníženie prevádzkových nákladov,
- zvýšenie stability systému,
- zvýšenie bezpečnosti systému,

- zaistenie ďalšieho rozvoja systému,
- lepší užívateľský komfort,
- zvýšenie efektivity funkcií,
- činnosť podľa definovaných schém,
- minimalizovanie chýb a anomálií,
- bezproblémová komunikácia systému.

5.1.2 Výhody aplikácie

Tvorba integrovaného poplachového systému prináša radu výhod, a to hlavne prostredníctvom týchto troch bodov: bezpečnosť objektu, užívateľský komfort objektu a redukcia prevádzkových nákladov. Hlavné výhody:

- zvýšenie účinnosti poplachových aplikácií,
- získanie predpoplachových informácií,
- získanie informácií o nežiadúcich zmenách,
- možnosť efektívneho riadenia krízových situácií,
- účelné riadenie prístupu osôb do jednotlivých častí objektu,
- získanie väčšieho počtu informácií a prehľadu o bezpečnostných situáciách v objekte,
- zvýšená možnosť kontroly osôb, vozidiel a materiálu,
- centralizovaná obsluha, jednotné užívateľské prostredie,
- široký rozsah funkcií, univerzálnosť a flexibilita,
- prehľadnosť, rýchlosť a náklady inštalácie v porovnaním s individuálnou aplikáciou systémov.

5.2 Predstavenie výrobnej spoločnosti

Pri predstavení spoločnosti som úzko spolupracoval s príslušnými zamestnancami výrobnej spoločnosti, ktorí so mnou ochotne spolupracovali počas celého času vypracovania diplomovej práce. Predstavenie spoločnosti prebehalo v troch bodoch:

- prehliadka objektu,
- prezentácia SKV a VDS,
- predanie interných informácií.

5.2.1 Prehliadka objektu

Prehliadka objektu bola prevedená spolu s ESH špecialistom výrobnej spoločnosti. Vzhľadom na zameranie a rozsah práce bola prehliadka zameraná na prístupové body výrobnej spoločnosti. Počas prehliadky bolo možné vidieť jednotlivé prístupové body v akcii počas identifikácií. Súčasťou prehliadky bola aj fotodokumentácia prístupových bodov, ktorá bola využitá na vytvorenie pôdorysov jednotlivých prístupových budov. Tieto vyhotovené pôdorysy je možné vidieť v predošlej kapitole. Fotky prístupových bodov vidíme na Obr.č.53.

Obr. 53 Fotky vstupov výrobnej spoločnosti

5.2.2 Prezentácia SKV a VDS

Prezentácia SKV a VDS prebehla v kancelárii zainteresovaných osôb výrobnej spoločnosti. Aleš Melichár mi odprezentoval systém kontroly vstupu Aktion 5.1, kde mi ukázal ako pracuje, a čo využíva v konkrétnej výrobnej spoločnosti. Následne mi poskytol informácie o hardware, s ktorými software spolupracuje. Technické informácie o hardware využívanom v spoločnosti sú vypísané v predošlej kapitole. Špecialista divízie ESH výrobnej spoločnosti mi zas prezentoval VDS ATEAS, ktorý využíva daná výrobná spoločnosť. V spolupráci sme dohľadali konkrétne typy kamier využité pri vstupoch, ktoré bolo na základe týchto informácií

možné zakresliť aj s írch zorným polom do pôdorysov. Pôdorysy jednotlivých vstupov sú uvedene v predošlej kapitole.

5.2.3 Predanie interných informácií

Predanie interných informácií bolo nevyhnutné pre vypracovanie diplomovej práce. Príslušní zamestnanci výrobnej spoločnosti mi poskytli tieto interné dokumenty:

- internú smernicu o evidencií osôb,
- pôdorys celého objektu,
- umiestnenie a typy hardwaru SKV,
- umiestnenie a typy hardwaru VDS.

5.3 Vypožičanie príslušného vybavenia

V rozsiahlej výrobnej spoločnosti prebieha nepretržitá prevádzka. Z dôvodu, aby nebol narušenýchod prevádzky, bolo dovolené pracovať na synergií SKV a VDS v priestoroch Univerzity Tomáša Bati ve Zlíne. Pre prácu na univerzite bolo nutné vypožičanie príslušných softwarov a hardwarov jednotlivých systémov.

5.3.1 Systém kontroly vstupu

Systém kontroly vstupu vo výrobnej spoločnosti spravuje nemenovaná externá firma. Zapožičanie pre Univerzitu Tomáša Bati ve Zlíne bolo teda riešené mimo výrobnú spoločnosť. Bohužiaľ, touto cestou vznikla komplikácia, čo sa odzrkadlilo na neskorom dodaní príslušných produktov, tým pádom aj predĺžení vypracovania diplomovej práce.

Vypožičané produkty:

- licenci na SW Aktion 5.1 a Aktion NEXT
- hardwere:
    - Terminál ProfiCon/Ethernet,
    - Multifunkčný terminál AXT-300/310,
    - Kontrolér MultiCon – KMC/E/2M,
    - Modul MultiCon – MMC.

5.3.2 Video dohľadový systém

Univerzita Tomáša Bati ve Zlíne už istú dobu spolupracuje s firmami ATEAS a AXIS. Disponuje so softwarmi a hardwarmi, ktoré sú potrebné pre otestovanie spolupráce so systémom Aktion, preto žiadne vypožičanie nebolo v tomto prípade nutné.

5.4 Práca v laboratóriu

Ako bolo už spomenuté, pre prácu bola zvolená práca v laboratóriu Univerzity Tomáša Bati ve Zlíne. Laboratórium sa nachádza v priestoroch fakulty aplikovanej informatiky a má označenie D209. Zodpovednou osobou za chod laboratória je Ing. Jíří Ševčík, ktorý je aj vedúcim diplomovej práce.

5.4.1 Laboratórne podmienky

Laboratórium je využívané hlavne na vyučovanie predmetu Kamerové systémy. Disponuje rozsiahlym moderným vybavením.

Obr. 54 Foto ukážka z laboratória

Pre vypracovanie práce boli využité prostriedky laboratória a prostriedky vypožičané od súkromného segmentu. Konkrétne sa jedná o tieto prvky:

- prostriedky laboratória:

  - Osobný PC
  - sieťový server
  - SW Ateas 4.4.0
  - AXIS M1125
  - AXIS P1435- LE
- vypožičané prostriedky
  - SW Aktion 5.1
  - Aktion NEXT
  - Terminál ProfiCon/Ethernet,
  - Multifunkční terminál AXT-300/310,
  - Kontrolér MultiCon – KMC/E/2M,
  - Modul MultiCon – MMC.

5.4.1.1 Kamery použité v laboratóriu

Obr. 55 AXIS M1125 [41]

Sieťová bezpečnostná kamera vybavená týmito funkciami:

- Deň/noc,
- Rozlíšenie 1920 x 1080 - 1080p
- objektiv auto iris
- varifokální
- MJPEG, H.264 - DC 8 - 28 V / PoEAXIS
- DC 8 - 28 V / PoE [41]

Obr. 56 AXIS P1435-*LE [41]*

Vonkajšia sieťová bezebečnostná kamera s vlastnosťami:

- Režim deň/noc
- Rozlíšenie 1920 x 1080 - 1080/60p,
- objektiv auto iris,.
- Varifokální
- MPEG-4, MJPEG, H.264 - PoEAXIS P1435-LE
- DC 8 - 28 V / PoE [41]

5.4.2 Práca na synergií Aktionu 5.1 a Ateasu 4.4.0

Pre prácu s jednotlivými SW bola vytvorená platforma VMwere, ktorá slúži pre virtualizáciu jedného alebo viacerých PC na jednom hostiteľskom PC. Do tohto virtuálneho prostredia boli postupne nainštalované softwar a hardwar Aktion 5.1 a Ateasu 4.4.0. Funkcionalita oboch softwarov bola otestovaná prepojením príslušným hardwarom. Následne začala práca na synergií dvoch spomínaných softwarov. Táto práca pozostávala z naštudovania jednotlivých manuálov a spoluprácou s informačnými technikmi jednotlivých spoločností. Ateas 4.4.0 sa ukázal ako vysoko výkonná softwarová platforma pre IP kamerové systémy, ktorá nemá problém s konektivitou s ostatnými softwarmi. Pri softwari Aktion Complete vznikol problém, a to vo forme absencie integračného modulu so softwarom Ateas. Na Tab. 6 je možné vidieť prehlaď softwarových modulov Aktionu 5.1.

