Česká zemědělská univerzita v Praze

Technická fakulta

Bezpečnostní systémy a možnosti jejich integrace

Diplomová práce

Vedoucí práce: Ing. Jan Hart, Ph.D.

Autor práce: Bc. Marek Častalovský

Praha 2018

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Marek Častalovský

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Bezpečnostní systémy a možnosti jejich integrace

Název anglicky

Security systems and their integration possibilities

Cíle práce

Diplomová práce je tematicky zaměřena na integraci bezpečnostních systémů. Hlavním cílem je provést monitoring integrace různých systémů a to včetně rozboru této problematiky s přihlédnutím k současným normám a omezením, které na jejich základě vznikají. Dílčí cíle diplomové práce jsou:
- vytvořit přehled řešené problematiky,
- provést rozbor možností integrace pro jednotlivé zabezpečovací systémy
- na základě rozboru možností integrace u jednotlivých bezpečnostních systémů porovnat možnosti jednotlivých integračních softwareů a na základě patřičných norem pak vytvořit plně integrovaný celek bezpečnostních systémů pro malé a střední objekty.

Metodika

Metodika řešené problematiky diplomové práce je založena na studiu a analýzách odborných informačních zdrojů. Praktická část práce je zaměřena na integraci prvků bezpečnostních systémů a následné zpracování zjištěných veličin a dat. Na základě rozboru teoretických poznatků a výsledků praktické části práce budou formulovány závěry diplomové práce.

Doporučený rozsah práce

50 až 60 stran včetně grafů, tabulek a obrázků

Klíčová slova

integrace, kamerový systém, poplachový zabezpečovací a tísňové systémy, integrační software

---

Doporučené zdroje informací

HEŘMAN, J., et al.: Elektrotechnické a telekomunikační instalace. Praha: VerlagDashöfer, 2008. ISSN 1803-0475

KŘEČEK, S., a spol.,: Příručka zabezpečovací techniky. Blatná: Circetus, 2006. 313s. ISBN 80-902938-2-4

UHLÁŘ, J.,: Technická ochrana objektů, II.díl, Elektrické zabezpečovací systémy II. Praha: PA ČR, 2005. 229s. ISBN 80-7251-189-0

Předběžný termín obhajoby

2017/18 LS – TF

Vedoucí práce

Ing. Jan Hart, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 12. 1. 2017

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 23. 1. 2017

prof. Ing. Vladimír Jurča, CSc.

Děkan

V Praze dne 18. 03. 2018

Prohlášení

Prohlašuji, že jsem diplomovou práci na téma: Bezpečnostní systémy a možnosti jejich integrace vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním diplomové práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje diplomová práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom 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, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

.....

Bc. Marek Častalovský

V Praze dne 22. 3. 2018

Poděkování

Děkuji svému vedoucímu Ing. Janu Hartovi, Ph.D. za vedení práce a mnohé rady, které napomohli u jejího vzniku. Dále bych chtěl poděkovat zaměstnancům firmy Alarm Absolon s.r.o. za konzultace, které mi poskytli.

Abstrakt

Práce se zabývá problematikou bezpečnostních technologií a možností jejich integrace do jednoho celku. Rešeršní část rozebírá jednotlivé technologie a popisuje jejich jednotlivé prvky, z kterých se skládají a také základy jejich fungování. Důraz je kladen na poplachové, zabezpečovací a tísňové systémy, vzhledem k jejich častému nasazování v praxi. V kapitole, která se jím věnuje jsou podrobně uvedeny jednotlivé prvky tohoto systému a detailněji jsou probrány možnosti ovládání a komunikace tohoto systému. Na základě tohoto rozboru je možné udělat si představu o fungování bezpečnostních technologií, které jsou v současné době používány. Následně je v rešeršní části představen obecný integrační software a jsou popsány jeho možnosti a oblasti nasazení. Dále jsou uvedeny možnosti propojení integračních softwarů a technologií. Na základě tohoto rozboru je možné udělat si představu o fungování integračních softwarů. Praktická část práce se zabývá výměnou starého poplachového, zabezpečovacího a tísňového systému za nový, který je vybrán v multikriteriální analýze. Po provedení výměny se práce věnuje integraci do vybraného integračního software, který je vybrán v multikriteriální analýze. Výsledkem je provedení výměny starého systému a následná instalace nového, včetně jeho oživení a následná integrace do integračního softwaru C4 s kamerovým systémem Hikvision.

Klíčová slova: poplachový, zabezpečovací a tísňový systém, kamerový systém, elektronická požární signalizace, elektronická kontrola vstupu, integrační software

Security systems and their integration possibilities

Abstract

The thesis deals with problematics of security technologies and possibilities of their integration into one unit. The research part analyzes the individual technologies and describes their individual elements, which they consist of, as well as the basics of their functionality. Emphasis is placed on intrusion alarm system due to their frequent use at installations. In the chapter devoted to it's details, elements of this system and the possibilities of control and communication of this system are discussed in more detail. Based on this analysis, it is possible to get knowledge of the functioning of the security technologies currently in use. Subsequently, the general integration software is intoduced in the research section and it's possibilities and areas of deployment are described. Then there are the possibilities of connecting integration software and technologies. Based on this analysis, it is possible to get an idea of integration software functionality. The practical part deals with the replacement of the old intrusion alarm system by new one, which is selected in a multi-criteria analysis. After the change, the thesis deals with integration into selected integration software, which is selected in a multi-criteria analysis. The result is the replacement of the old system and the subsequent installation of new one, including it's setting and subsequent integration with the integration software C4 with the Hikvision closed circuit television.

Keywords: Intrusion alarm system, closed circuit television, access control system, fire protection system, integration software

Obsah

1 Úvod

V dnešní době je nezbytné chránit majetek a lidské životy více než kdykoli v minulosti, protože se objevují stále nové hrozby, které mohou zapříčinit ztrátu majetku a ohrozit lidské životy. V dřívějších dobách bylo možné tyto hrozby z velké části eliminovat pomocí mechanických zábran. V dnešní době jsou hrozby mnohem komplexnější, a proto je nezbytné používat dokonalejší bezpečnostní systémy, především doplnit obvyklé mechanické zábrany o elektronické bezpečnostní systémy.

Elektronické bezpečnostní systémy jsou moderní elektronické zařízení, které mají za úkol detekovat narušitele, zaznamenat ho při narušení bezpečné oblasti a v kombinaci s mechanickými zábranami ho udržet mimo tuto oblast. Dalším častým úkolem je detekce událostí, které mohou ohrozit životy lidí v bezpečné oblasti. Jedná se například o požáry nebo úniky nebezpečných plynů. Pokud dojde k detekci narušitele nebo detekci nebezpečné události, úkolem bezpečnostních systémů je upozornit obsluhu, a pokud mohou, tak minimalizovat následky nastalé události. V praxi se využívá kombinace více technologií, které mají za úkol ochranu majetku a lidských životů. Jedná se především o poplachové, zabezpečovací a tísňové systémy, elektronické požární systémy, kamerové systémy a přístupové systémy.

Obsluha kombinace výše uvedených technologií může být komplikovaná, a proto jsou objekty, na kterých jsou tyto technologie instalovány často doplněny o integrační softwary. Integrační softwary umožňují obsluze obsluhovat všechny technologie z jednoho grafického prostředí, což snižuje nároky na obsluhu. Díky tomuto je možné také rychleji reagovat na události ohrožující bezpečnost.

2 Cíl práce

Diplomová práce je tematicky zaměřena na integraci bezpečnostních systémů. Hlavním cílem je provést monitoring integrace různých systémů, a to včetně rozboru této problematiky s přihlédnutím k současným normám a omezením, které na jejich základě vznikají. Dílčí cíle diplomové práce jsou:

- vytvořit přehled řešené problematiky

- detailně se zaměřit na fungování poplachových, zabezpečovacích a tísňových systémů

- provést rozbor možností integrace pro jednotlivé zabezpečovací systémy

- na základě rozboru možností integrace u jednotlivých bezpečnostních systémů porovnat možnosti jednotlivých integračních softwarů a na základě patřičných norem pak vytvořit plně integrovaný celek bezpečnostních systémů pro malé a střední objekty.

- provést instalaci PZTS

- provést integraci instalované PZTS do vhodného integračního SW

3 Metodika práce

Prvně bude nezbytné prostudovat doporučenou literaturu k vytvoření představy o řešené problematice. Následně se vytvoří detailněji provedený rozbor poplachových, zabezpečovacích a tísňových systémů, dále bude vytvořen stručný rozbor kamerových systémů, elektronické požární signalizace a přístupových systémů. Provede se prostudování literatury týkající se integračních softwarů a na základě nabytých znalostí se vytvoří rozbor integračních softwarů. Srovnají se zabezpečovací systémy pro velké instalace v multikriteriální analýze a na základě této analýzy bude vybrán vhodný systém pro instalaci. Srovnají se integrační softwary v multikriteriální analýze a na základě této analýzy bude vybrán vhodný integrační software pro instalaci. Následně bude získán objekt pro instalaci nového zabezpečovací systému, na tomto objektu se provede demontáž starého systému a instalace nového. Po provedení instalace se provede integrace nového systému do integračního softwaru C4 společně s kamerovým systémem Hikvision, který je již na objektu nainstalován. Výsledkem bude integrované řešení pro snadné ovládání a správu obou technologií.

4 Přehled řešené problematiky

První elektronický systém pro ochranu majetku vznikl roku 1853 v Americe a jeho tvůrcem byl Augustus Russell Pope. Tento alarm byl tvořen pouze proudovou smyčkou pro detekci otevření dveří nebo oken a sirénou pro akustickou signalizaci. Patent na alarm byl prodán Edwinu Holmesovi. Ten se zasadil o rozšíření podobných jednoduchých alarmů. V roce 1858 také vytvořil první monitorovací stanici, dnes nazývanou pult centrální ochrany (zkráceně PCO). Pro připojení jednotlivých alarmů využil již natažených telefonních kabelů. V této době byla detekční technologie omezena pouze na proudovou smyčku a destruktivní detektory (například natažené lanko před oknem). Postupem času byly vynalezeny další detekční technologie a samotné ústředny byly zdokonaleny do dnešní podoby. Rozvoj dalších technologií pro ochranu majetku a osob následoval především během 20. století.[1,2]

4.1 Bezpečnostní systémy

Pojmem bezpečnostní systémy je označováno více systémů, které mají za úkol ochranu lidí a majetku. Mezi tyto systémy patří především poplachové, zabezpečovací a tísňové systémy (PZTS), kamerové systémy (CCTV - Closed Circuit Television), elektrická požární signalizace (EPS), elektronická kontrola vstupu (EKV nebo častěji ACS, z anglického Access Control Systems), a další. Výše uvedené systémy se nasazují samostatně nebo v kombinaci, záleží na objektu a podmínkách, na kterém jsou tyto systémy nasazovány.[3,4,5]

Na rodinných domech se nejčastěji používá pouze PZTS, případně kombinace PZTS s CCTV. Vzhledem k nutnosti osazení domu protipožární ochranou pro kolaudaci se dnešní novostavby rodinných domů osazují autonomním požárním detektorem, případně požárním detektorem připojeným do PZTS. Již postavené rodinné domy jsou osazovány především PZTS.[3,4,5]

U nově vybudovaných komerčních objektů se dnes již stává standardem užití PZTS a CCTV, k tomu také plnohodnotná EPS, která je vyžadována legislativou. Také se rozšiřuje využití ACS, která může být integrována v ústředně PZTS, nebo může být samostatná. Dále se také rozšiřují elektronické docházkové systémy, které usnadňují evidenci docházky a generují vhodné výstupy pro mzdové oddělení. [3,4,5]

4.1.1 Poplachové, zabezpečovací a tísňové systémy

Účelem PZTS je především ochrana majetku. Může se jednat o prostory, objekty nebo jednotlivé předměty. Nicméně na specifických místech může být hlavním účelem i ochrana osob. Příkladem jsou věznice, kde PZTS pomáhá dohlížet, aby vězni zůstali kde mají a nedošlo k ohrožení vězeňské služby. [3]

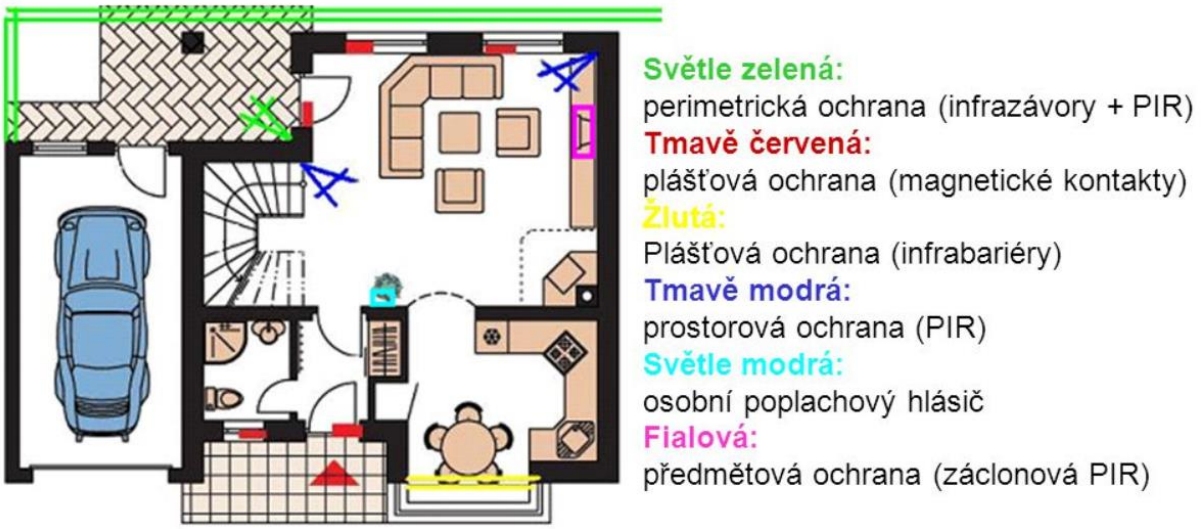
Předmětová ochrana se zabývá ochranou cenných předmětů. Nejčastěji se jedná o umělecká díla v galeriích a na dalších místech, kde jsou veřejně vystavována. Dále také může jít o ochranu trezorů v bankách. Cílem této ochrany je tedy zabezpečení jednotlivých předmětů. Nejčastěji využívané technologie jsou Michelangelo, Ladon, Vincent Van Gogh, Raffael a Piccasso. [3,5]