Tab. 6 Softwarové moduly Aktionu 5.1

ACL	Základný modul správy a riadenia vstupov
MDO	Záznamy o účasti
EVO	Záznamy o výrobných operáciách (len MDO)
AMM	Messenger, správa udalostí
AWB	AktionWEB, intranetová nadstavba, návštevy, návštevnosť, prítomnosť, SW Terminal
ADM	Komunikačný softvér (Aktion Device Manager)
AST	Správa o výdaji studenej stravy
AFT	Pripojenie a obsluha fotoaparátu OLYMPUS od SW Aktion
AMB	Mobilný terminál (AktionMobile) pre PDA, licencie pre jedno PDA
SWT	SW, funkčný iba s snímačom APR-P20 / HS / T / USB
AST	Základný modul ASTRIS, administratíva, strava, recept, štandardizovaný
AOS	Terminálne objednávanie stravy
ASH	Skladové hospodárstvo
APP	Priamy predaj- pokladňa
AWZ	AstrisWEB, objednávanie na internete pre zamestnancov
AWP	AstrisWEB, objednávanie na internete pre zamestnancov

Tento problém bol riešený s IT technikmi a špecialistami firmy EFG a Aktionu. Bolo zistené, že pre túto spoločnú konektivitu, by bolo nutné preprogramovanie softwaru alebo vytvorenie modulu, na ktorý by následne bolo nutné vyžiadať rôzne licencie, ktoré si vyžadujú vedomosti presahujúce študenta daného oboru.

5.4.2.1 Zistené poznatky

Navrhujem aktualizáciu softwaru Aktionu 5.1 na Aktion NEXT, ktorý je novším produktom spoločnosti EFG. Tento software bol otestovaný a neprejavil žiadne problémy v spolupráci so softwarovou platformou Ateas 4.4.0. Navyše Aktion NEXT je výbornou voľbou do budúcna.

Jednou z možností prepojenia so softwarom Ateas je aj funkcia rozpoznávanie ŠPZ vozidiel, čo sa v dnešnej dobe stáva stále a stále väčším trendom.

5.4.3 Aktion NEXT

Aktion NEXT je určený firmám, ktoré vyžadujú prispôsobenie systému svojim podmienkam a špecifikáciám. Tento software komunikuje so zariadeniami na sieti pomocou TCP/IP s vysokou úrovňou zabezpečenia. Umožňuje prístup užívateľom podľa ich zaradení a oprávnení. [42]

Obsahuje zabudované funkcie dochádzky, stravovania, výroby a ďalších aplikácií, vrátaním podpory výmeny dát s inými softwarmi. Je určený pre firmy, ktoré očakávajú vyššiu pridanú hodnotu ako evidencia príchodov a odchodov do/z objektu. [42]

Funkcie:

- management kariet, užívateľov a prístupových oprávnení
- monitorovanie pripojených HW zariadení,
- kalendáre a časové plány,
- definícia agend/integrácia (ATEAS...)
- variabilné reporty a žurnály dát,
- vyhodnocovanie pracovnej doby. [42]

5.5 Overenie konektivity Aktion NEXT a Ateas 4.4.0

Pre overenie konektivity týchto dvoch softwarov bol aplikovaný tento postup.

5.5.1 Nastavenie kontroléru

V prvom rade je dôležité nastaviť kontrolér, ktorý bude ovládať závoru. Nastavenie pozostáva z dvoch bodov

- nastavenia komunikačnej linky,
- vytvorenia adresového bodu.

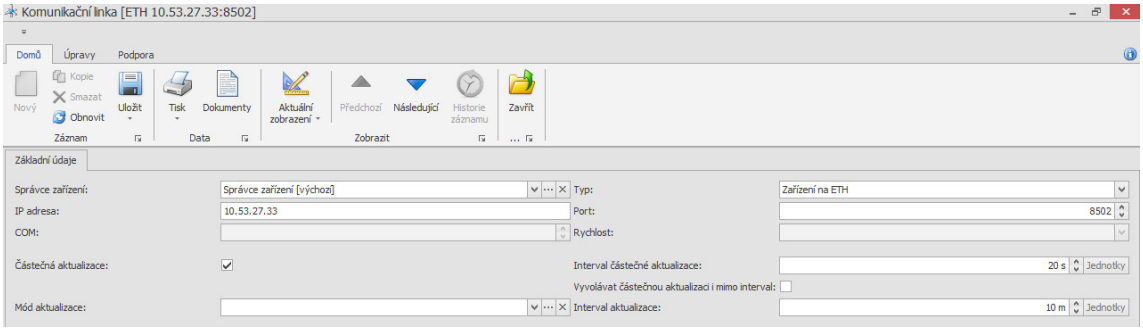
5.5.1.1 Nastavenie komunikačnej linky

V software Aktion NEXT sa preklikáme cez terminál prostredia týmto postupom **Konfigurace>komunikační linky>Nový**

Následne musia byť v okne pre vytvorenie novej komunikačnej linky vyplnené tieto údaje:

- **Správce zařizení**
- **IP adresa kontroléru**

Pre dokončenie komunikačnej linky je nutné uloženie. Okno pre túto konfiguráciu je zobrazené na obrázku Obr 57.



Obr. 57 Nastavenie komunikačnej linky

5.5.1.2 Nastavenie adresového bodu

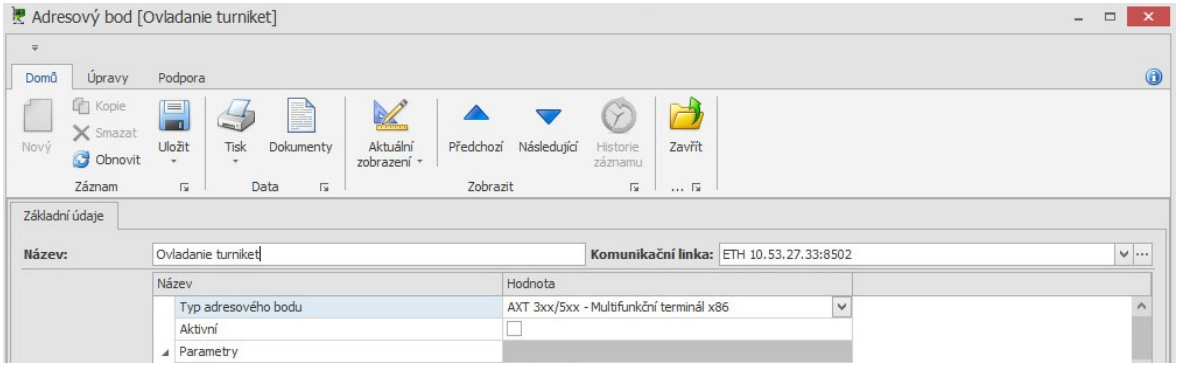
Bol použitý postup:

Konfigurace>komunikační linky>Nový

Nutné vyplniť:

- názov adresového bodu,
- pridelenie nastavenej komunikačnej linky,
- typ adresového bodu
- následne ostatné parametre podľa nastavených stanovených podmienok

Následné uloženie.

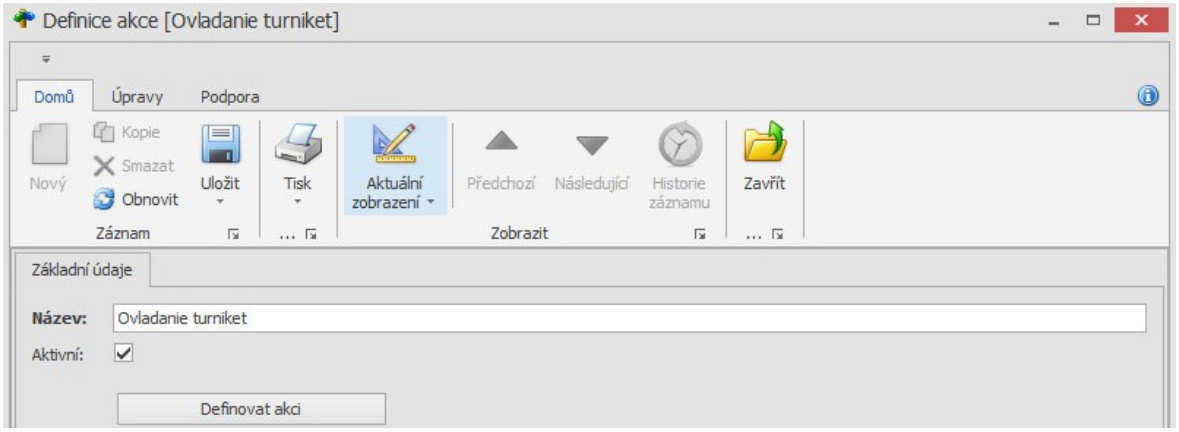


Obr. 58 Nastavenie adresového bodu

5.5.2 Prepojenie kontroléru

Postup:

Definice akcií>Centrum akcí>Nový



Obr. 59 Definovanie kontroléru

Následné sa definujú akcie v postupných oknách:

- výber typu akcie,
- výber udalosti,
- výber osôb,
- vyber HW štruktúry,
- výber akcie + čas,
- akcie na adresovom bode,

a následné uloženie.