Plášťová a prostorová ochrana se zabývá ochranou vnitřních prostor objektů a plášťů budov. Plášťová ochrana se zabývá detekcí narušitele při vniknutí do objektu. Nejčastěji je realizována pomocí magnetických kontaktů a detektorů tříštění skla. Nevýhodou plášťové ochrany oproti perimetrické ochraně je, že obvykle dojde k poškození objektu dříve (rozbití okna, vypáčení dveří), než je pachatel detekován. Prostorová ochrana je nejčastěji realizována pomocí PIR (Passive Infrared), PIR + MW (Micro Wave) detektorů, detektorů tříštění skla a magnetických kontaktů. Cílem prostorové ochrany je detekce narušitele, pokud se mu povedlo vniknout do objetu, a nebyl detekován již plášťovou ochranou. Plášťová a prostorová ochrana má značnou výhodu oproti perimetrické v počtu falešných poplachů. U perimetrické ochrany i při ideálním nastavení citlivosti detekční technologie musíme počítat s falešnými poplachy.[3,5]

Perimetrická ochrana se zabývá ochranou obvodu pozemku kolem chráněného objektu. Elektronická perimetrická ochrana se vždy kombinuje s mechanickou perimetrickou ochranou, jako jsou například ploty, valy, přírodní překážky a další. Úkolem perimetrické ochrany je zachytit narušitele již při vstupu na pozemek, případně odrazení narušitele od pokusu vniknout na pozemek. Dále perimetrická ochrana detekuje narušitele bez toho, aniž by došlo k poškození majetku, na rozdíl od objektové ochrany (plot většinou vydrží přelezení), kdy pachatel musí vniknout do objektu, a tak se dá počítat s poškozením dveří či oken. [3,5]

Detektory použité v perimetrické ochraně musí disponovat širším rozsahem pracovních teplot a také IP (International Protection Marking) krytím. Mezi nejčastěji používané technologie patří PIR a MW detektory a závory, zemní detekční kabely a plotové systémy. [3,5]

Obrázek 1 Příklady ochrany ukazuje, jak je který způsob ochrany realizován. Na tomto obrázku jsou k vidění příklady všech výše zmíněných ochran.



Obrázek 1 Příklady ochrany

[Online]: http://slideplayer.cz/slide/2008692/ (Staženo 6.1. 2018)

4.1.1.1 Norma ČSN EN 50131

Norma ČSN EN 50131 se zabývá PZTS. Tato norma se skládá z více částí, hlavní je ČSN EN 50131-1 ed.2. V této části jsou popsány hlavní požadavky na systém, v ostatních částech jsou požadavky na jednotlivé komponenty. V Tabulka 1 Norma ČSN EN 50131 je kompletní rozpis všech částí normy ČSN EN 50131 z které je patrné, čím vším se norma pro PZTS zabývá.[6]

Tabulka 1 Norma ČSN EN 50131

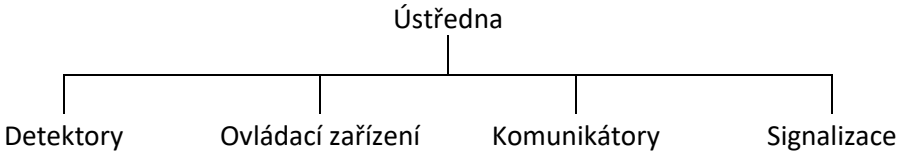
Část 1	Systémové požadavky
Část 2-2	Požadavky na pasivní infračervené detektory
Část 2-3	Požadavky na mikrovlnné detektory
Část 2-4	Požadavky na kombinované pasivní infračervené a mikrovlnné detektory
Část 2-5	Požadavky na kombinované pasivní infračervené a ultrazvukové detektory
Část 2-6	Požadavky na kontakty otevření (magnetické)
Část 2-7	Detektory vniknutí – detektory rozbíjené skla akustické nebo otřesové
Část 3	Ústředny PZTS
Část 4	Výstražná zařízení
Část 5-3	Požadavky na zařízení využívající bezdrátového propojení
Část 6	Napájecí zdroje
Část 7	Pokyny pro aplikace
Část 8	Zabezpečovací zamlžovací zařízení
Část 9	Verifikace poplachu – metody a principy
Část 10	Aplikace specifických požadavků na komunikátory ve střeženém prostoru (SPT)

Norma ČSN EN 50131-1 rozděluje PZTS na čtyři stupně zabezpečení dle schopnosti PZTS odolávat sabotáži podle zkušenosti narušitele a dalších parametrů. Stupeň 1 je definován jako Nízké riziko, kde se předpokládá, že narušitel nemá žádnou znalost instalovaného systému a má k dispozici pouze jednoduché nástroje, jako je například kladivo. Stupeň 2 je definován jako Nízké až střední riziko, kde se předpokládá, že narušitel má malou znalost instalovaného systému a má pouze běžné nářadí. Stupeň 3 je definován jako Střední až vysoké riziko, kde se předpokládá, že narušitel má omezené znalosti instalovaného systému a disponuje běžným nářadím v kombinaci s přenosnými přístroji. Stupeň 4 je definován jako Vysoké riziko, kde se

předpokládá, že narušitel je znalý nainstalovaného systému a disponuje veškerou možnou technikou k sabotáži systému. [6]

4.1.1.2 Prvky PZTS

PZTS se skládá z více prvků, které se dohromady starají o ochranu objektu. Základní prvky jsou k vidění na Obrázek 2 Struktura PZTS.[5,7,8]



Obrázek 2 Struktura PZTS

Zdroj: Archív autora

Ústředna je základním prvkem PZTS. Stará se o vyhodnocování všech vstupů a následnou realizaci definovaných činností. Dále zajišťuje napájení ostatních připojených prvků. Vzhledem k tomu, že ústředna je základním prvkem celého PZTS, je nutné ji vhodně umístit v objektu, aby nebyla snadno dosažitelná. Typická PZTS ústředna je vyobrazena na Obrázek 3 Ústředna PZTS.[3,5,7,8]

Obrázek 3 Ústředna PZTS

[Online]: https://eshop.eurosat.cz/image/380065/ (Staženo 9.1. 2018)

Detektory slouží k detekci narušitele ve střeženém prostoru. Nejčastěji je používáno PIR nebo PIR + MW detektorů a magnetických kontaktů. Tyto detektory mohou být připojeny k expandérům vstupů nebo přímo k ústředně. Obvyklé detektory jsou vyobrazeny na Obrázek 4 Stropní detektor a Obrázek 5 Magnetický kontakt. [3,7,8,9]

Obrázek 4 Stropní detektor

[Online]: http://www.thecrowgroup.com/Products_Systems/tlc360/tlc360/360.jpg (Staženo 9.1. 2018)

Obrázek 5 Magnetický kontakt

[Online]: http://www.asita.cz/downloads/mas_zapustny_hl.jpg (Staženo 9.1. 2018)

Signalizace slouží především k lokální signalizaci poplachů, ale i případných dalších stavů, které bude chtít uživatel signalizovat. Provedení typické venkovní sirény je na Obrázek 6 Venkovní siréna.[3,8]

Obrázek 6 Venkovní siréna

[Online]: https://www.riscogroup.com/sites/default/files/Lumin%208%20Wired%20Blue-_MG_0419%2873%29%20540x510%20side_0.JPG (Staženo 9.1. 2018)

Ovládací zařízení mají na starost zprostředkovat uživatelům ovládání a případně umožnit instalačním technikům nastavování systému. Nejčastějším ovládacím prvkem je klávesnice. Na Obrázek 7 Klávesnice je k vidění klávesnice pro pohodlné ovládání PZTS.[3,7,8]

Obrázek 7 Klávesnice

[Online]: https://eshop.eurosat.cz/image/565413/ (Staženo 9.1. 2018)

Komunikátory složí pro přenos poplachové informace majiteli objektu, případně pro přenos na PCO. Komunikátory jsou více popsány níže. [3,7,8]

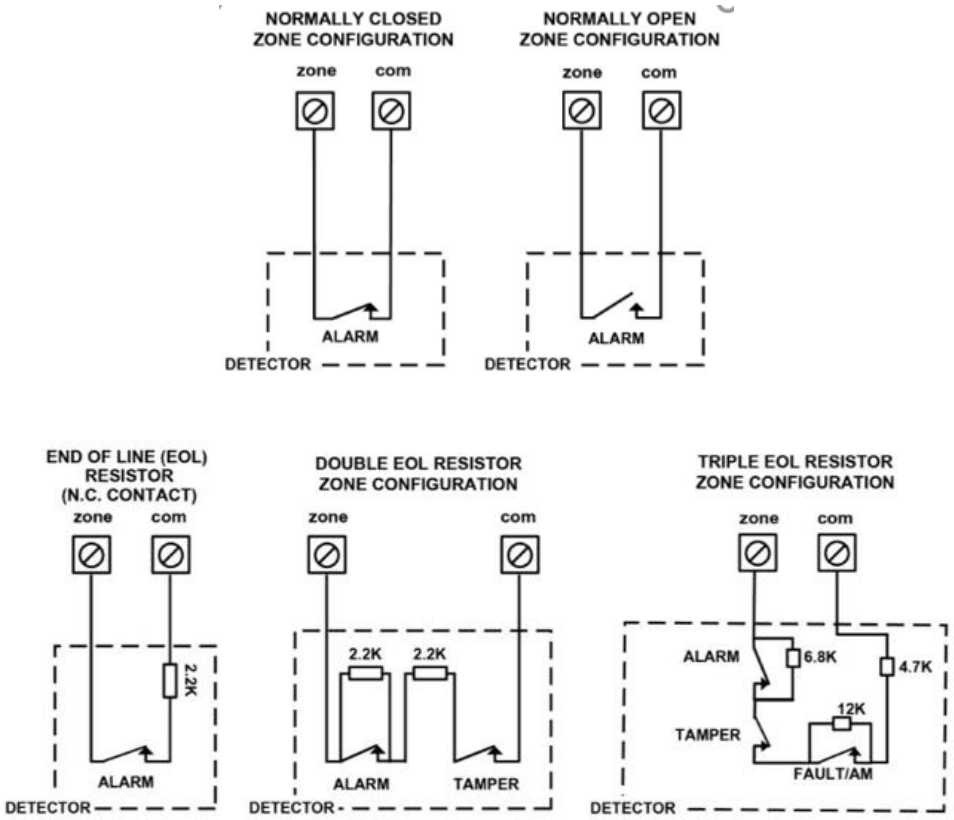
4.1.1.3 Propojení prvků PZTS

Pro komunikaci s klávesnicemi a expandéry vstupů a výstupů se používá sběrnice. Obvykle se jedná o modifikovanou RS-485 daným výrobcem, případně se tyto periferie připojují bezdrátovým přenosem. Pokud budou připojeny sběrnicové moduly k ústředně, budou připojeny nejčastěji po RS-485. RS-485 má omezenou maximální délku po metalickém vodiči, proto je možné sběrnici vést i optickými vodiči. Toto řešení se využívá k propojení více budov, kde optické propojení zaručí i galvanické oddělení, případně ve velkých skladech, kde jsou vzdálenosti mezi jednotlivými prvky příliš velké. Připojené moduly a klávesnice mají svou adresu, kterou se na sběrnici hlásí. Tato adresa se nejčastěji nastavuje pomocí DIP přepínačů, které jsou na modulu. Výše popsané moduly se dají také připojit k ústředně pomocí bezdrátového přenosu, nicméně je snadné tento přenos rušit pomocí rušičky. Kvůli tomuto je vhodné nasazovat sběrnicové systémy, kde je možné natahat nezbytnou kabeláž pro tyto systémy. [3,9,10]

Připojení detektorů může být realizováno třemi způsoby. Mohou být připojeny na sběrnici, obdobně jako výše popsané klávesnice a expandéry, dále mohou být připojeny k jednotlivým vstupním expandérům nebo jsou připojeny bezdrátově. Pokud jsou připojeny na sběrnici,

nastavuje se jim adresa podobně jako klávesnicím a modulům. Pokud je detektor připojen k expandéru, tak je připojen na principu proudové smyčky. Je možné realizovat více zapojení, díky kterým je možné rozpoznat více stavů na detektoru. Nejčastěji se jedná o rozeznání poplachu, tamperu a antimaskingu (schopnost detektovat přiblížení k detektoru v řádu desítek centimetrů) nebo poruchy (pokud má detektor schopnost samotestu). Bezdrátově připojené detektory se připojují k bezdrátovému vysílači ústředny. Parametry detektorů jsou nastaveny v SW. Nicméně je problémem, že přenos bezdrátových čidel může být snadno rušen, proto neposkytují takovou ochranu, jako fyzicky připojené detektory.[3,9,10]

Možná smyčková zapojení jsou **NO** (Normaly open), **NC** (Normaly closed), **EOL** (End of line), **DEOL** (Double end of line), **TEOL** (Triple end of line). Někteří výrobci také přišli se zapojením **ATZ** (Advanced technology zoning) a **ATZ EOL**. NO zapojení se používá především pro připojení požárních detektorů do PZTS. NO znamená, že proudová smyčka je v klidovém stavu rozpojena a při poplachu na detektoru je spojena. U NO zapojení se počítá s tím, že dojde k vyhlášení poplachu tehdy, pokud dojde ke spálení izolace vodičů a tím dojde k uzavření smyčky. Tohoto efektu se využívá především u požárních detektorů. NC je nevyvážená proudová smyčka pro zapojení detektorů, kde je minimální riziko sabotáže. Toto zapojení není obecně doporučováno, kvůli jednoduché možnosti sabotáže. Takto zapojený detektor je možno přemostit, a tím ho vyřadit. EOL zapojení slouží k znesnadnění sabotáže smyčky. Jeden vyvažující odpor se přidá do detektoru, a pokud by došlo k přemostění smyčky, potom by se změnilo napětí ve smyčce, což dokáže ústředna vyhodnotit jako napadení systému a vyhlásit poplach. DEOL zapojení je podobné jako EOL, ale přidává možnost rozlišení 2 stavů na detektoru. Nejčastěji se jedná o detekci narušitele a o poplach ze sabotážního kontaktu (tamper). TEOL zapojení je podobné jako DEOL, ale přidává možnost rozlišení dalšího stavu na detektoru. Zapojení ATZ je zapojení dvou detektorů na jednu smyčku a rozeznávání jednotlivých detektorů pomocí odporů. Realizace výše popsaných zapojení je na Obrázek 8 Zapojení detektorů 1 a Obrázek 9 Zapojení detektorů 2. [3,9,10]



Obrázek 8 Zapojení detektorů 1

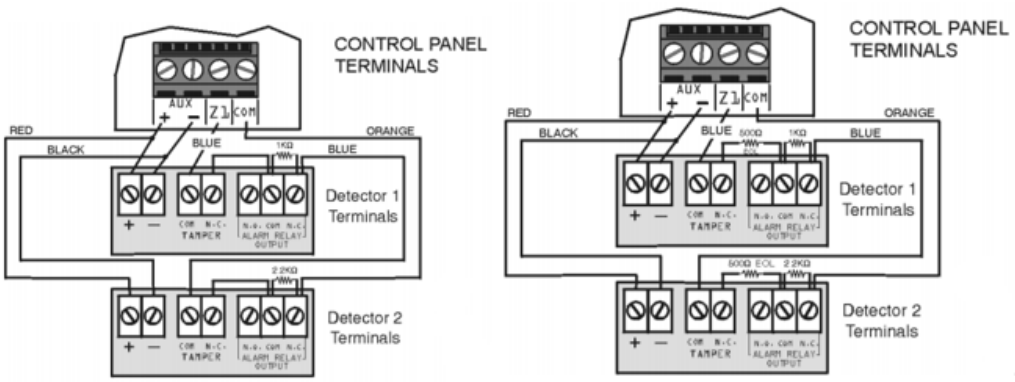
[Online]:

https://www.riscogroup.com/downloader/51519/25b2830e885552c9bdafd2faac99cc2a

(Staženo 12.1. 2018)

ATZ s rozpoznáním tamperu

ATZ s rozpoznáním taperu a EOL



Obrázek 9 Zapojení detektorů 2

[Online]: https://eshop.eurosat.cz/product/61807/2324/evohd/im.pdf (Staženo 12.1. 2018)

4.1.1.4 Signalizace

Signalizaci PZTS můžeme rozdělit na lokální a dálkovou. Obvykle se využívá kombinace obou signalizací pro dosažení maximální efektivity PZTS.[3,5,11]

Lokální signalizace je nejčastěji řešena pomocí vnitřních nebo venkovních sirén. Tyto sirény by měly být zálohované vlastním akumulátorem, aby dokázaly signalizovat přerušení jejich vedení od ústředny. Existují i bezdrátové sirény, které není možné fyzicky odstřihnout od ústředny, ale je možné jim rušit bezdrátový přenos informace o poplachu k siréně. Instalace lokální signalizace na vhodné místo může mít dva efekty. Prvním efektem je preventivní funkce, kdy případný narušitel bude preferovat dům, na kterém sirénu neuvidí. Druhým efektem je informativní funkce. Pokud bude k objektu při poplachu vyslána policie nebo bezpečnostní služba, hlasité houkání sirény a blikání majáku jim ulehčí lokaci objektu, a tím se zvýší pravděpodobnost zastavení narušitele a jeho dopadení.[3,5,7,11]

Dálková signalizace je přenos informace o poplachu na PCO, kde je neustálý dohled a kde probíhá okamžitá reakce na poplach. Nejčastěji se jedná o vyslání fyzické ostrahy k objektu, kde vznikl poplach, nebo se může jednat o kontaktování policie. Další možností je kontakt majitele objektu, který následně reaguje dle svého uvážení (například povoláním policie).[3,5,7,11]

4.1.1.5 Ovládání

Ovládání ústředny může být realizováno mnoha způsoby. Nejčastěji se používá klávesnice s případnými čipy, bezdrátové ovladače, telefonní aplikace a SMS (Short message service) zprávy.[3,5,12]

Klávesnice je základní zařízení pro ovládání systému. Klávesnice také umožňuje nastavování parametrů ústředny. Ovládání uživatelem spočívá v zadání kódu a stisknutí příslušného tlačítka pro zastřežení nebo odstřežení. Zadání kódu může být nahrazeno přiložením čipu.[3,5,12]

Bezdrátové ovladače jsou bezdrátová zařízení pro jednoduché ovládání systému. Bezdrátové ovladače obvykle mají několik tlačítek s jasně nadefinovanými funkcemi.[3,5,12]

Telefonní aplikace je nedávnou novinkou v PTZS. Tyto aplikace umožňují ovládání systému, také jsou schopny ovládat případné výstupy. Aplikace dokáží zobrazit i poruchy systému.

Sofistikovanější ústředny disponují možností propojení IP (Internet Protocol) kamer s ústřednou pro video verifikaci poplachů a případné živé video ze střeženého objektu. Tyto funkce jsou možné právě díky aplikaci v telefonu. Před telefonními aplikacemi se používalo SMS zpráv k ovládání. Obvykle se zaslala SMS obsahující kód a příkaz, který má ústředna provést.[3,5,12]

4.1.1.6 Komunikátory

Přenos zpráv z PZTS se dá rozdělit na tři destinace – na uživatele (majitele objektů), PCO a integrační SW. Majitelé dostávají informace v podobě prostého textu, zatímco na PCO chodí zpráva kódována v CID (Contact ID) formátu, případně v SIA (Security Industry Association) formátu (v ČR se nepoužívá). Integrační SW jsou s PZTS obvykle propojeny pomocí IP komunikátoru a dochází k oboustranné výměně dat. Některé PZTS mohou být ovšem připojeny i jinou cestou, nejčastěji se jedná o přímé připojení na systémovou sběrnici a pomocí převodníku být připojeny do integračních SW.[3,4,5]

Pro přenos poplachové informace se používají především čtyři kanály. Prvním z nich je JTS (jednotná telekomunikační síť), dalším je GSM (Global System for Mobile Communications), dále IP sít a posledním je rádiový přenos ve vyhrazeném pásmu.[3,4,5]

JTS je nejstarší přenosový kanál pro přenos poplachové zprávy. JTS je klasická telefonní linka, která byla dříve používána pro hlasovou komunikaci. V dnešní době je tento kanál na ústupu. Je to způsobeno tím, že mnoho lidí ruší svoje připojení k JTS. Náhradou bývá GSM a IP kanál. [3,4,5]

IP je rozšiřující se kanál pro přenos poplachové informace, ale i dalších událostí ze systému. Výhodou IP kanálu je velká propustnost dat a jeho rychlost, stejně tak i dostupnost. Proto se používá pro přenos dat i do telefonních aplikací. V současné době je mnoho PCO, které jsou schopny přijímat IP přenos. Internet je dnešní době zaveden do většiny objektů, a proto nevznikají další náklady na přenos informací z PZTS. [3,4,5]

GSM je přenos poplachové informace prostřednictvím sítě pro mobilní telefony. Pokrytí této sítě je téměř 100 % celé ČR, proto není problém využít tento kanál kdekoliv. Nevýhodou sítě

GSM je to, že nebyla určena pro PZTS, ale pro přenos informací nižší důležitosti, a proto není ideálně spolehlivá. Při využívání tohoto přenosu je vhodné mít záložní kanál.[3,4,5]

Rádiový přenos je bezdrátový přenos ve vyhrazeném pásmu. Ústředny od většiny výrobců nemají systémový rádiový komunikátor, proto PCO které dokáží přijímat rádiový přenos mají vlastní komunikátory, které se připojí na JTS komunikátor, který ústředny obvykle mají. Rádiový přenos má výhodu nízkých nákladů. Další výhodou je, že ústředna se může hlásit v krátkých intervalech. Proto i rušení komunikace na PCO je možno detekovat jako útok na chráněný objekt.[3,4,5]

4.1.2 Kamerové systémy

CCTV je dnes velmi rozšířené řešení pro ochranu objektů a je často kombinováno s PTZS nebo je provozováno samostatně. Vhodná je kombinace obou, protože moderní CCTV a PZTS spolu dokáží spolupracovat, například se jedná o natáčení kamer ve směru detektoru, na kterém vznikl poplach.[13,14]

CCTV také slouží pro ochranu venkovních prostor, například od vandalismu a loupeží. V dnešní době jsou kamery k vidění na mnoha místech venku. Často se jedná o otočné kamery zavěšené na lampách, kde mají přehled o ulici, případně na semaforech, kde mají přehled o provozu na křižovatce.[13, 14]

Dnešní CCTV dokáží mnohem více, než jen zaznamenávat obraz. V současné době mohou být kamery využity pro detekci požáru v rámci EPS. Jedná se o upravené termovize, které při překročení určité teploty vyhlásí požární poplach. Další časté využití je rozpoznávání SPZ a jejich předávání kontrolérům ACS. Toto řešení je dnes realizováno na mnohých parkovištích. Další novou funkcí kamer je schopnost rozpoznání pohybu v obraze. Díky této funkci je možné nahradit pohybové detektory v PZTS kamerami z CCTV, nicméně tato technologie se teprve rozvíjí. Další využití kamer mimo obor zabezpečení je v průmyslové automatizaci, kde kamery rozpoznávají tvary a pomáhají s řízením manipulátorům a dalších akčních členů.[14,15]

Propojení CCTV a integračních SW je poměrně snadné, jelikož běžné rekordéry disponují možností připojení k internetu a díky tomu jsou přímo připojeny k integračním SW přes internet. Do integračního SW následně stačí zadat přihlašovací údaje k rekordéru a následně je možné zobrazit obraz z jednotlivých kamer. [14,15]

4.1.2.1 Provedení kamer

Kamery jsou vyráběny v mnoha provedeních. Základní rozdělení provedení je na vnitřní a venkovní kamery. Nicméně v dnešní době existují také kamery pro současné vnitřní a venkovní použití.[13,16]

Bullet kamery jsou určeny k použití ve venkovním prostředí. Jejich kryt obvykle má IP krytí 68 a je v něm místo na vyhřívání. Také jejich kryt je odolnější proti vandalům. Kamery mají lepší objektivy z hlediska zoomu, především kvůli tomu, že venku kamera musí být schopna zaznamenat detaily na desítky až stovky metrů. Typické provedení je vidět na Obrázek 10 Bullet kamera. [13,16]

Obrázek 10 Bullet kamera

[Online]:
http://www.hikvision.com//uploadfile/image/product/big/20170605074453780.png
(Staženo 15.1. 2018)

Cube kamery jsou určeny do vnitřního prostředí. Jejich objektiv bývá 2,8 mm nebo 3,6 mm, kvůli obsažení co největší části vnitřního prostoru. Objektiv nemá zoom nebo má pouze minimální zoom. Typické provedení je vidět na Obrázek 11 Cube kamera. [13,16]

Obrázek 11 Cube kamera

[Online]:

http://www.hikvision.com//uploadfile/image/product/big/20160314200508833.jpg

(Staženo 15.1. 2018)

Dome kamery jsou určeny do vnitřních i venkovních prostor. Tyto kamery jsou parametricky kompromis mezi Cube a Bullet kamerami, proto nejsou úplně ideální ani pro jedno prostředí. Nicméně pokud zákazník požaduje stejný design kamer uvnitř i venku, tak jsou tyto kamery nejlepší řešení. Typické provedení je vidět na Obrázek 12 Dome kamera. [13,16]

Obrázek 12 Dome kamera

[Online]:

http://www.hikvision.com//uploadfile/image/product/big/20170606020712872.png

(Staženo 15.1. 2018)

Dále existují speciální kamery, které jsou především určeny do venkovních prostor. Příkladem je například PanoVu (Panoramatic View) kamera, která zaznamenává obraz v 360° a zároveň disponuje dalším snímačem, který se dá zaměřit na určité místo vybrané z 360° obrazu. Další speciální kamery jsou Dark Fighter kamery, které jsou určeny pro barevné vidění v noci. [17]

4.1.2.2 Objektivy

Každá kamera má objektiv, stejně jako fotoaparáty. Objektiv hraje důležitou roli v kvalitě pořízeného záznamu, ale také upravuje zorné pole kamery. Objektiv je soustava čoček, která tedy vhodně upravuje obraz před jeho záznamem. Většina dnešních kamer má již objektiv zabudovaný z výroby, ale u mnohých je možné ho vyměnit za jiný.[13,18]

V současné době se používají čtyři typy objektivů – Fixní objektiv, Varifokální objektiv, Zoom objektiv a Širokoúhlý objektiv. Fixní objektiv je pevně zaostřen již z výroby a není možné ho upravovat. Varifokální objektiv umožňuje po instalaci kamery na její místo zaostřit na požadovanou vzdálenost. Zoom objektiv umožňuje opticky přiblížit objekt. Širokoúhlý objektiv slouží pro velké zorné pole, snímá tedy velký prostor. Tento objektiv ovšem deformuje obraz. [13,18]

4.1.2.3 Analogové řešení

Analogové řešení je již několik desítek let staré, jenže kvůli svým nevýhodám a ceně, která je za obě řešení velmi podobná, je dnes postupně vytlačováno IP řešením. IP kamery mají výhodu větší vlastní inteligence, dokáží například rozpoznávat SPZ a vyhodnocovat je. Další nevýhodou analogových kamer je rozlišení záznamu. Současné kamery mají maximální rozlišení 2052x1536 (3 MPx), kdežto digitální kamery nabízejí až 12 MPx. Výhodou analogových kamer je možnost připojení přímo k televizi nebo monitoru a rovnou zobrazit jejich obraz.[4,19,20]

Na rozdíl od IP řešení, analogové řešení využívá koaxiální kabel k propojení kamery se záznamem. Proto je mnohem obtížnější instalovat analogové kamery do stávajících objektů. IP kamery se pouze připojí ke stávající datové síti objektu, která je dnes v objektech standardem. Dále je také nutné od každé analogové kamery vést jeden koaxiální kabel k záznamu. U IP kamer není problém použít switch a tím snížit náklady na kabeláž. [4,19,20]

Záznamovým zařízením pro analogové řešení je DVR (Digital Video Recorder). Každá kamera je připojena k DVR vlastním koaxiálním kabelem a oproti záznamovým zařízením u IP řešení je zde nižší počet připojitelných kamer. Obvykle jsou rekordéry vyráběné s podporou připojení 4/8/16 analogových kamer. Záznamové zařízení pro více kamer se objevují spíše ojediněle.