5.5.3 Nastavenie externých zariadení

Pre spoluprácu je nutne nakonfigurovať server ATEAS a jednotlivé kamery.

5.5.3.1 Administračný server ATEAS

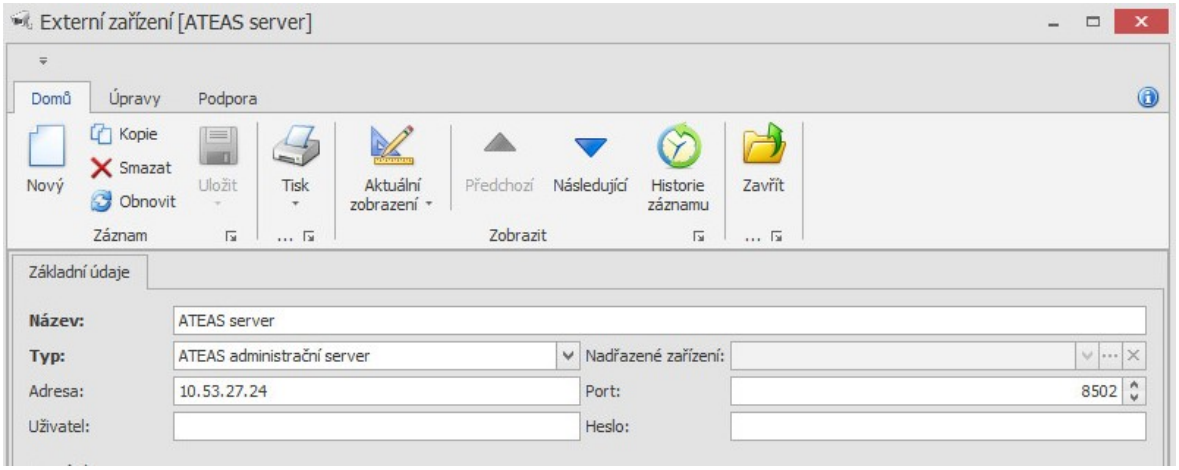
Postup:

Přístup> Externí zařízení >Nový

Následne je nutné vyplniť:

- **názov,**
- **typ (ATEAS administrační server),**
- **IP administračného serveru,**

- **Port**
- **užívateľské údaje pre pripojenie do server ATEA**



Obr. 60 Nastavenie Administračného serveru

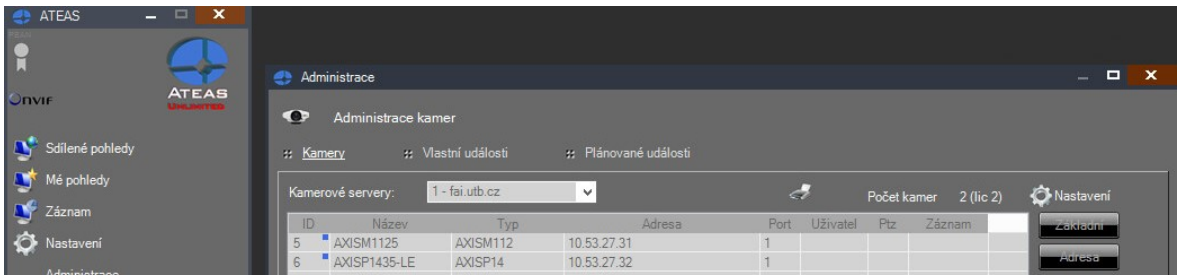
5.5.3.2 Nastavenie Kamier

Postup:

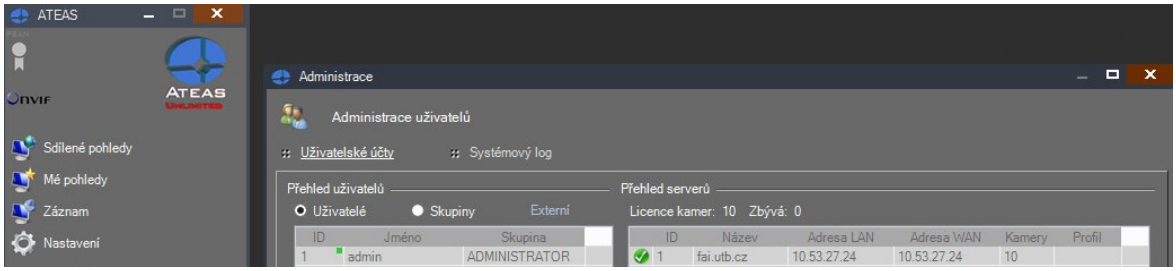
Přístup> Externí zařízení >Nový

Nutné vyplniť:

- **názov,**
- **typ (ATEAS kamera),**
- **nadriadené zariadenie (názov administračného serveru),**
- **adresa zariadenia(formát[ID serveru-ID kamery]),**
- **Tieto informácie je možné nájsť v software ATEAS (Administrace> Kamery a Administrace>Užívatelé).**

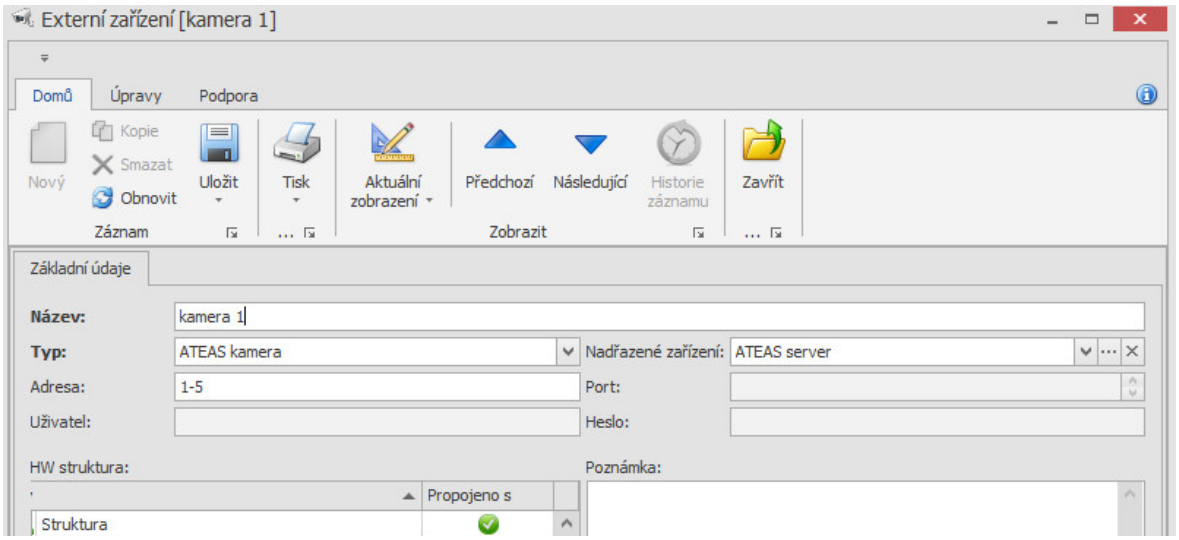


Obr. 61 Vyhľadanie ID kamier ATEAS

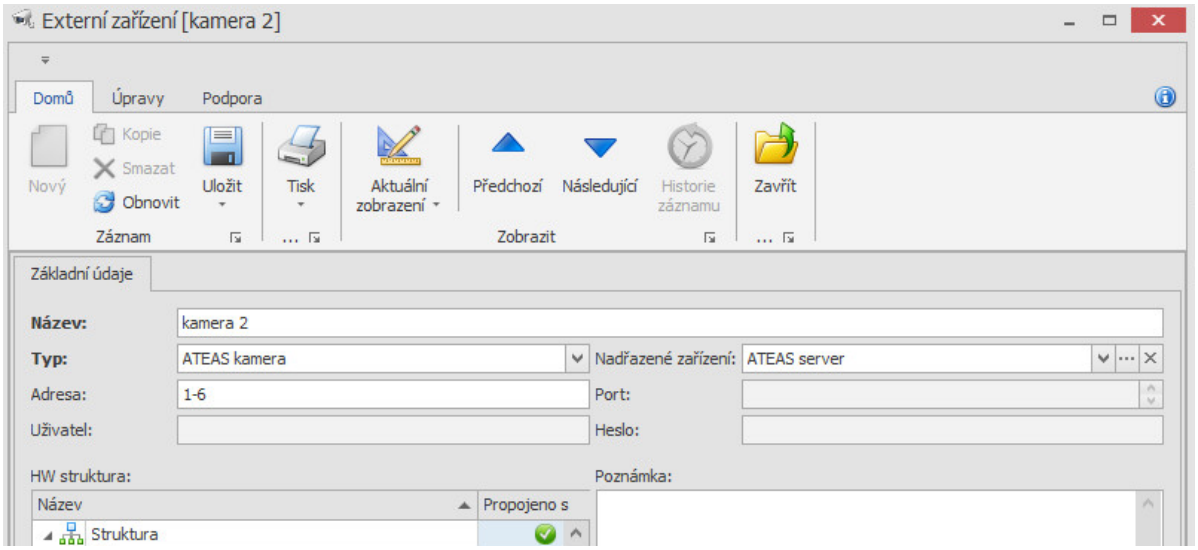


Obr. 62 Vyhľadanie ID serveru ATEAS

- **výber HW štruktúry (priradenie k nastavenému kontroléru)**



Obr. 63 Pridanie kamery 1



Obr. 64 Pridanie kamery 2

5.5.4 Sledovanie záznamu z kamier

Postup:

Číselníky> Udalosti

Následne v zozname udalostí vyberieme príchod/odchod a dvojklikom otvoríme. V otvorenom okne je možné si pozrieť kamerový záznam z vybranej udalosti.

Obr. 65 Záznam udalosti z kamery 1 v software Aktion NEXT

Obr. 66 *Záznam udalosti z kamery v software Aktion NEXT*

5.6 Návrh integrácie

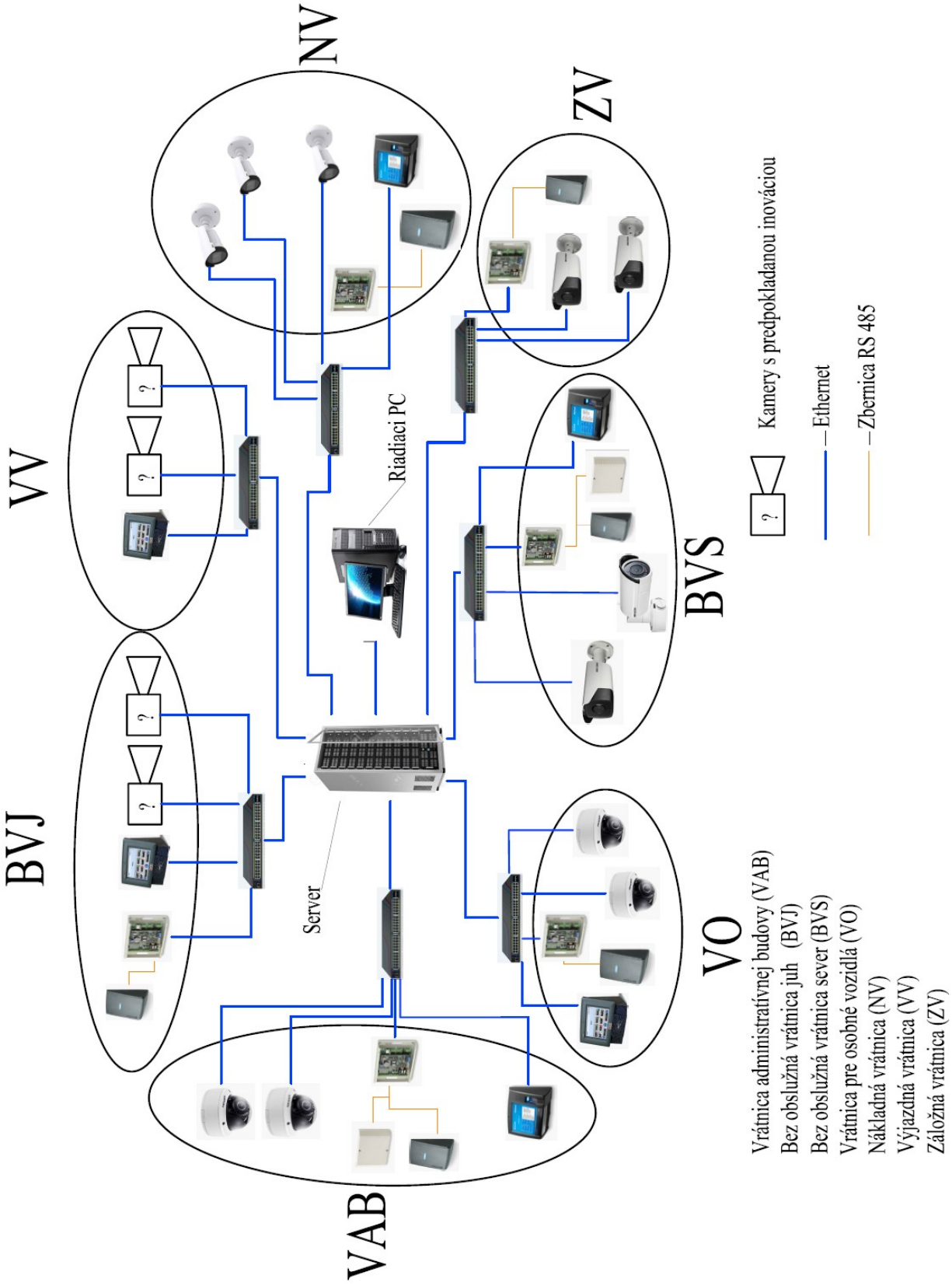
Návrh je výstupom použitej metodiky, ktorá bola použitá pre daný bezpečnostný projekt. Projekt je zameraný na integráciu SKV a VDS danej spoločnosti. Na základe získaných a overených informácií bolo zistené, že je možné daný návrh zrealizovať. Pre danú integráciu je možné využiť všetok súčasný hardware spoločnosti. Vzhľadom na fakt, že daná rozsiahla výrobná spoločnosť disponuje s veľkým počtom hardwaru VDS, ktorý spolupracuje so softwarom ATAS bude v ukážke návrhu uvedená len časť, ale rovnakým spôsobom budú prepojené všetky hardwarové komponenty spoločnosti.

Vzhľadom na zameranie práce bude ukážka návrhu prezentovaná v oblasti prístupových bodov objektu. Pre dané hardwarové prepojenie sú využité tieto komponenty systému kontroly vstupu Aktion a videodohľadového systému Ateas.

Tab. 7 Hardwarové komponenty

Aktion NEXT	Ateas 4.4.0
Terminál ProfiCon/Ethernet,	Hikvison DS-CD4132FWD-IZ
Multifunkční terminál AXT-300/310,	Hikvison DS-2CD432FWD-IS
AXR 300i	Hikvison DS-2CD4A65F-IZS
Modul MultiCon – MMC	Hikvison DS-2CD4A35FWD-IZS
Kontrolér MultiCon – KMC/E/2M	AXIS P1435-LE
	AXIS P3225-LVE

Hardwarové prepojenie komponentov z Tab č.7 je prevedené prostredníctvom zbernice 485 a ethernetového rozhrania pripojeného cez switche, ktoré podporujú PoE, na server a v zapätí na daný server. Štruktúru toho prepojenia hardawaru z Tab 7 je možné vidieť na Obr. 67.



Obr. 67 Štruktúra integrácie

Na obr. č. 67 je uvedená značka kamery  . Táto značka signalizuje IP kamery, pre ktoré sa aktuálne vypracováva projekt, čiže v dnešnej dobe ešte nie sú známe konkrétne modely.

Pre softwarovú integráciu navrhujem inováciu softwaru Aktion 5.1 ktorý v praktickom teste v laboratóriu FAI UTB neukázal možnú konektivitu so softwarom Ateas 4.4.0, a to no základe absencií príslušného modulu.

Navrhujem prechod na novší produkt spoločnosti Aktion s názvom Aktion NEXT. Aktion NEXT. V praktickej skúške v laboratóriu ukázal možnosť prepojenia so systémom ATEAS. Nevyhnutné je dodať, že software Aktion NEXT podporuje všetok použitý hardware danej spoločnosti, tým pádom nieje nutná žiadna nová investícia do hardwaru. Navyše tento software otvára ďalšie aplikovateľné možnosti a to napríklad prostredníctvom rozpoznávania registračných značiek automobilov, kde tiež dokáže s ATEASOM účelne a efektívne spolupracovať.