Rekordéry mohou mít i další funkce. Jedním z příkladů je záznam zvuku, pokud záznamem zvuku disponuje i kamera, dalším je ovládat otočné PTZ (Pan–Tilt–Zoom) kamery. [4,19,20]

4.1.2.4 IP řešení

IP řešení je oproti analogovému řešení novou technologií. Disponuje však většími možnostmi než analogové řešení. Hlavní výhodou je vlastní inteligence kamer, díky které kamery mohou vyhodnocovat SPZ. Mohou také vyhlašovat poplach, pokud zaznamenají pohyb, ale mají i další funkce. Jejich cena se stále snižuje a nyní je již velmi podobná analogovému řešení. [4,21]

Záznamovým zařízením pro IP řešení je NVR (Network Video Recorder). Všechny nainstalované IP kamery jsou připojeny k Ethernetové síti, která je větvena pomocí switchů. Proto je možné připojit více IP kamer do NVR pomocí jednoho Ethernetového kabelu. Vzhledem k tomu, že většina dnešních budov má svoji datovou síť, je poměrně snadné nainstalovat IP kamerový systém do stávající budovy. Nevýhodou však může být zatížení datové sítě, na které je potřeba myslet dopředu. [4,21]

Vzhledem k použití Ethernetového kabelu a switchů je možné kamery napájet vzdáleně pomocí PoE (Power Over Ethernet). Pro přenos videa do kamery jsou využity pouze dva páry, další dva páry jsou nevyužité při komunikaci s kamerou. Díky tomu bylo vytvořeno PoE, které nevyužité dva páry vodičů využívá pro napájení kamery. Díky tomu je možné mít společný zdroj napájení pro více kamer. Vhodným umístěním PoE switche jsou kamery napájeny a obraz z nich je přenášen pomocí jednoho Ethernetového kabelu k záznamovému zařízení. Další možností pro připojení kamer k NVR je optické vedení. To se používá v případech, pokud je kamera příliš daleko od NVR a nechceme používat opakovače. Nevýhodou optického vedení jsou aktivní prvky (převodníky) na obou koncích optického vedení a také jejich cena. Nicméně optické řešení se bude v budoucnu rozšiřovat ve velkých objektech a areálech, ve kterých budou kamery po celých objektech nebo areálech a jejich obraz se bude přenášet do jednoho centrálního záznamu. [4,21]

4.1.2.5 Legislativa ohledně používání CCTV

Pokud je nahráván záznam obrazu, je provozování CCTV považováno za zpracování osobních údajů. Proto používání CCTV podléhá zákonu č. 101/2000 sb., o ochraně osobních údajů.

Provozovat CCTV se záznamem je možné na základě následujících důvodů

- Pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce nebo jiného subjektu
- Jestliže je zpracování nezbytné pro dodržení právní povinnosti správce
- Na základě souhlasu subjektů

Nicméně existuje i mnoho dalších zákonů, které upravují výše uvedené, ale detailní rozbor těchto zákonů by vydal na samotnou práci.[22]

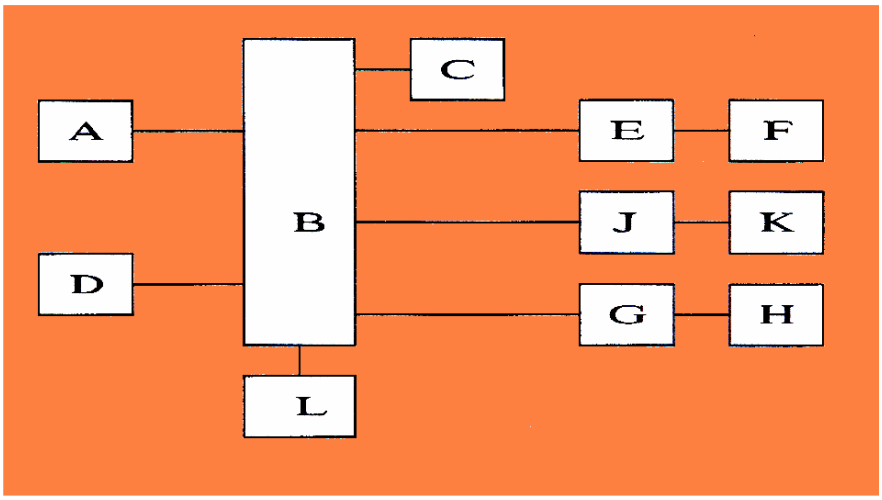
4.1.3 Elektrická požární signalizace

EPS je soubor technických prvků, který má za úkol detekovat a vyhodnocovat požáry v objektu. Hlavní účel EPS je, na rozdíl od ostatních bezpečnostních systémů, ochrana životů lidí, kteří se v objektu nacházejí a až sekundárně ochrana majetku. EPS v případě poplachu má za úkol provést lokální akustickou a optickou signalizaci v místě stálé služby. V tomto místě musí co nejpřesněji signalizovat místo požáru a zároveň automaticky začít zamezovat šíření požáru. Typicky se jedná o spuštění automatického hasicího systému a aktivaci nejrůznějších protipožárních přepážek. EPS také musí aktivovat vzduchotechniku v objektu, pokud je instalována, a začít odsávat kouř z místa požáru. Ve větších budovách, kde je instalován výtah, je na EPS, aby ho v případě požáru svezla do prvního patra a v něm zablokovala, výjimkou je však evakuační výtah.[4,23]

Současné EPS ústředny disponují síťovým portem nebo sériovým rozhraním, které se využívá pro připojení do integračního SW. V případě, že EPS ústředna má síťový port, stačí pouze propojit EPS ústřednu a server s integračním SW. Pokud má ústředna sériové rozhraní, tak je nezbytné použít převodník a následně EPS ústřednu připojit k serveru s integračním SW. [4,23]

4.1.3.1 Schéma systému

Na Obrázek 13 Schéma EPS jsou uvedeny všechny možné prvky EPS. Jejich popis je v Tabulka 2 Vysvětlení schématu EPS.[4,24]



Obrázek 13 Schéma EPS

[Online]: www.tzb-info.cz/docu/clanky/0147/014239o91.jpg (Staženo 20.1. 2018)

Tabulka 2 Vysvětlení schématu EPS

A – Samočinné hlásiče požáru	B – Ústředna EPS
C – Požární poplachové zařízení (signalizace)	D – Hlásiče tlačítkové
E – Zařízení pro přenos požárního poplachu	F – Ohlašovna požáru
G – Řídící jednotka samočinné požární ochrany	H – Samočinné zařízení požární ochrany
J – Zařízení pro přenos hlášení poruch	K – Stanice přijímající hlášení poruch

[Online]: www.tzb-info.cz/docu/clanky/0147/014239o91.jpg (Staženo 20.1. 2018)

Z výše uvedeného schématu jasně vyplývá, že EPS je složitý a velmi rozvětvený systém, který bude podrobněji rozebrán níže. [4,24]

4.1.3.2 Ústředna

Podobně jako u PZTS je ústředna hlavní mozek systému, který má za úkol vyhodnocovat všechny signály na všech vstupech a vhodně na ně reagovat. Nicméně existují 3 typy ústředen, u každé funguje vyhlašování poplachu rozdílně. Každá ústředna má linky, na které se připojují jednotlivé detektory. Jejich vyhodnocování je pak rozdílné podle jednotlivého typu ústředny. [4,25]

Základní rozdělení ústředen je následující

- Konvenční
- Adresovatelné
- Analogové

Konvenční systémy mají hlásiče připojeny na linku ústředny. Jednotlivé linky mohou mít pouze dva stavy, a to poplachový a klidový. O vyhlášení poplachu rozhoduje samotný hlásič. Při vyhlášení poplachu dokáže ústředna poznat pouze na které lince se poplach udál. Není tedy možné poznat, na kterém místě se poplach přesně udál. Cenově jsou však tyto ústředny a jejich hlásiče nejlevnější, protože hlásiče nepotřebují vlastní inteligenci.[26,27]

Adresovatelné systémy jsou vylepšením Konvenčních systémů, u kterých dokáže ústředna rozpoznat, na jakém hlásiči došlo k poplachu. O vyhlášení poplachu rozhoduje samotný hlásič. Po vyhlášení poplachu dokáže ústředna přesně určit linku i hlásič, na které nastal poplach a který hlásič jej vyhlásil. Cenově je tento systém dražší než Konvenční systém, protože každý hlásič musí být adresný. [26,27]

Analogový systém je velmi odlišný od obou předcházejících. Jednotlivé hlásiče neustále provádějí měření fyzikální veličiny a tyto hodnoty předávají ústředně, která je vyhodnocuje. Každý hlásič je adresný, tudíž je jasné, na kterém hlásiči nastal poplach. Vzhledem k tomu, že jednotlivé linky jsou sběrnicemi, tak jednotlivé hlásiče mohou také signalizovat své poruchy a je možné nastavovat parametry pro vyhlášení poplachu. Tento systém dosahuje nejlepších výsledků detekce požárů. Z uvedených typů ústředen je však nejdražší a také klade největší nároky na kabeláž. [26,27]

4.1.3.3 Hlásiče

Hlásiče slouží k detekci požáru a mohou fungovat na různých principech. Existují tři druhy hlásičů požáru – hlásiče tlačítkové, hlásiče automatické a teplotní kabely. Ve větších instalacích se používá jejich kombinace a v menších instalacích se používají automatické hlásiče.[4, 28]

Tlačítkové hlásiče slouží k vyhlášení požárního poplachu osobou, která zjistila, že se v objektu vyskytl nebezpečný jev spojený s požárem. Tlačítkové hlásiče jsou vždy červené barvy. Mohou obsahovat mikrospínač nebo složitější elektroniku podle typu ústředny. Tlačítkové hlásiče je nutné zabezpečit proti samovolné nebo náhodné aktivaci. Kvůli tomu bývá obvykle samotné tlačítko za sklem, které je nutné rozbít pro jeho stisknutí. Tlačítkové hlásiče se instalují především v prostorech, do kterých má přístup více osob. Pro lepší představu o provedení je tlačítkový hlásič vyobrazen na Obrázek 14 Tlačítkový hlásič. [4, 28]

Obrázek 14 Tlačítkový hlásič

[Online]: https://www.absolon.cz/deploy/img/products/7521/hfm37202_7521.jpg (Staženo 20.1. 2018)

Automatické hlásiče monitorují fyzické nebo chemické jevy v místě, kde jsou instalovány. Existují následující typy hlásičů – Hlásič ionizační, Hlásič optický, Hlásič teplotní, Hlásič tlakový, Hlásič odporový a Hlásiče kombinované. V praxi se však vyskytují jen Optické hlásiče a Teplotní hlásiče, ostatní se nepoužívají, jelikož jsou cenově dražší nebo nedosahují podobných výsledků (více falešných poplachů, pomalejší detekce skutečných požárů). Teplotní hlásiče mají dva možné principy fungování. Statický teplotní hlásič detekuje překročení určité teploty, Diferenciální teplotní hlásič detekuje rychlost změny teploty ve stupních Celsia za minutu. Většina dnes instalovaných teplotních hlásičů je kombinovaná, tedy obsahuje statickou i diferenciální technologii. Pro lepší představu o provedení je automatický hlásič vyobrazen na Obrázek 15 Automatický hlásič. [4, 28]

Obrázek 15 Automatický hlásič

[Online]: https://www.absolon.cz/deploy/img/products/4893/4893.jpg (Staženo 20.1. 2018)

Teplotní kabely jsou obvykle umístěny pod stropem a reagují na vyzařované teplo. Na rozdíl od samočinných hlásičů nejsou teplotní kabely bodové detektory, ale mohou detekovat požár na velké ploše. Teplotní kabely mají obvykle vlastní vyhodnocovací jednotku, která je připojena na vstup ústředny EPS. Pro lepší představu o provedení je teplotní kabel vyobrazen na Obrázek 16 Teplotní kabel. [4, 28]

Obrázek 16 Teplotní kabel

[Online]: http://www.protectowire.com/wp-content/uploads/bfi_thumb/bsdvds789.jpg (Staženo 20.1. 2018)

4.1.3.4 Signalizace EPS

Signalizace požáru je nezbytná. Je nutné, aby ihned po detekci požáru byly upozorněny všechny osoby, které mají nastalou situaci řešit. Nejčastěji se jedná o obsluhu na stálém dohledovém místě. Obvykle se kombinuje optická a akustická signalizace.[29]

4.1.3.5 Obslužné pole požární ochrany

OPPO je univerzální typizovaný ovládací prvek, který je jednotný pro ústředny všech výrobců. OPPO využívá Hasičský záchranný sbor. Pro hasiče je nezbytné, aby byli schopni ovládat všechny ústředny od všech výrobců. Díky tomuto mohou znát pouze jeden ovládací prvek a dokáží ovládat důležité funkce každé ústředny. OPPO je vyobrazeno na Obrázek 17 OPPO.[30]

Obrázek 17 OPPO

[Online]: https://www.lites.cz/sites/lites3v01.localhost/files/katalog/mhy912_1.jpg (Staženo 20.1. 2018)

4.1.3.6 Klíčový trezor požární ochrany

Podobně jako OPPO je KTPO určen pro hasiče. Má za cíl usnadnit jejich zásah při likvidaci požáru. Jedná se o úložný prostor pro podstatné nebo univerzální klíče od prostoru, kde je instalován. Využívá se především v prostorech, kde není stálá ochrana. Trezor je dvoukomorový, první komoru otevře ústředna EPS při požárním poplachu a druhou komoru si otevře hasič pomocí hasičského univerzálu. Díky tomu se mohou hasiči snadněji dostat do objektu a nemusí při tom ničit dveře objektu. Provedení KTPO je vyobrazeno na Obrázek 18 KTPO.[30]

Obrázek 18 KTPO

[Online]: https://www.schraner.de/img/large/import/11773- 10.png (Staženo 20.1. 2018)

4.1.3.7 Normy a legislativa EPS

Norma ČSN EN 54 se věnuje EPS a jejím částem. Tato norma se skládá z osmnácti částí, kde jsou uvedeny požadavky na jednotlivé komponenty, ze kterých se může celá EPS sestávat. Dále ČSN 73 0875 a ČSN 34 2710 se týkají projektování EPS.[31]

Dále zákon 133/1985 Sb. se věnuje problematice EPS, který byl později doplněn o další vyhlášky. Vzhledem k tomu, že EPS chrání primárně lidské životy, je více pod dohledem legislativy než ostatní technologie.[31]

4.1.4 Elektronická kontrola vstupu

Elektronická kontrola vstupu (EKV nebo také ACS, z anglického Access Control System) je systém, který má na starosti dohled nad osobami přistupujícími do určitého místa (například budova). Zná jejich oprávnění na jednotlivé části objektu a dle nich je vpouští do jednotlivých částí, zároveň také zaznamenává všechny průchody osob. Díky této schopnosti spolehlivě nahrazuje fyzické strážné, kdy při jejich nedbalosti mohlo dojít ke vstupu osob tam, kam nemají. Tento systém také zredukuje náklady na strážného jednorázovou investicí.[4,32]

Výše uvedeného je dosaženo tak, že osoba disponuje určitým unikátním identifikátorem. Nejčastěji se jedná o čip nebo kartu, pokud je identifikátorem fyzický předmět. Dalším častým identifikátorem je unikátní kód, který zná pouze osoba. V poslední době se velmi rozšiřují i biometrické čtečky, které využívají otisky prstů nebo krevního řečiště dlaně ruky. Fyzické identifikátory mají však nevýhodu v tom, že mohou být ztraceny nebo ukradeny. V objektu jsou rozmístěny čtečky těchto identifikátorů. Jednotlivé čtečky ovládají zámek dveří, u kterých se nacházejí. Pokud má mít osoba přístup do prostoru za čtečkou, tak po přiložení identifikátoru (případně zadání kódu) dojde k otevření těchto dveří a osoba je vpuštěna do prostoru za dveřmi. Dále je tento průchod zaznamenán pro případné zpětné dohledání pohybu určité osoby, nebo pro dohledání, kdo byl v určité době v určitém prostoru.[4,32,33]

V dřívějších dobách se ACS používala převážně v komerčních prostorech, nicméně v poslední době s poklesem pořizovací ceny se ACS nasazuje v oblasti rodinných domů a bytových jednotek. Často je však ACS součástí PZTS, protože je to jednodušší na instalaci a správu. Díky tomuto spojení je pouze jedna databáze osob a vše je propojeno jednou kabeláží (moduly pro

ACS jsou připojeny na stejné sběrnici jako moduly a klávesnice pro PZTS), tím je uspořeno na nákladech na instalaci. Společné databáze osob je dosaženo také pomocí Integračních SW, které budou probrány v další kapitole. [4,32,33]

Běžné ACS mají integrovaný síťový port, proto propojení ACS s integračním SW je snadné, stačí fyzicky propojit ACS a server s integračním SW. [4,34]

4.1.4.1 Identifikátory

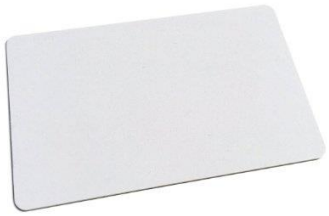
Jak již bylo zmíněno, identifikátorů existuje celá řada a je možné dělení dle jejich typu na následující

- Vlastní identifikátor
- Kód
- Biometrické údaje

V případě **vlastního identifikátoru** se jedná nejčastěji o čipy a karty. Typické provedení je vyobrazeno na Obrázek 19 Čip a Obrázek 20 Karta. Tyto identifikátory mají několik nevýhod. První nevýhodou může být možná ztráta identifikátoru, případně odcizení či zneužití. Další nevýhodou je možnost padělání tohoto identifikátoru. Na druhou stranu mají výhodu nízké ceny čtečky. Nicméně cenová výhoda může zaniknout, pokud je na objektu jen několik málo čteček, ale zato je velmi mnoho identifikátorů. K tomuto dochází například ve velkých bytových domech, kde bývá čtečka u společných vstupních dveří a identifikátor vlastní každý obyvatel tohoto domu.[35]

Obrázek 19 Čip

[Online]: http://pro.comelitgroup.com/files_cms/2-prodotti/image/SK9050G_A.jpg (Staženo 25.1. 218)



Obrázek 20 Karta

[Online]: http://www.hikvision.com/uploadfile/image/product/big/201709111456139.jpg (Staženo 25.1. 2018)

Využívání kódu jako identifikátoru je nejlevnější možnou podobou řešení ACS. Místo čteček jsou nasazeny kódové klávesnice, na nichž se při vstupu zadává kód. Cena klávesnic je podobná jako cena čteček čipů a karet. Výhodou pak je, že samotný identifikátor nic nestojí a také se nedá ztratit. Pokud dojde k jeho zapomenutí, je snadné ho obnovit (správce systému může tuto operaci provést vzdáleně, pokud daný systém podporuje dálkovou správu). Další výhodou je, že uživatel systému může mít dva kódy, jeden pro normální užívání a druhý pro signalizaci nátlaku jinou osobou. Nátlakový kód se zpravidla používá o jedna vyšší než standardní, například normální kód je „1111“ a nátlakový kód je „1112“.[35]

Biometrické údaje jsou jedinečné měřitelné fyziologické znaky člověka. Díky nim je možné jednoznačně určit člověka, kterému tyto biometrické údaje patří. Využívá se fyziologických znaků, které jsou časem neměnné. Jedná se o otisky prstů, krevní řečiště, oční sítnice nebo geometrie obličeje. Nicméně v praxi se nasazují většinou čtečky otisků prstů, které jsou nejlevnější. Mají však problém v tom, že pokud dojde k poškození prstu (lehké zranění způsobené prací, například na zahrádce), tak čtečka nevyhodnotí otisk správně. Nicméně je možné uložit do databáze ACS otisky z více prstů, takže lze použít jiný prst. Čtečky pro ostatní biometrické údaje se zatím používají výrazně méně, především kvůli jejich pořizovacím nákladům.[36,37]

4.1.4.2 Čtečky a klávesnice

Jsou to zařízení, kde se načte identifikátor nebo zadá kód. Čtečka provede převod načteného identifikátoru na kód v binární soustavě a odešle ho řídící jednotce. Existují také autonomní čtečky, které rovnou identifikátor vyhodnotí a sepnou/rozepnou relé, na které je připojen

zámek. Autonomní čtečky jsou vhodné na malé instalace, kde jsou jedny, nebo malý počet elektronicky ovládaných dveří. Na Obrázek 21 Biometrická čtečka je typická čtečka otisků prstu.[38]

Obrázek 21 Biometrická čtečka

[Online]:
http://en.cdvi.com/var/ezflow_site/storage/images/internet/catalogue/gamme/biometrie/systeme-biometrique/biosys-1/194971-1-fre-FR/BIOSYS-1.png (Staženo 25.1. 2018)

4.1.4.3 Řídící jednotka

Řídící jednotka má v sobě uložené všechny identifikátory, které byly do systému naučeny. Když čtečka odešle kód identifikátoru, tak řídící jednotka porovná kód identifikátoru se svojí databází identifikátorů a pokud identifikátor nalezne a není nijak omezen (nemá oprávnění na dané dveře nebo je časově omezen, např. identifikátor má fungovat pouze od 8 do 18 hodin a byl načten v 7:45), tak řídící jednotka sepne/rozepne relé příslušného zámku. Další důležitou funkcí je uložení každého načteného identifikátoru řídící jednotkou do své paměti a k němu uloží případné otevření dveří.[4,38]

4.1.4.4 Docházkové systémy

Docházkové systémy jsou rozšířením ACS, které se využívají především ve firmách, kde pomáhají s dohledem nad docházkou zaměstnanců do firmy. To může firmě zjednodušit administrativu ohledně evidence docházky zaměstnanců. Pro zaměstnance je to také zjednodušení, stačí pouze přiložit identifikátor k terminálu při příchodu a znovu jej přiložit při odchodu. Docházkový systém na konci měsíce generuje podklady pro mzdové oddělení, a tím

zjednoduší určení výše mzdy zaměstnanců. Na Obrázek 22 Docházkový terminál je vyobrazen typický docházkový terminál, ke kterému zaměstnanci přikládají své identifikátory.[39]

Obrázek 22 Docházkový terminál

[Online]: http://www.aktion.cz/aktion_cs/images/content/picture/er-310b.jpg (Staženo 25.1. 2018)

4.2 Integrační software

Integrační SW je software, který napomáhá správě všech instalovaných zabezpečovacích technologií. Všechny tyto instalované zařízení jsou do integračního SW fyzicky připojeny a odesílají do integračního SW většinu údajů (například ovládání PZTS ze strany uživatelů nebo průchody uživatelů dveřmi u ACS). V integračním SW jsou následně prováděny operace obsluhou nebo jsou prováděny automatické operace (například pokud někdo projde určenými dveřmi a tím se zapne klimatizace). Tyto automatické operace je vhodnější nastavit na úrovni integračního SW, protože je pro obsluhu snadnější jejich úprava nebo zakázání.[40]

Obvyklé provedení integračního SW je server – klient. Na serveru běží jádro integračního SW a k tomuto serveru jsou připojeny všechny technologie. Tento PC bývá obvykle uložen v technické místnosti poblíž připojených technologií. Klientské stanice jsou nainstalované na dalších PC, u kterých se nachází obsluha, která pracuje s integračním SW. Klientskou stanicí se může stát i mobilní telefon, pokud to daný integrační SW umožňuje. Může se jednat o recepční vydávající karty/čipy pro osoby přistupující do objektu. Další místo, kde se využije možností integračního SW je dohledová místnost, kde je stálá bezpečnostní služba, která dohlíží na objekt.[40]

Každá technologie připojená do integračního SW přenáší určitá data do integračního SW. Nejjednodušší je to u CCTV, kde dochází k přenosu videa a případných poruch do integračních SW a z integračních SW jsou ovládány případné otočné kamery. PZTS do integračního SW přenáší poplachy, které na PZTS nastaly, zastřežení a odstřežení podsystémů a také poruchy. Naopak z integračního SW jsou do PZTS přenášeny ovládací příkazy na zastřežení a odstřežení vybraných podsystémů. U EPS jsou přenášeny poplachy a poruchy do integračního SW. Z integračního SW jsou do EPS přenášeny příkazy na utišení v případě požárního poplachu. U ACS jsou do integračního SW přenášeny všechny průchody přes ACS, dále případné detekce dlouho otevřených dveří a násilně otevřených dveří. Z integračního SW jsou do ACS přenášeny příkazy pro otevření určitých dveří na nastavenou dobu, případně trvalé otevření dveří. Výše uvedené události jsou pouze základní události společné pro všechny typy technologií, ale každá technologie může přenášet i další události, které dokáže vyhodnocovat.[40]

4.2.1 Propojení

Propojení mezi serverem a klientskými stanicemi se provádí obvyklou LAN (Local area network) sítí. Není problém se připojit do stávající LAN sítě objektu, pokud nějaká existuje. Pokud není, je dostačující vytvořit obdobnou LAN síť, jako je LAN síť pro obvyklé propojení PC a dalších prvků v LAN síti.[41]

U propojení mezi technologií a serverem je to složitější, protože každá technologie má jiný komunikační interface. Některá zařízení mají obvyklý LAN port, jiné disponují pouze sběrnicí (nejčastěji RS-485 a RS-232). Dále je možné (i časté), že zařízení disponuje LAN portem a některou sběrnicí, ale výrobce uvolnil komunikační protokol pouze pro sběrnici, a proto integrace zařízení byla provedena prostřednictvím komunikačního protokolu sběrnice a následně bylo užito převodníku RS232/LAN pro připojení do LAN sítě. Pro tyto účely se často využívají převodníky od firmy Papouch s.r.o., která dodává mnoho druhů převodníků vysoké kvality a spolehlivosti. Dále je také vhodné, aby technologie byla připojena vlastní LAN sítí k serveru.[41]

Po fyzickém propojení dle dostupných interfaců a komunikačních protokolů je třeba disponovat naprogramovaným driverem. Jedná se o program, který má na starosti překlad z komunikačního protokolu zařízení na komunikační protokol, který využívá integrační SW a obráceně. Každá technologie potřebuje vlastní driver a díky němu může komunikovat s integračním SW.[41]

4.2.2 Výhody

Využití integračního SW přináší mnoho výhod pro všechny osoby, které potřebují pracovat s technologiemi nainstalovanými na objektu.[42]

- Velkou výhodou je, že pracují s jedním programem a jedním grafickým prostředím při používání všech nainstalovaných technologií.
- Další výhodou je, že pokud více technologií disponuje podporou osob, tak v integračním SW je centrální správa osob (tedy například jejich identifikátorů a úrovní oprávnění) pro všechny technologie.