ZÁVER

Hlavným cieľom diplomovej práce bolo vypracovať návrh bezpečnostného projektu videodohľadového prístupového systému tvoreného systémom kontroly vstupu a videodohľadového systému danej rozsiahlej výrobnej spoločnosti.

V teoretickej časti boli analyzované relevantné informácie, definujúce požiadavky na spomínané oblasti systémov technického zabezpečenia a možnosti ich integrácie V prvej kapitole boli podrobne rozobrané systémy kontroly vstupu, a to hlavne cez jej funkčné vlastnosti, ktorým sa venuje technická norma ČSN EN 60839-11-1. Prvá kapitola zahŕňa aj topológiu, prehľad legislatívneho rámca a možnosti prepojenia daného systému.

Druhá časť teoretickej časti je zameraná na videodohľadové systémy a analýzu ich funkčných vlastnosti, ktoré sú obsiahnuté v technickej norme ČSN EN 62676-1-1. Takisto ako predošlá kapitola aj táto poskytuje topológiu, prehľad legislatívneho rámcu a možnosti prepojenia s inými systémami.

Nasledujúca tretia kapitola a zároveň posledná kapitola teoretickej časti sa zaoberá spôsobmi integrácie daných systémov. Kapitola sa opiera o technickú normu ČSN EN CLC/TS 50398 uvádza a objasňuje všetky možnosti hardwarovej a softwarovej integrácie.

Praktická časť diplomovej práce uvádza danú rozsiahlu výrobnú spoločnosť ako výrobcu automobilových súčastok. Kapitola charakterizuje výrobnú spoločnosť so zameraním na prístupové práva a prístupové body. Venuje sa každému prístupovému bodu zvlášť a poukazuje na použitý software a hardware systému kontroly vstup a videodohľadového systému, ktorých komponenty sú aj vyobrazené na jednotlivých pôdorysoch. Súčasťou kapitoly je aj predstavenie softwaru Aktiona 5.1 s jeho hardwarovými zložkami a technickými špecifikácie výrobcu. Kapitola taktiež predstavuje software Ateas 4.4.0 tiež s časťou hardwarových zložiek, s ktorými spolupracuje. Ná základe týchto informácií bola zvolený spôsob integrácie, a to aj s voľbou konkrétneho integračného softwaru pre danú spoločnosť. Výber zvoleného softwaru bol zdôvodnený a následne aplikovaný v nasledujúcej kapitole diplomovej práce.

Posledná a zároveň najdôležitejšia kapitola predstavuje bezpečnostný projekt videodohľadového prístupového systému, ktorý predstavuje integráciu spomínaných systémov danej výrobnej spoločnosti. Bezpečnostný projekt opisuje prácu študenta, získavanie informácií, softwaru a hardwaru. Časť bezpečnostného projektu tvorilo aj

praktické overenie synergie daných systémov. Študent sa rozhodol túto aplikáciu realizovať v priestoroch FAI UTB ve Zlíne, aby nezasahoval do výrobného procesu za chodu spoločnosti. Na základe tejto práce v laboratóriu, bolo zistené, že daný software za daných okolností a vedomostí študenta nie je možné prepojiť z dôvodu absencie integračného modulu systému Aktion 5.1. Preto študent navrhuje aktualizáciu software Aktion 5.1 na Aktion NEXT, touto aktualizáciou nevzniknú žiadne náklady spojené s hardwarom, ale len so zakúpením licencie na nový software. Aktualizácia otvorí aj nové cesty do budúcna, a to napríklad prostredníctvom využitia prepojenia s Ateasom pre rozpoznávanie ŠPZ vozidiel. Táto spoločná implementácia sa dnes využíva a stáva sa čím ďalej viac populárna. Konektivita Aktionu NEXT s Ateasom 4.4.0 bola v praktickej časti úspešne overená a zdokumentovaná. Z dôvodu tejto spolupráce je táto alternatíva navrhnutá pre aplikáciu do návrhu bezpečnostného projektu video-dohladového systému danej rozsiahlej výrobnej spoločnosti.

SEZNAM POUŽITÉ LITERATURY

[1] 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.

[2] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-05-7.

[3] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-35-4.

[4] FOJTÍK, Daniel Bc. *Systémy kontroly vstupu pro kombinované a integrované systémy*. Zlín, 2010. Diplomová práce. UTB ve Zlíně. Vedoucí práce Ing. Rudol Dga.

[5] ČSN EN 60839-11-1. *Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty.* 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 33 4593.

[6] http://www.aspisys.com/pricelist.php

[7] *Gras* [online]. In: . 2014 [cit. 2017-08-24]. Dostupné z: http://www.gras.sk/e-shop2/komponenty/cip/cipove-karty/

[8] *Tesel* [online]. In: . 2014 [cit. 2017-08-24]. Dostupné z: http://tesel.sk/domovy-vratnik/samostatne-citacky/

[9] *ID-karta* [online]. In: . 2014 [cit. 2017-08-24]. Dostupné z: http://www.id-karta.sk/

[10] ČSN EN 60839-11-2. *Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace* 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016. Třídící znak 334593.

[11] ČR. *Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů.* Sbírka zákonů, Česká republika. 2000

[12] ČSN EN 62676 1 - 1. *Dohledové videosystémy pro použití v bezpečnostních aplikacích: Systémové požadavky*. 1. Praha 1: Úřad pro technickou normalizaci, metrologii a státní zku-šebnictví, 2014.

[13] POLKA, Oliver. *Užití GTEM cely pro testy elektromagnetické kompatibility zab-ezpečovacích systémů*. Zlín, 2015. Bakalářske práce. UTB ve Zlíně. Vedoucí práce Doc. RNDr. Vojtěch Křesálek, Csc.

[14] *GMElctronic* [online]. [cit. 2017-08-27]. Dostupné z: https://www.gme.cz/venkovni-analogova-kamera-ds-2ce16c2p-it3

[15] Lukáš, Luděk: *Bezpečnostní technologie, systémy a management II*. - 1. vyd. -- Zlín: VeRBuM, 2012. -- 387 s. ISBN 978-80-87500-19-4

[16] KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 3. aktualiz. S.l.: Cricetus, 2006. ISBN 80-902938-2-4 [14]

[17] *Metody přenosu dat* [online]. [cit. 2017-05-13]. Dostupné z: http://www.net-cam.cz/encyklopedie-ip-zabezpeceni/metody-prenosu-dat.php

[18] *ONVIF* [online]. [cit. 2017-05-13]. Dostupné z: https://www.onvif.org/

[19] SULEK, Martin. *Pokročilá videoanalýza obrazu* [online]. 2015 [cit. 2017-05-05]. Dostupné z: http://www.abbas.cz/clanky/recenze-technika/pokrocila-videoanalyza-obrazu/

[20] *Securityproflorida* [online]. http://www.securityproflorida.com/security-cameras/securityproflorida [cit. 2017-08-27].

[21] BC. POLÁK, David. *Kamerový systém a jeho využití v občanském životě*. Zlín, 2014. Diplomová prace. UTB ve Zlíně. Vedoucí práce JUDr. Jíří Kamenik.

[22] *Komprese H.265 / H.265+: Výhody komprese H.265 / H.265+ jsou důležitým krokem kupředu* [online]. [cit. 2017-05-05]. Dostupné z: https://www.abso-lon.cz/aktuality/_zobraz=komprese-h.265--h.265--jiz-brzy

[23] *Rapid-system: Kamerové systémy* [online]. [cit. 2017-08-28]. Dostupné z: http://www.rapid-system.cz/kamerove-systemy.html

[24] TECHNICKÉ NORMY: kategorie: 33 - ELEKTROTECHNIKA - ELEKTROTECHNICKÉ PŘEDPISY 3345 - Elektrická řídicí zařízení. *Technor* [online]. [cit. 2017-08-28]. Dostupné z: http://www.technicke-normy-csn.cz/technicke-normy/elektrotechnika-elektrotechnicke-predpisy-33/elektricka-ridici-zarizeni-3345/?do[]=setOffset&offset=0

[25] NILSSON, Frederik. Intelligent Network Video : Understanding Modern Video Surveillance Systems. Har/Dvdr edition. [s.l.] : CRC Press, 2008. 416 s. ISBN 1420061569, 978-1420061567.