- Integrační SW dokáží exportovat vybraná data a dát je k dispozici komukoli, kdo na ně má nárok a požádá o ně. Jedná se například o přístupy jednotlivých osob na ACS.
- Okamžitý přehled o poruchách na prvcích všech nainstalovaných technologií na jednom místě.
- Synchronizace času všech technologií. To je vhodné pro zpětné dohledávání záznamu z určité kamery v závislosti na poplachu na PZTS.
- Integrační SW může provádět automatické akce nad více technologiemi v definovaném čase.
- Integrační SW umožňuje připojení technologií, které nejsou na stejné budově. Umožňuje tedy správu zařízení na více místech. Pro firmu, která má více poboček, umožní tento systém mít jednotnou databázi osob, která je společná pro všechny technologie na všech pobočkách a každé osobě je přiřazeno pouze oprávnění na pobočky, na které mají mít přístup.
- Díky integračnímu SW může člověk zodpovědný za správu osob během krátkého času vymazat osobu, případně upravit její oprávnění, pokud je to požadováno. Například po podání výpovědi zaměstnancem.

4.2.3 Nasazení

Oblastí, kde se nasazují integrační SW je mnoho. Obecně se dá říci, že integrační SW je vhodný pro všechny místa, kde jsou užity zabezpečovací systémy. [42]

Administrativní budovy jsou častým místem, kam se integrační SW nasazují. Vzhledem k tomu, že administrativní budovy může sdílet více firem, je nezbytné obsluze zabezpečovacích technologií poskytnout pomocný nástroj, aby nedocházelo k chybám ohledně nastavení přístupových práv, které by mohlo ohrozit firemní tajemství jednotlivých firem.

Věznice jsou dalším místem, kde jsou integrační SW velmi často nasazovány. Ve vězeních jsou obvykle dohledové místnosti, ve kterých se nachází nepřetržitá služba. Na tomto místě je nezbytné snadné zjištění vzniku bezpečnostního rizika a případně ho okamžitě a jasně identifikovat.

Bezpečností agentury mohou využít integračního SW při zásahu na objektu. Integrační SW ve vizualizaci jasně zobrazí, kde došlo k poplachu a zobrazí záznam z příslušných kamer. To pomůže bezpečnostní službě k dopadení narušitele.

Obchodní centra jsou místem, kde se vyskytuje mnoho lidí, kteří přicházejí do kontaktu s technologií a bez integračních SW by bylo náročné hlídat, zdali je vše v pořádku. Jelikož každý obchod má jinou obsluhu a provozní dobu, integrační SW zjednoduší práci v dohledovém centru, protože dokáže pomoci s vyhodnocením, zdali vybraná osoba v určitou dobu může na určité místo či nikoli.

Korporace mají více poboček a integrační SW umožní dohledovému centru dohlížet nad všemi pobočkami z jednoho centrálního dohledového místa. To přináší úsporu nákladů, protože není potřeba mít dohledové centrum na každé pobočce.

Bytové komplexy jsou místem, kde má mnoho lidí většinu svého osobního majetku. Tyto bytové komplexy mohou být rozsáhlé, a proto je vhodné použít integrační SW, který pomůže bezpečnostní službě najít místo narušení mnohem rychleji než bez něj.

Oblastí kde se nasazují integrační SW je mnohem více, výše byly vyjmenovány pouze nejčastější oblasti.

4.2.4 Nastavení

Nastavení integračních SW od jednotlivých výrobců se liší, proto zde budou probrána nastavení podobná pro všechny integrační SW krok po kroku.[43,44]

Prvním krokem je výběr vhodného serverového PC, jehož parametry musí odpovídat velikosti instalace. Na tento server se nainstaluje serverová část integračního SW a následně se nainstalují ovladače – drivery pro jednotlivé technologie, které budou připojeny. Následně jsou na další PC nainstalované klientské stanice, tyto PC již nemusí být příliš výkonné. [43,44]

Druhým krokem je vytvoření stromu zařízení. To znamená okopírovat rozložení prvků na jednotlivých připojených zařízeních. Tento strom zařízení je nezbytný pro správné zobrazování poplachů, poruch a případných dalších událostí. Všechny prvky ve stromu zařízení musejí být naadresovány, podobně jako jsou adresovány v technologii. Některé integrační SW disponují

funkcí automatického načtení stromu zařízení. Zde je však podstatné, jaký komunikační protokol poskytl výrobce pro technologii, protože ne každý komunikační protokol umožní přenést informace potřebné k vytvoření stromu zařízení. [43,44]

Třetím krokem je vytvoření vizualizace. Vezmou se nejčastěji stavební výkresy a z nich se umaže vše tak, aby zůstal pouhý jednoduchý půdorys, případně bokorys objektu. Které a kolik jich bude třeba je dáno složitostí objektu. Pokud je objekt pouze v jednom patře, potom obvykle stačí jeden půdorys, který je kvůli zvýšení přehlednosti rozdělený na více částí. Do těchto provázaných půdorysů a bokorysů jsou zaneseny prvky všech technologií, aby na svém místě mohly signalizovat poplach. [43,44]

Dalším krokem je nastavení automatických akcí. Mezi nejjednodušší automatické operace patří provázání kamer s detektory PZTS a hlásiči EPS. Když vznikne poplach na některém prvku těchto technologií, tak integrační SW okamžitě zobrazí příslušnou kameru a nabídne i záznam z doby poplachu. To může pomoci obsluze vyhodnotit, zdali se jedná o falešný poplach nebo je třeba nějak reagovat. Automatických akcí může být mnoho, záleží na požadavcích obsluhy. Současné integrační SW umožňují skriptování vlastních automatických akcí, takže je možné svázat jakékoli fyzické i virtuální prvky pomocí libovolné existující vazby. [43,44]

Dalším krokem je vytvoření uživatelů. Ty jsou dvojího typu, první je uživatel integračního SW a druhý je uživatel technologie. Pro první typ uživatele je nezbytné uživateli vytvořit přihlašovací údaje do integračního SW a přiřadit mu oprávnění na práci s integračním SW, tedy do jakých nastavení má oprávnění se dostat. Pokud má být zároveň i uživatelem technologie, je pro něj nezbytné nastavit oprávnění na jednotlivé nainstalované technologie, tedy především na podsystémy u PZTS a přístupové oprávnění na jednotlivé dveře u ACS. [43,44]

Dále je možno nastavit mnoho dalších parametrů, ty se ale liší podle integračních SW od jednotlivých výrobců. Často se využívá recepčního modulu, který slouží ke zprávě návštěv. Tyto návštěvy při příchodu poskytnou občanský průkaz, který je naskenován a tím je osoba zanesena do integračního systému, kde jsou jí přiřazena oprávnění a je jí vydán identifikátor pro samostatný pohyb po objektu, je-li třeba. [43,44]

5 Praktická část práce

Byl hledán požadavek na instalaci nebo výměnu PZTS a následnou integraci do integračního SW. Následně byl nalezen požadavek na výměnu PZTS ústředny a jejího příslušenství za novou, následná integrace nově instalované ústředny do integračního SW spolu s kamerovým systémem Hikvision, který již byl na objektu instalován.

5.1 Výběr vhodné PZTS a integračního SW

Nejdříve bylo nezbytné vybrat vhodnou technologii a integrační SW odpovídající požadavku zákazníka. Zákazník požadoval kvalitní ústřednu od výrobce, který je na trhu alespoň 20 let. Dále chtěl mít možnost budoucího rozšíření, a proto trval na ústředně vhodné pro velké instalace. Dalším požadavkem byla certifikace do 3. stupně dle EN 50131-1. Dále očekával snadné ovládání, ideálně pomocí telefonní aplikace. Od integračního SW zákazník očekával snadnou správu a provázání obou instalovaných technologií.

5.1.1 Multikriteriální analýza PZTS ústředen

K multikriteriální analýze byly vybrány tři PZTS ústředny – Risco ProSYS Plus, Honeywell Galaxy Dimension, Inner Range Concept. Byly porovnány jejich základní parametry a jejich cena. V Tabulka 3 Parametry ústředen jsou parametry a ceny jednotlivých ústředen a v Tabulka 4 Multikriteriální analýza je vyhodnocení jejich parametrů a ceny prostřednictvím multikriteriální analýzy.

Tabulka 3 Parametry ústředen

	ProSYS Plus	Galaxy Dimension	Concept	Váha kritéria
Počet vstupů	512	520	400	5
Počet podsystémů	32	32	96	3
Počet výstupů	262	266	64	4
Počet kódů	500	1000	2000	6
Cloudová nadstavba	Ano	Ne	Ne	10
Paměť událostí	2000	1500	1300	4
Počet klávesnic	48	32	32	2
Cena ústředny (Kč)	11 960	22 344	23 240	10

V Tabulka 4 Multikriteriální analýza PZTS je přepočet hodnot jednotlivých kritérií. V této tabulce jsou porovnávány jednotlivé PZTS ústředny.

Tabulka 4 Multikriteriální analýza PZTS

	ProSYS Plus	Galaxy Dimension	Concept
Počet vstupů	8*5	9*5	6*5
Počet podsystémů	7*3	7*3	10*3
Počet výstupů	10*4	10*4	5*4
Počet kódů	5*6	7*6	10*6
Cloudová nadstavba	10*10	0*10	0*10
Paměť událostí	10*4	7*4	6*4
Počet klávesnic	10*2	8*2	8*2
Cena ústředny (Kč)	10*10	2*10	3*10
Součet	391	212	210

Z výše uvedené tabulky vyplývá, že ústředna ProSYS Plus je nejvhodnější náhrada za stávající systém. Proto bude v realizační části užita právě tato ústředna.

Ústředna ProSYS Plus je vyráběna izraelskou firmou RISCO LTD. Jedná se o hybridní ústřednu, která disponuje čtyřmi nezávislými sběrnicemi a možností bezdrátové nadstavby. Parametry ústředny jsou uvedeny výše v Tabulka 3 Parametry ústředen. Ústředna je v modulárním provedení, komunikační moduly se připojují na porty, které jsou umístěné na ústředně. Tím se redukují přebytečné náklady na nepotřebné komunikační moduly. Ústředna je certifikována do stupně 3 dle ČSN EN 50131-1. Provedení ústředny je k vidění na Obrázek 23 ProSYS Plus.

Obrázek 23 ProSYS Plus

[Online]: https://store.riscogroup.com/EN/PSP/main.jpg (Staženo 28.2. 2018)

5.1.2 Multikriteriální analýza integračních SW

K multikriteriální analýze byly vybrány tři integrační SW – Alvis, C4 a SBI. Byly porovnány jejich parametry, cena a uživatelská přívětivost. Parametry těchto integračních SW jsou v Tabulka 5 Parametry integračních SW. Protože některé parametry jsou subjektivní, bylo osloveno devět firem, které mají zkušenosti se všemi uvedenými integračními SW a poskytly své hodnocení číselně v rozmezí 0–10, podle jejich preference daného SW.

Tabulka 5 Parametry integračních SW

	Alvis	C4	SBI	Váha kritéria
Počet podporovaných technologií	89	157	188	8
Náročnost instalace	8	9	7	4
Uživatelský komfort	5	10	7	10
Cena SW pro realizovanou instalaci	120 000	125 000	130 000	10
HW náročnost	9	7	5	4
Složitost instalace klientů	6	9	8	5

V Tabulka 6 Multikriteriální analýza integračních SW je přepočet hodnot jednotlivých kritérií. V této tabulce jsou porovnávány jednotlivé integrační SW.

Tabulka 6 Multikriteriální analýza integračních SW

	Alvis	C4	SBI
Počet podporovaných technologií	4*8	8*8	10*8
Náročnost instalace	8*4	9*4	7*4
Uživatelský komfort	5*10	10*10	7*10
Cena SW pro realizovanou instalaci	10*10	9*10	8*10
HW náročnost	9*4	7*4	5*4
Složitost instalace klientů	6*5	9*5	8*5
Součet	280	363	318

Z výše uvedeného vyplývá, že nejvhodnějším integračním SW je C4, která disponuje velkým uživatelským komfortem a příznivou cenou.

C4 je integrační SW od slovenské firmy Gamanet a.s.. C4 disponuje otevřenou architekturou, díky které je možné k C4 připojit mnohé technologie, často se jedná o parkovací systémy, biometrické systémy a další. Běžné bezpečnostní technologie jsou již integrované od výrobce. C4 je schopna automatických akcí, dokáže tedy samostatně reagovat na nastalé události bez zásahu obsluhy. C4 díky své uživatelské přívětivosti umožňuje obsluze snadnou správu všech instalovaných zařízení.

5.2 Realizace výměny a oživení PZTS ústředny

Po vybrání vhodné ústředny bylo přistoupeno k samotné realizaci výměny stávající PZTS ústředny za ústřednu ProSYS Plus.

5.2.1 Příprava

V rámci realizace byly jako první demontovány všechny komponenty staré ústředny, s výjimkou detektorů a sirén. Dále byly ponechány boxy, ve kterých byla nainstalována stará ústředna, kvůli ušetření nákladů na nové a snížení pracnosti výměny. V boxech stačilo pouze vyvrtat nové otvory pro distanční sloupky dle potřeb nových komponent. Také byla zachována velká část kabeláže, s výjimkou kabeláže v boxech, ve kterých se nacházejí nové komponenty. Tato kabeláž byla odstraněna a při montáži byla doplněna nová, podle potřeb ústředny ProSYS Plus.

Před instalací byl spočítán počet detektorů a dalších prvků, které se nachází v objektu. Celkový počet jednotlivých prvků je 15 PIR detektorů, 18 magnetických kontaktů, 10 detektorů tříštění skla, 8 požárních detektorů, 2 sirény, 3 zónové expandéry, 1 expandér výstupů a 3 klávesnice. Následně byl spočítán celkový odběr výše uvedených komponent, tento součet je v Tabulka 7 Spotřeba prvků PZTS.

Tabulka 7 Spotřeba prvků PZTS

Prvek	Odběr (mA)	Počet (ks)	Celkový odběr (mA)
PIR detektor	20	15	300
Magnetický kontakt	0	18	0
Detektor tříštění skla	15	10	150
Požární detektor	25	8	200
Siréna	500	2	1000
Zónový expandér	20	3	60
Expandér výstupů	20	1	20
Klávesnice	100	3	300
Ústředna	400	1	400
Celkem			2430

Z výše uvedeného vyplývá, že celkový odběr je 2430 mA, což je více, než je ústředna schopna dodat, proto bylo nezbytné přidat posilující zdroj. Výrobce dodává 3A systémový posilující zdroj, který je pro napájení všech komponent dostačující. Díky tomu, že zdroj je systémový, bude možné provádět diagnostiku a nastavovat jeho parametry prostřednictvím ústředny.

5.2.2 Montáž

V prvním kroku bylo rozvrženo přibližné umístění jednotlivých komponent v boxech vzhledem ke stávající kabeláži a možnostem nové PZTS ústředny. Poté bylo provedeno několik přesunů v hlavním boxu, kde se bude nacházet ústředna, jeden expandér a pomocný napájecí zdroj. Po vhodném rozvržení komponent byly do boxu namalovány značky dle umístění distančních sloupků pro jednotlivé komponenty. Ty byly následně provrtány. Dále byly připraveny otvory pro uchycení transformátoru a druhého zdroje, který bude napájet ústřednu a pomocný zdroj. Do připravených otvorů byly upevněny distanční sloupky a na ně nasazeny jednotlivé komponenty. Na všech komponentech byly na DIP přepínačích nastaveny jejich adresy. Dále byl do připravených otvorů přichycen transformátor.

5.2.3 Kabeláž

Po montáži jednotlivých komponent bylo nezbytné je propojit. Prvně byla propojena sběrnice, kterou byla propojena ústředna s expandérem výstupů, zónovými expandéry, klávesnicemi a

pomocným zdrojem. V případě ústředny ProSYS Plus je sběrnice čtyřvodičová, první pár je pro napájení komponent, tedy +12 V a 0 V a druhý pár je datový. Sběrnici je možné libovolně větvit. Při využití pomocného zdroje je důležité nepropojit napájecí vodič z ústředny k pomocnému zdroji.

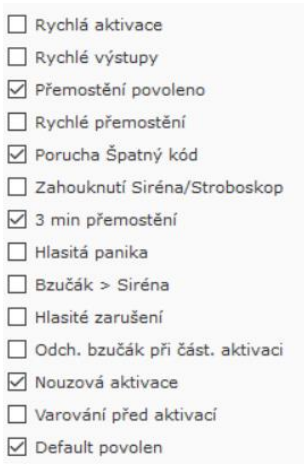
Výše zmíněné komponenty byly propojeny dle výše uvedených pravidel. Následně byly připojeny sirény, nezálohované přímo na svorky pro ně určené, zálohované byly připojeny na napájení z pomocného zdroje a na programovatelný výstup, který je bude spouštět. Dále byly připojeny všechny detektory na příslušné vstupy na ústředně a zónových expandérech.

Následně byla celá kabeláž ověřena, především zdali se neuvolnil některý kabel. Po kontrole kabeláže bylo přivedeno napájení pro ústřednu a pomocný zdroj.

5.2.4 Nastavení ústředny

Připojením napájení došlo k prvnímu spuštění ústředny a klávesnice s adresou jedna vyzvala k provedení základního nastavení ústředny. Toto nastavení spočívalo v nastavení jazyku ústředny, času a data a počtu podsystémů (je možné si vybrat v rozmezí 8 až 32). Po provedení tohoto nastavení se ústředna spojila s Cloudem, aby se pokusila stáhnout případné zónové licence. Nicméně základní počet licencí byl dostačující, a proto nebylo nezbytné nějaké další dokupovat. Ústředna následně nabídla možnost automaticky naskenovat sběrnici, čehož bylo využito. Ústředna zobrazila všechny komponenty připojené na sběrnici a nastavila jim defaultní nastavení. Poté bylo nastavení uloženo.

Následně byl připojen programovací SW Konfigurační software (dále CS) a bylo staženo stávající nastavení celé ústředny do PC. První položkou v nastavení bylo nastavení samotného systému. Zde bylo nastaveno například příchodové a odchodové zpoždění, které bylo přebráno ze staré ústředny. Dále byly nastaveny další potřebné časovače. Následně byla povolena komunikace na pult centrální ochrany a na Cloud, naopak komunikace s uživateli byla zakázána. Dále byly v systémovém nastavení nastaveny názvy podsystémů, které byly převzaty ze staré ústředny. Dále bylo nastaveno časové pásmo a NTP server pro automatické srovnávání času. Následně bylo v systémovém nastavení nastaveno chování systému. Jednalo se například o vypnutí rychlé aktivace (nutnost zadat kód pro aktivaci) nebo automatická změna letního a zimního času. Část těchto nastavení je na Obrázek 24 Nastavení systému.



Obrázek 24 Nastavení systému

Další částí nastavení bylo nastavení zón. V prvním kroku byly přepsány názvy všech zón ze staré ústředny. Dále byly ze staré ústředny také převzaty zakončení a typy zóny. Zde byla však udělána malá změna, protože stará ústředna nabízela jiné možnosti nastavení. Pokud bylo potřeba zóny s odchodovým a příchodovým zpožděním, která má mít možnost být narušena během odchodového zpoždění, byl typ zóny nastaven jako odchodový a příchodový otevřený, který umožňuje být narušen během odchodového zpoždění. Tento typ zóny byl využit pro dveře a PIR detektory, které jsou mezi vchodem do objektu a klávesnicemi. Dále byly všechny zóny rozděleny do jednotlivých podsystémů tak, aby šlo ústřednu snadno ovládat. Nastavení prvních dvaceti zón je na Obrázek 25 Nastavení zón.

č.	Popis	Kanál	Typ	Zvuk při Akt.	Zakončení	Skupina	Podsystém
1	Dv. sklad	E 0:00:01	Odchod/Vstup 1	Siréna	NC	A B C D	2
2	Dv. dvorek	E 0:00:02	Odchod/Vstup 1	Siréna	NC	A B C D	1-2
3	Zavory	E 0:00:03	Okamžitá	Siréna	EOL	A B C D	2
4	Vchod mag.	E 0:00:04	Okamžitá	Siréna	EOL	A B C D	1
5	Vchod PIR	E 0:00:05	Okamžitá	Siréna	EOL	A B C D	1
6	Zona 006	E 0:00:06	Nepoužitá	Siréna	EOL	A B C D	1
7	Zona 007	E 0:00:07	Nepoužitá	Siréna	EOL	A B C D	1
8	PIR chodba bzuc	W 3:04:04	Okamžitá	Siréna		A B C D	7
9	PIR technici	E 3:01:01	Okamžitá	Siréna	DEOL	A B C D	1
10	GB technici	E 3:01:02	Okamžitá	Siréna	DEOL	A B C D	1
11	Pozar technici	E 3:01:03	Požár	Siréna	NO	A B C D	1
12	Pozar sklad v.	E 3:01:04	Požár	Siréna	NO	A B C D	2
13	Pozar sklad m.	E 3:01:05	Požár	Siréna	NO	A B C D	2
14	Tamper SIR	E 3:01:06	Nepoužitá	Siréna	EOL	A B C D	1
15	Zona 015	E 3:01:07	Nepoužitá	Siréna	EOL	A B C D	1
16	PIR prodejna	E 3:01:08	Vstupní následná	Siréna	DEOL	A B C D	2
17	PIR u dvorku	E 3:01:09	Vstupní následná	Siréna	DEOL	A B C D	1-2
18	PIR sklad v.	E 3:01:10	Okamžitá	Siréna	DEOL	A B C D	2
19	PIR sklad m.	E 3:01:11	Okamžitá	Siréna	DEOL	A B C D	2
20	GB sklad m.	E 3:01:12	Okamžitá	Siréna	DEOL	A B C D	2

Obrázek 25 Nastavení zón

Poté byly nastaveny výstupy, na kterých jsou připojené sirény. Jednalo se o relé na desce ústředny a o relé na výstupním expandéru. Oba výstupy byly nastaveny tak, aby kopírovaly systémovou sirénu. Dále byl jeden výstup nastaven tak, aby sledoval čidlo u vstupních dveří a

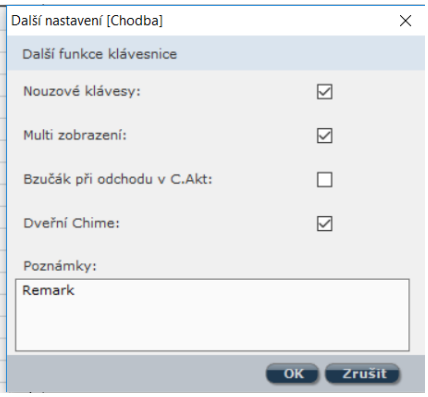
sepnul se, pokud by někdo dveřmi prošel. Na tomto výstupu je připojen bzučák umístěný u obsluhy. Nastavení výstupů je na Obrázek 26 Nastavení výstupů.

č.	Popis	Kanál	Charakter	Pulsní	Typ	Sleduje událost
1	001 Sirena	0:00:01	Přepínací NO		Sleduje systém	Siréna
2	Vystup 002	0:00:02	Pulsní NO	5	Není	
3	003 Bzucak	0:00:03	Pulsní NO	1	Sleduje zónu	Zona
4	Vystup 004	0:00:04	Pulsní NO	5	Není	
5	Vystup 005	0:00:05	Pulsní NO	5	Není	
6	Vystup 006	0:00:06	Pulsní NO	5	Není	
7	Vystup 007	3:01:01	Přepínací NC		Sleduje systém	Siréna
8	Vystup 008	3:01:02	Pulsní NO	5	Není	
9	Vystup 009	3:01:03	Pulsní NO	5	Není	
10	Vystup 010	3:01:04	Pulsní NO	5	Není	

Obrázek 26 Nastavení výstupů

Další položkou bylo nastavení klávesnic, u kterých byla nastavena maska, tedy podsystémy, které může klávesnice ovládat a podsystém, ve kterém je klávesnice umístěna. Poté bylo pro všechny klávesnice nastaveno zobrazení přehledu stavu jednotlivých podsystémů místo toho, aby ukazovaly pouze stav svého podsystému. Nastavení klávesnic je na Obrázek 27 Nastavení klávesnic.

č.	Popis	Kanál	Typ	Podsystém	Maska
1	Chodba	3:00:01	LCD	1	1-3, 7
2	Mriz	3:00:02	LCD	2	1-3
3	Uctarna	3:00:03	LCD	3	1-3
4	Klavesnice 4	0:00:00	NONE	1	1-8
5	Klavesnice 5	0:00:00	NONE	1	1-8
6	Klavesnice 6	0:00:00	NONE	1	1-8
7	Klavesnice 7	0:00:00	NONE	1	1-8
8	Klavesnice 8	0:00:00	NONE	1	1-8
9	Klavesnice 9	0:00:00	NONE	1	1-8
10	Klavesnice 10	0:00:00	NONE	1	1-8
11	Klavesnice 11	0:00:00	NONE	1	1-8
12	Klavesnice 12	0:00:00	NONE	1	1-8
13	Klavesnice 13	0:00:00	NONE	1	1-8
14	Klavesnice 14	0:00:00	NONE	1	1-8
15	Klavesnice 15	0:00:00	NONE	1	1-8
16	Klavesnice 16	0:00:00	NONE	1	1-8



Obrázek 27 Nastavení klávesnic

Dále byly nastaveny kódy pro zaměstnance, kteří mají mít přístup do některé z částí objektu. Všem uživatelům byl vytvořen defaultní kód v rozsahu 9400-9410 a byly jim přiřazeny oprávnění podle toho, kam se mají dostat. Všichni zaměstnanci si následně jim přidělený kód změnili přes klávesnici na takový, který jim vyhovoval. Nastavení kódů je na Obrázek 28 Nastavení kódů.

č.	Popis	Úroveň oprávnění	Kód	Proximity Tag	Podsystém
	Hlavni kod	Hlavní kód	••••		1-8
1	SIMEK	Uživatel	••••		1-3, 7
2	Rybak	Uživatel	••••		1-3
3	UZIV 003	Uživatel	*		1
4	Kounovsky	Uživatel	••••		1-3
5	Sladkova	Uživatel	••••		1-3
6	Apjarova	Uživatel	••••		1-3
7	Kacirek M	Uživatel	••••		1-3
8	Kacirek O	Uživatel	••••		1-3
9	Pausarova	Uživatel	••••		3
10	Urbancok	Uživatel	••••		1-3
11	Sebek	Uživatel	••••		1-3
12	CASTALOVSKY	Uživatel	••••		1-3, 7

Obrázek 28 Nastavení kódů

Následně byly nastaveny komunikátory ústředny. Prvně byl deaktivován PSTN komunikátor, který nebude nijak využit. Následně byl nastaven GSM komunikátor, u kterého byl nastaven PIN kód SIM karty. Dále bylo také nastaveno APN pro připojení k internetu, toto připojení bude využito pro komunikaci s PCO. Dále byl nastaven IP komunikátor, kde byla nastavena statická IP adresa, kterou měla předcházející ústředna a ostatní nezbytná síťová nastavení. Nastavení PCO je na Obrázek 29 Nastavení PCO.

	Typ	Kanál	Telefon	IP adresa	IP port
Monitorovací stanice 1	IP	Pouze GPRS		90.176.62.19	3010
Monitorovací stanice 2	IP	Pouze GPRS		83.208.59.243	3010
Monitorovací stanice 3	Hlas	PSTN/GSM			0

Obrázek 29 Nastavení PCO

5.3 Integrace do C4

Dle multikriteriální analýzy byla zvolena C4 jako nejvhodnější integrační SW. Proto po dokončení instalace PZTS ústředny byla provedena integrace právě do integračního SW C4. Tato integrace zahrnovala mnoho kroků, od přípravy serveru až po vytvoření vizualizace objektu.