[26] ING. VALOUCH, Jan, Ph.D. *PROJEKTOVÁNÍ INTEGROVANÝCH SYSTÉMŮ*. Druhé. Zlín: Univerzita Tomáše Bati ve Zlíně, 2015. ISBN 978-80-7454-557-3.

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

[28] VALOUCH, Jan. Integrované poplachové systémy. 2. část Technické způsoby integrace. Security magazín. Vyd. č. 112, 2/2013. Praha: Security Media, 2013, s. 54-57. ISSN 1210-8273.

[29] Siemens. Systémy kontroly vstupu. [online]. [cit. 20131024]. Dostupné z <https://www.siemens.cz/acs>.

[30] VALOUCH, Jan. *PROJEKTOVÁNÍ INTEGROVANÝCH SYSTÉMŮ*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-296-1.

[31] VALOUCH, Jan. Integration Techniques of Alarm Systems. In *TRANSACTIONS of the VŠB - Technical University of Ostrava.* Ostrava: VŠB, 2012. No. 1, Vol. VII. Safety Engineering Series. p. 65-72. ISSN: 1801-1764.

[32] *Variant plus. SecurityView.* [online]. [cit. 20131029]. Dostupné z <http://www.variant.cz/vyhledavani/?search=security+view>.

[33] EFG. *Užívatelský manual Aktion 5.1* – KMC/E/2M [onli-ne]. In: . 2014, s. 11 [cit. 2017-08-28]. Dostupné z: www.efg.cz

[34] PILZ. *Technický list TPC_E*: Terminál ProfiCon/Ethernet. [online] In: . 2007, s. 3 [cit. 2017-05-04]. Dostupné z: www.aktion.cz

[35] STEPAN. *Technicky_List_AXT-300-310*: Multifunkční terminál AXT-300/310 [online]. In: . 2015, s. 6 [cit. 2017-05-04]. Dostupné z: www.aktion.cz

[36] *EFG* [http://shop.efg.cz/z19762-axr-300i]. [cit. 2017-08-28].

[37] MOON. *Technicky_List_KMC_E_2M*: Kontrolér MultiCon – KMC/E/2M [onli-ne]. In: . 2014, s. 11 [cit. 2017-05-04]. Dostupné z: www.aktion.cz

[38] STEPAN. *Technicky_List_MMC_2*: Modul MultiCon - MMC [online]. In: . 2015, s. 4 [cit. 2017-05-04]. Dostupné z: www.aktion.cz

[39] *ATEAS* [http://www.ateas.net/]. [cit. 2017-08-28].

[40] *123SECURITY* [https://www.123securityproducts.com/]. [cit. 2017-08-28]

[41] *AXIS* [https://www.axis.com/cz/cs/]. [cit. 2017-08-28].

[42] Software Aktion.NEXT [cit. 2017-08-28].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

APAS	Ovládacie prvky a snezory miest prístupu
BVJ	Bezobslužná vrátnica juh
BVS	Bezobslužná vrátnica sever
CCD	Charge coupled devic
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central procesin unit
ČR	Česká republika
ČSN	Česká štátna norma
DPPC	Dohladové poplachové prijmacie centrum
DVR	Digital videorekorder
EACS	Elektronické systemy kontroly vstupu
FAI	Fakulta aplikovanej informatiky
GSM	Group special device
HW	Hardware
HZS	Hasičský záchranný zbor
ID	Identifikate
IN	Vstup
IP	Internet protocol
LAN	Local area network
NV	Nákladná vrátnica
NVR	Sietovy videorekorder
ONVIF	Open network video interface forum
OUT	Výstup
PoE	Power over Ethernet
PTZ	Pan tilt zoom
PZTS	Polachove zabezpečovacie a tiesnove systémy
RJ	Riadiaca jednotka
RTSP	Real time streaming protocol
SIE	Aplikácie systémovej elektroinštalácie
SKC	Systémy kontroly vstupu
SW	Software

ŠPZ	Štátna poznávacia značka
TCP	Transmission control protocol
UDP	User datagram protocol
UTB	Univerzita Tomaše Bati
VAB	Vratnica administrativnej budovy
VDPS	Video-dohľadový prístupový systém
VDS	Video dohľadový systém
VO	Vrátnica osobné vozidla
VSS	Video Surveillance system
VTD	Video prenosová sieť
VV	Výjazdová vrátnica
WAN	Wide area network
ZV	Záložná vrátnica
ZZS	Zdravotná záchranná služba

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PRÍLOHA PI: POŽIADAVKY

Tabulka 3 – Požadavky na indikaci a hlášení

Požadavky na indikaci a hlášení		Indikace			Přiřazení stupně			
					1	2	3	4
	A – Portál (místní indikace)							
1	Požaduje se vizuální a/nebo akustická indikace, jestliže je povolen přístup	•			P	P	P	P
2	Požaduje se vizuální a/nebo akustická indikace, jestliže je přístup odmítnut	•			P	P	P	P
3	Vizuální a/nebo akustická indikace stavu uzamčení portálu dokud není přístup povolen	•			V	V	V	V
4	Vizuální a/nebo akustická indikace je požadována pro poslední časový interval (doba před výstrahou) maximální povolené doby otevření portálu jestliže portál zůstane otevřen, pro varování uživatele (uživatelů), že uplyne doba otevření portálu. Zanikne, je-li portál uzavřen. Doba otevření musí být v celém systému definovaná, nebo konfigurovatelná u jednotlivých portálů (doporučená doba: 10 sekund)	•			V	V	P	P
	B – Ovládací panel (hlášení)							
		Zobrazení	Výstraha	Záznam				
5	Požaduje se vizuální informace, je-li přístup povolen	•			V	V	V	V
6	Požaduje se záznam, je-li přístup povolen			•	V	V	P	P
7	Požaduje se vizuální informace, výstraha a záznam při stavu nátlaku	•	•	•	V	V	V	P
8	Počitadlo použití karty	•		•	V	V	V	V
9	Požaduje se vizuální informace, výstraha a záznam při zamítnutí přístupu v důsledku pokusu o použití identifikačního prostředku, jehož platnost vypršela	•	•	•	V	V	V	P

Tabulka 3 – Požadavky na indikaci a hlášení *(pokračování)*

Požadavky na indikaci a hlášení		Indikace			Přiřazení stupně			
					1	2	3	4
B – Ovládací panel (hlášení)								
		Zobrazení	Výstraha	Záznam				
10	Požaduje se vizuální informace, výstraha a záznam, při zamítnutí přístupu z důvodu překročení konfigurovatelného počtu pokusů o použití identifikačního prostředku s neplatnou uloženou informací. Není-li počet pokusů konfigurovatelný, musí být omezen na 5°	•	•	•	V	V	V	P
11	Požaduje se vizuální informace, výstraha a záznam, při zamítnutí přístupu z důvodu překročení konfigurovatelného počtu následných pokusů použít neplatnou zapamatovanou informaci (např. použití PIN pouze pro identifikaci). Není-li počet pokusů konfigurovatelný, musí být omezen na 5 následných pokusů v rámci 30 sekund každého z nich	•	•	•	V	V	N	N
12	Vizuální indikace míst výstrahy v půdorysu střežených prostorů	•			V	V	V	P
13	Po poplachu musí být následně zobrazena instrukce	•			V	V	V	P
14	Transakce			•	V	P	P	P
15	Vizuální hlášení a záznam pro otevřený stav portálu poté, co byl povolen přístup. Může být pro jednotlivé portály programovatelný v souladu s požadavky stupně	•		•	V	V	P	P
16	Vizuální hlášení, výstraha a záznam pro stav, že portál zůstal v uzavřeném stavu poté, co byl odepřen přístup. Může být pro jednotlivé portály programovatelný v souladu s požadavky stupně	•	•	•	V	V	V	P
17	Přístup odepřen, může být pro jednotlivé portály programovatelný v souladu s požadavky stupně	•	•	•	V	V	P	P
18	Příčina odepření přístupu. Může být konfigurovatelné podle portálu a/nebo příčině odepření v souladu s požadavky stupně	•	•	•	V	V	V	P
19	Plánovaná nebo manuální změna stavu portálu			•	V	V	P	P
20	Porucha primárního zdroje napájení	•	•	•	V	V	P	P
21	Obnova primárního zdroje napájení	•		•	V	V	P	P
22	Stav problému záložního zdroje napájení (nízké napětí baterie a chybějící baterie)	•	•	•	V	V	P	P
23	Vstup a opuštění režimu konfigurace	•		•	V	V	P	P
24	Ztráta komunikace mezi řídicí jednotkou a ovládacím panelem	•	•	•	V	P	P	P
25	Kontrola přítomnosti	•		•	V	V	P	P
26	Portál uzavřen následně po násilném otevření nebo příliš dlouho otevřený portál	•		•	V	V	P	P
27	Veškeré události musí být identifikovány podle typu, místa a data kdy k nim došlo	•		•	V	V	P	P
28	Výstrahy musí obsahovat indikaci jejich priority, jestliže systém určení úrovní priority umožňuje	•		•	V	V	P	P
29	Souběžně přijaté výstrahy musí být zobrazeny podle priority, jestliže systém určení úrovní priority umožňuje	•			V	V	P	P

Tabulka 3 – Požadavky na indikaci a hlášení *(dokončení)*

	Požadavky na indikaci a hlášení	Indikace			Přiřazení stupně			
					1	2	3	4
	B – Ovládací panel (hlášení)							
		Zobrazení	Výstraha	Záznam				
30	Detekce sabotáže	•	•	•	V	P	P	P
31	Násilně otevřený portál	•	•	•	V	P	P	P
32	Vizuální hlášení, výstraha a záznam pro uplynutí povolené doby otevření (příliš dlouho otevřený portál)	•	•	•	V	P	P	P
33	Sledování karet	•		•	V	V	V	P
34	Sledování čteček	•		•	V	V	V	P
35	Off-line stav čtečky	•	•	•	V	V	V	P
36	Abnormální stav uzamykacího zařízení	•	•	•	V	V	V	P
37	Hlášení dosažení limitu 90 % od maxima kapacity prostoru pro záznam	•	•	•	V	V	P	P
38	Maximální zpoždění signálů přicházejících na ovládací panel (90 s, 45 s a 15 s)	•	•	•	V	90 s	45 s	15 s
39	Maximální zpoždění pro zobrazení instrukcí následujících výstrahu poté co na ovládací panel došla výstraha (5 s)	•	•		V	V	V	P
40	Maximální zpoždění obrázku a/nebo grafiky poté co na ovládací panel došla výstraha (6 s)	•	•		V	V	V	6 s
41	Systém musí umožňovat určení úrovní priority pro určité události výstrahy	•			V	V	P	P
42	Výstrahy přijaté na ovládacím panelu vyžadují potvrzení příjmu operátorem	•	•	•	V	V	P	P
43	Požaduje se vizuální hlášení, výstraha a záznam jestliže nebyly respektovány podmínky dvojnásobné/vícenásobné přítomnosti (není přítomen minimální počet osob)	•	•	•	V	V	V	V
44	Musí být zaznamenávány všechny operátorem iniciované změny včetně typu, identifikace operátora, čas a datum kdy nastaly			•	V	V	V	P
45	Operátorovy komentáře k výstrahám musí být zaznamenány s identifikací operátora, času a data příchodu záznamu komentáře. Musí být identifikovány specifické komentované výstrahy	•		•	V	V	V	P
46	Přístup k zaznamenaným informacím pro jejich vyvolání (událostí tj. zobrazení, tisk, export) musí být zaznamenán s identifikací operátora, času a data příchodu kdy se přístup uskutečnil			•	V	V	P	P
47	Záznamová kapacita minimálního počtu zaznamenávaných systémových událostí v průměru na čtečku			•	V	200	500	1 000

POZNÁMKA Zkratky používané v tabulce jsou následující:
N = nepovoleno
V = volitelné
P = povinné
V* = musí být implementována jedna z variant v označené skupině (šedá oblast)
N/A = neaplikovatelné

PRÍLOHA P2: POŽIADAVKY NA ROZHRANIE MISTA PRÍSTUPU

Tabulka 2 – Požadavky na rozhraní místa přístupu

	Požadavky na rozhraní místa přístupu	Přiřazení stupně			
		1	2	3	4
	A – Doba uvolnění				
1	Doba uvolnění musí být definována systémem	V*	V*	N	N
2	Doba uvolnění musí být pro jednotlivé portály konfigurovatelná	V*	V*	P	P
3	Je-li doba uvolnění definována systémem, nesmí být povolená doba kratší než 3 s	P	P	N/A	N/A
4	Je-li doba uvolnění konfigurovatelná, mohou hodnoty pro jednotlivé portály souviset s přístupovými oprávněními systému	V	V	V	V
	B – Kontrola přístupu				
5	Umožnění přístupu pro vstup do chráněného (kontrolovaného) prostoru	P	P	P	P
6	Umožnění přístupu pro odchod z chráněného (kontrolovaného) prostoru	V	P	P	P
7	Zábrana proti opakovanému průchodu s následným zamítnutím přístupu	V	V	P	P
8	Výstraha při nerespektování zábrany proti opakovanému průchodu	V	V	V	V
9	Globální zábrana proti opakovanému průchodu	V	V	V	P
10	Překonání/vyřazení zábrany proti opakovanému průchodu	V	V	V	P
11	Časově závislá zábrana proti opakovanému průchodu	V	V	V	P
12	Podmíněný přístup do data účinnosti/platnosti	V	V	P	P
13	Podmíněný přístup podle platnosti oprávnění (blokované, pozastavené, neplatné)	P	P	P	P
14	Přístup pro doprovázenou osobu	V	V	V	V
15	Režim dohlížitele	V	V	V	V
16	Dvojnásobná přítomnost (kontrola přítomnosti dvou nebo více osob)	V	V	V	V
17	Dvojnásobný přístup (přístup dvou osob)	V	V	V	P
18	Singularizace/zamezení následného průchodu více osobami	V	V	V	V
19	Kontrola výtahu	V	V	V	V
	C – Monitorování místa přístupu				
20	Místo přístupu/stav musí být monitorován	V	P	P	P
21	Přípustná doba otevření místa přístupu musí být definována systémem (doporučená doba nemá být menší než 10 s)	V	V*	N	N
22	Doba otevření místa přístupu musí být konfigurovatelná pro jednotlivé portály	V	V*	P	P
23	Jsou-li konfigurovatelné, mohou být přípustné doby otevření spojeny s přístupovými právy pro jednotlivá místa přístupu	V	V	V	V
	D – Vstupní signály				
24	Musí být zpracovávány digitální vstupní signály (tj. jiné než komunikační signály) s aktivní periodou přesahující 400 ms	V	P	P	P

POZNÁMKA Zkratky používané v tabulce jsou následující:
N = nepovoleno
V = volitelné
P = povinné
V* = musí být implementována jedna z variant v označené skupině (šedá oblast)
N/A = neaplikovatelné

PRÍLOHA P3 : POŽIADAVKY NA ROZPOZNÁVANIE

Tabulka 4 – Požadavky rozpoznávání

	Požadavky rozpoznávání	Přiřazení stupně			
		1	2	3	4
	A – Přístupové úrovně				
1	Vestavěné hodiny reálného času musí mít přesnost ±10 s za týden a umožňovat nastavení letního času a přestupného roku	V	P	P	P
2	Systém musí umožňovat více časových pásem	V	V	V	V
3	U systémů s více propojenými řídicími jednotkami musí být hodiny synchronizovány s hlavními hodinami nebo jiným spolehlivým zdrojem synchronizace nejméně jednou za 24 hodin	V	V	P	P
4	Synchronizace hlavních hodin systému s úředním časem	V	V	V	P
5	Hodiny reálného času musí být po uvedenou minimální dobu v provozu v případě úplné ztráty napájení (s výjimkou ztráty energie baterie pro uchovávání dat)	V	24 h	120 h	120 h
6	Minimální počet uživatelských přístupových úrovní	1	8	16	64
7	Minimální počet konfigurovatelných časových úseků	0	4	8	16
8	Minimální rozpoznávání pro čas v rámci přístupových úrovní zahrnující den v týdnu, hodinu a minutu denního času	N/A	P	P	P
9	Minimální rozpoznávání pro čas v rámci přístupových úrovní zahrnující den v měsíci, měsíc a rok	N/A	V	V	P
10	Systém musí být schopen zvládnout určitý počet konfigurovatelných dní (např. státní svátky, speciální pracovní dny a dny pracovního klidu)	N/A	2	16	24
11	Systém má umožňovat přidělení přístupových oprávnění skupině oprávněných jedinců	V	V	V	V
12	Systém má být schopen měnit přístupová práva skupině přístupových oprávnění v návaznosti na bezpečnostní podmínky	V	V	V	V
	B – Zařízení a způsoby identifikace				
13	Systém musí přidělit jedinečnou identifikaci každému oprávněnému uživateli	V	P	P	P
14	Systém musí používat pouze zapamatovanou informaci	V*	V*	N	N

Tabulka 4 – Požadavky rozpoznávání *(dokončení)*

	Požadavky rozpoznávání	Přiřazení stupně			
		1	2	3	4
	B – Zařízení a způsoby identifikace				
15	Systém musí používat buď jen biometrii, nebo v kombinaci s dalšími způsoby rozpoznávání	V*	V*	V*	V*
16	Systém musí používat identifikační prostředky	V*	V*	V*	V*
17	Systém musí používat zapamatovanou informaci a identifikační prostředky	V*	V*	V*	V*
18	Přístup musí být odmítnut po každém pokusu o získání přístupu s použitím identifikačního prostředku s neplatnou zapamatovanou informací a po předdefinovaném počtu neúspěšných pokusů o získání přístupu s identifikačním prostředkem s přístupovými oprávněními pozastavenými na přednastavené trvání. Počet pokusů může být konfigurovatelný. Není-li konfigurovatelný, musí být počet pokusů omezen na 5	V	P	P	P
19	Přístup musí být odmítnut po každém pokusu o získání přístupu jen s neplatnou zapamatovanou informací. Přístup musí být vyloučen po 5 následných nesprávných zadání v rámci přednastaveného časového úseku	V	V	N/A	N/A
20	Při použití biometrie nesmí FAR_{eff} překročit limit stanovený pro každý stupeň. POZNÁMKA 1 $FAR_{eff} = FAR$ (četnost falešných přijetí) je-li prováděno porovnávání 1:1 (např. biometrická verifikace identity potvrzená zapamatovanou informací nebo identifikačním prostředkem) nebo $FAR_{eff} = FAR \times n$ je-li prováděno porovnávání 1:n a n = počet uložených vzorků (např. biometrická verifikace identity bez použití zapamatované informace nebo identifikačního prostředku). POZNÁMKA 2 Hodnoty FAR jsou založeny na přehledu údajů ve výrobcem přiložené dokumentaci.	1 %	0,3 %	0,3 %	0,1 %
21	Minimální poměr mezi počtem možných uživatelských kódů a počtem přidělených kódů musí být nejméně 1 000 ku 1, je-li systém používán k rozpoznávání uživatelů pouze zaznamenanou informací Např.: do 10 uživatelů – 4 číslice, do 100 uživatelů – 5 číslic, do 1 000 uživatelů – 6 číslic; atd.	P	P	N/A	N/A
22	Pro systémy používající rozpoznávání uživatelů zapamatovanou informací v kombinaci s identifikačním prostředkem nebo biometrií vyžaduje zapamatovaná informace nejméně 4 číslice	V	V	P	P
23	V normálním provozním režimu musí systém pro identifikaci používat kompletní informaci identifikačního prostředku (kód objektu a číslo karty, nebo jedinečné číslo karty)	P	P	P	P
24	Podpora pro vícenásobné kódy objektů, jestliže systém používá kódy objektů	V	V	V	P
25	V degradovaném režimu činnosti může systém pro identifikaci používat částečnou informaci identifikačního prostředku (např. pouze kód objektu).	V	V	V	N
26	Nesmí být používány identifikační prvky se strukturou kódovacího systému viditelnou pouhým okem	P	P	P	P
27	Identifikační číslo identifikačního prostředku nemá být přímou reprezentací celého kódování	P	P	P	P

POZNÁMKA Zkratky používané v tabulce jsou následující:
N = nepovoleno
V = volitelné
V* = musí být implementována jedna z variant v označené skupině (šedá oblast). Viz také doplňující požadavky na identifikační prostředky pro každý stupeň. Položka 9) v 6.8
P = povinné
N/A = neaplikovatelné

PRÍLOHA P4 : POŽIADAVKY NA SIGNALIZACIU NÁTLAKU

Tabulka 5 – Požadavky na signalizaci nátlaku

Požadavky na signalizaci nátlaku		Přiřazení stupně			
		1	2	3	4
1	Aktivování funkce signalizace nátlaku musí být konfigurovatelné	V	V	V	P
2	Výstraha nátlaku na ovládacím panelu má být odlišná od ostatních výstrah	P*	P*	P*	P
3	Činnost iniciačního zařízení výstrahy nesmí vyvolat signál, který by mohl být slyšitelný nebo viditelný v místě, kde byla signalizace nátlaku vyvolána	P*	P*	P*	P

POZNÁMKA Zkratky používané v tabulce jsou následující:
V = volitelné
P = povinné
P* = povinné pouze je-li volitelná funkce podporována pro určitý stupeň

PRÍLOHA P5 : POŽIADAVKY NA VLASTNU OCHRANU SYSTÉMU

Tabulka 7 – Požadavky na vlastní ochranu systému *(dokončení)*

	Požadavky na vlastní ochranu systému	Přiřazení stupně			
		1	2	3	4
	A – Prevence				
17	Minimální doba zachování dat pro zaznamenané události uložené v řídicí jednotce systému pro kontrolu vstupu během provozní ztráty napájení (v důsledku ztráty komunikace s ovládacím panelem) musí odpovídat uvedeným hodnotám	V	24 h	120 h	120 h
18	U veřejně sdílených sítí (např. internet) se požaduje šifrování komunikačních signálů mezi komponentami EACS	V	V	P	P
19	Informace uložené na identifikačním prostředku musí být chráněny proti neoprávněné modifikaci nebo kopírování	V	V	P	P
20	Porucha nebo obnovení komunikačního kanálu nesmí mít za následek uvolnění místa přístupu	P	P	P	P
21	Porucha komunikace s ovládacím panelem nesmí přerušit proces rozhodování o přístupu	P	P	P	P
22	Procesní pravidla uložená ve čtečce místa přístupu nesmí být pro uživatele systému viditelná	P	P	P	P
23	Světelné nebo zvukové indikátory aktivace stisku kláves klávesnice nesmí být přímou reprezentací skutečných kódů, ale musí mít stejnou výšku tónu a trvání	P	P	P	P
24	Komunikace mezi čtečkami a řídicími jednotkami musí umožňovat šifrování s autentizací	V	V	V*	P
25	Návod k obsluze musí obsahovat podrobné montážní požadavky pro mechanickou ochranu omezující přístup ke komunikačním spojům mezi čtečkami a řídicí jednotkou systému kontroly vstupu	V	V	V*	V
	B – Detekce a podávání zpráv				
26	Změna stavu digitálního vstupu detekčního obvodu (otevřeno, zavřeno, sabotáž (rozpojení nebo sepnutí sabotážního kontaktu)) musí být výrobcem konstruován tak, že se tolerance pro každý stav vstupního obvodu nesmí překrývat se sousedním stavem	V	V	P	P
27	Validace systému vstupu dat. Systém musí poskytovat hlášení na ovládacím panelu, jestliže byla v průběhu konfiguračního režimu vložena neplatná data.	P	P	P	P
28	Přístup ke konfiguračnímu režimu se musí přerušit po překročení přednastavené doby nečinnosti	P	P	P	P

POZNÁMKA Zkratky používané v tabulce jsou následující:

N = nepovoleno

V = volitelné

P = povinné

V* = musí být implementována jedna z variant v označené skupině (šedá oblast)

N/A = neaplikovatelné

PRÍLOHA P6 : POŽIADAVKY NA NAPÁJANIE

Tabulka 8 – Požadavky na napájení

Požadavky na napájení		Přiřazení stupně			
		1	2	3	4
1	Řídicí jednotka systému kontroly vstupu musí být vybavena záložním zdrojem napájení, schopným zajistit provoz systému a jeho příslušenství ve stavu specifikovaného plného zatížení po uvedenou dobu. (Podmínky zatížení nezahrnují ovládací panel nebo aktivační prvky přístupových míst)	V	V	2 h	4 h
2	Po delším výpadku primárního zdroje napájení (nastalo přerušení činnosti systému) a obnovení napájení musí být baterie dobity na 80 % jmenovité kapacity během 24 hodin a na 100 % jmenovité kapacity během 72 hodin	P	P	P	P
3	Výpadek primárního zdroje napájení nebo jeho obnovení nesmí negativně ovlivnit normální činnost systému.	V	V	P	P
4	Jestliže je zajištěn záložní zdroj napájení, musí být možné monitorovat jeho následující stavy: nízké napětí a baterie není přítomna (akceptovatelné je společné hlášení obou stavů)	V	V	P	P
POZNÁMKA Zkratky používané v tabulce jsou následující: V = volitelné P = povinné					