5.3.1 Příprava serveru

Nejdříve bylo nutné vybrat vhodný server, na kterém poběží C4. Vzhledem k tomu, že se jedná o malou instalaci, je výrobcem C4 doporučený server s parametry: Intel i5, HDD 60 GB a RAM 4 GB. Dle těchto parametrů byl vybrán sever HP Pavilion HPE h8-1000cs, který disponuje následujícími parametry:

- Procesor: Intel® Core i5-2500
- Paměť: 4 GB DDR3 (1x4GB)
- Pevný disk: 1 TB (7200 ot/min)
- Optická mechanika: DVD+/-RW/RAM LightScribe DL
- Grafická karta: NVIDIA® GeForce™ GT 545 3GB
- Další: LAN 10/100/1000, Čtečka paměťových karet 15v1, 8xUSB 2.0, 2x USB 3.0

Jelikož se server dodává s nainstalovaným operačním systémem, nebylo po jeho obdržení nutné do něj instalovat jakýkoliv SW, kromě C4 a jejích komponent.

5.3.2 Instalace C4 serveru

C4 server je základní část C4, která se stará o komunikaci s technologiemi, zpracovává data a dává je k dispozici klientům. C4 server běží na serveru neustále a jednotliví uživatelé se k němu připojují z klientských stanic podle vlastní potřeby.

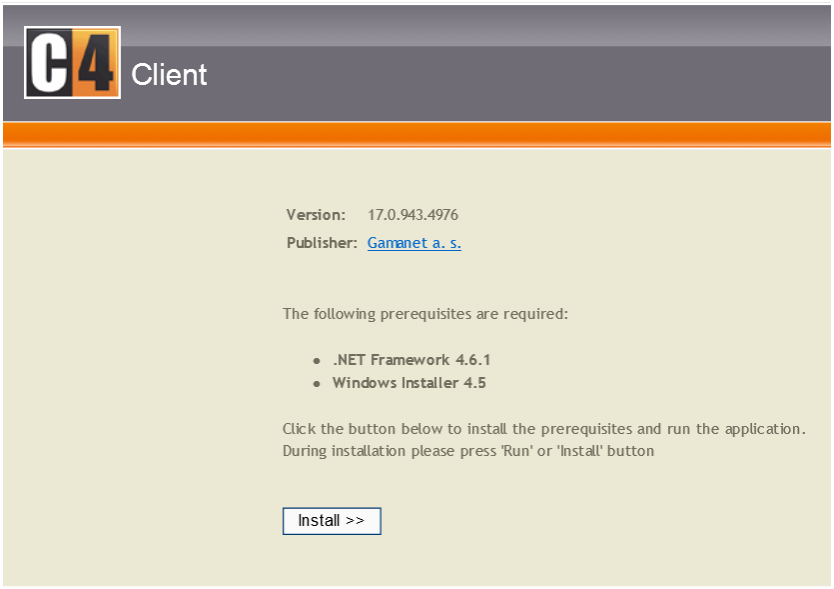
Po výběru a vhodného serveru byla provedena instalace C4 serveru verze 2017. Samotná instalace byla jednoduchá, průvodce provede vše sám, stačilo vybrat pouze adresář, kam se měla C4 nainstalovat. Průvodce dále nainstaloval další prekvizity, které jsou nezbytné pro fungování C4. Jednalo se o .NET framework a SQL server. Následně byl již nainstalován samotný C4 server. Celá instalace trvala na vybraném serveru přibližně 20 minut. Po dokončení instalace bylo možné nainstalovat klienta a připojit se do samotné C4.

5.3.3 Instalace klientů C4

Klienta C4 je možné nainstalovat na stejný PC, na kterém běží C4 server, ale výrobce to nedoporučuje. Proto byl klient C4 nainstalován na jiný PC, a to na PC správce objektu.

Instalace C4 klienta byla provedena z internetového prohlížeče Internet Explorer (v ostatních to není možné). Byla zadána adresa http://xxx.xxx.xxx.xxx/c4client/, kde xxx.xxx.xxx.xxx byla IP adresa serveru. V našem případě má server IP adresu 10.10.101.141. Objevila se stránka, která obsahovala základní informace o C4 serveru a byla zde možnost nainstalovat C4 klienta. Stránka je na Obrázek 30 Instalace klienta C4. Po kliknutí na tlačítko pro instalaci se objevilo dialogové okno, kde bylo nezbytné instalaci potvrdit a ta se následně provedla. Po jejím

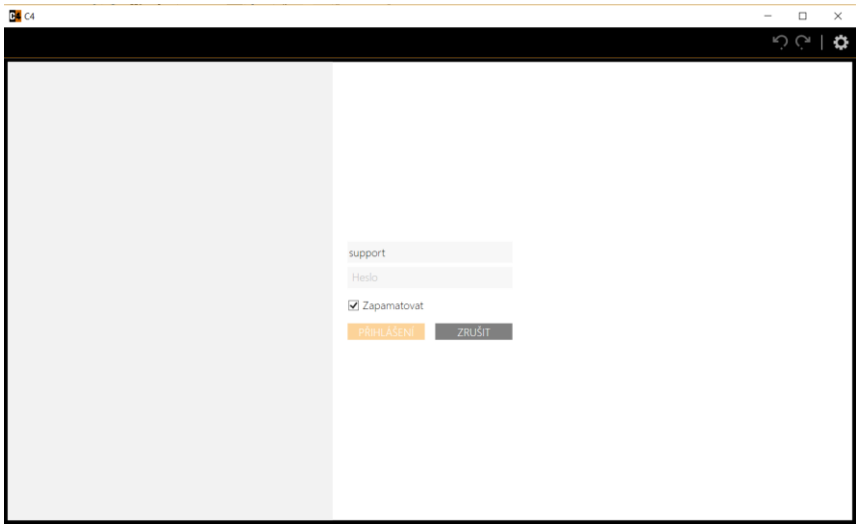
provedení bylo možné spustit C4 klienta, zástupce pro spuštění se automaticky vygeneroval na ploše.



Obrázek 30 Instalace klienta C4

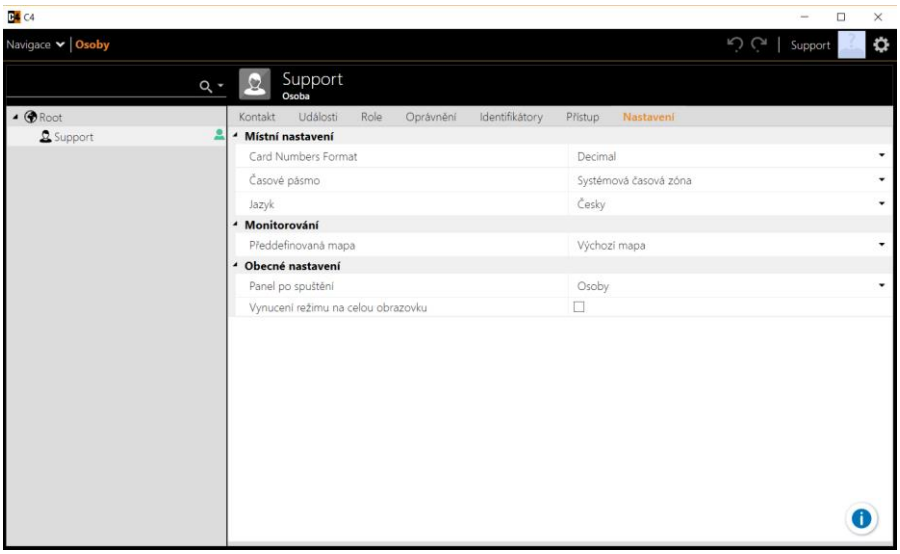
5.3.4 První spuštění systému

Pro první spuštění je defaultní účet „support“ a defaultní heslo „support“, které bylo nutné při prvním přihlášení změnit. Bez této změny hesla se nebylo možné do C4 přihlásit. Heslo bylo proto změněno na „Support“. Na Obrázek 31 Přihlašovací obrazovka C4 je k vidění přihlašovací okno C4.



Obrázek 31 Přihlašovací obrazovka C4

Jedná se administrátorský účet, který má nejvyšší oprávnění pro změny nastavení C4. Následně se zobrazilo okno, kde jsou vidět základní nastavení pro administrátorský účet. Toto okno je na Obrázek 32 Základní nastavení C4. Při prvním přihlášení byla C4 v anglickém jazyce, a proto byl ihned po přihlášení změněn jazyk na český. Následně bylo nutné C4 restartovat, aby se projevila změna jazyku. Při následném přihlášení byla již C4 v českém jazyce.



Obrázek 32 Základní nastavení C4

5.3.5 Instalace driverů

Drivery slouží jako propojovací člen mezi technologií a C4. Starají se o překlad komunikačního protokolu technologie na komunikační protokol C4, a tím zajišťují obousměrnou komunikaci mezi technologií a C4.

Pro instalaci driverů do C4 je určena záložka „Ovladače“. Při jejím otevření se ukáže seznam dostupných driverů. Je možné přidat i jiné drivery, a to pomocí načtení těchto driverů ze souboru. Dále je možné zobrazit nainstalované drivery a také je updatovat, pokud existuje vyšší verze. Pro tuto instalaci byly nainstalovány drivery na ProSYS Plus a Hikvision.

5.3.6 Přidání licencí

Aby bylo možné spojení se zařízením, je potřeba kromě driverů také licencí. Licenci bylo nezbytné získat od výrobce C4 Gamanetu a.s.. Pro vygenerování bylo nutné poskytnout MAC (Media Access Control) adresu serveru a jeho název. Proti těmto údajům bylo možné vygenerovat licenci. Po vygenerování licence byla licence přidána do C4 pomocí jednoduchého

průvodce, kterým C4 disponuje. Po její aktivaci se v C4 zobrazil stav licence, verze C4, MAC adresa PC a zařízení, které bylo možné připojit. Stav licence této instalace po jejím přidání je na Obrázek 33 Licence C4.

Obrázek 33 Licence C4

5.3.7 Strom zařízení

V dalším kroku bylo nezbytné vytvořit strom zařízení, který slouží k zobrazení stavů jednotlivých komponent, prvků jednotlivých technologií a také pro jejich ovládání.

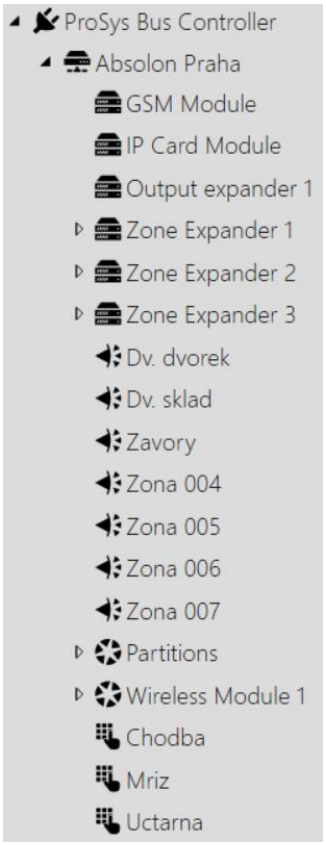
5.3.7.1 Strom ProSYS Plus

V prvním kroku integrace ProSYS Plus bylo nezbytné přidat řadič sběrnice. Řadič sběrnice je první bod, kde se nastavují základní parametry pro komunikaci s ústřednou ProSYS Plus. Jedná se o kód pro vzdálenou komunikaci (musí být stejný jako je nastavený v ústředně), interval dotazování (doba, po které se načítají události z ústředny), IP adresa a port, časové pásmo a povolení správy uživatelů v ústředně. Bez nastavení těchto údajů nebylo možné pokračovat dále. Řadič sběrnice se také používá pro ovládání komunikace driveru, tedy pro spuštění a zastavení této komunikace.

Dále byla vytvořena samotná ústředna, která se používá pro celkové zastřežení a odstřežení. Ústředna také slouží k zobrazení všech událostí ze zařízení.

Dále byl přidán IP a GSM modul. Ten slouží pouze pro zobrazení stavů těchto modulů. Dále byly přidány zónové expandéry a pod ně byly přidány zóny umístěné na těchto expandérech. Expandéry a jejich zóny byly naadresovány tak, jak jsou naadresovány v technologii. Tyto prvky slouží pouze k zobrazení svých stavů. Dále byly přidány jednotlivé podsystémy a pod ně byly nalinkovány zóny vytvořené pod zónovými expandéry. Podsystémy slouží pro odesílání příkazů

na zastřežení a odstřežení jednotlivých podsystémů. Dále byly přidány všechny výstupy, na kterých jsou zobrazeny stavy, tedy jejich sepnutí a rozepnutí, a které se zde dají ovládat. Poslední přidanou částí byly klávesnice, které slouží pouze pro zobrazení poruch z jednotlivých klávesnic. Ukázka stromu ProSYS Plus je na Obrázek 34 Ukázka stromu ProSYS Plus.



Obrázek 34 Ukázka stromu ProSYS Plus

5.3.7.2 Strom Hikvision

Nejprve byl přidán Hikvision řadič sběrnice, na kterém byly nastaveny základní parametry komunikace se záznamovým zařízením. Následně byly pod řadič přidány kamery a naadresovány podle kanálů v záznamovém zařízení. Tyto kamery se dají použít k zobrazení živého videa a případného záznamu. Strom je k vidění na Obrázek 35 Strom Hikvision.

Obrázek 35 Strom Hikvision

5.3.8 Vizualizace

Vizualizace slouží ke zjednodušení interpretace poplachů a dalších událostí obsluhou. Také slouží pro snazší ovládání technologií.

V prvním kroku vizualizace bylo rozplánováno, jak na sebe jednotlivé úrovně budou navazovat. Pro přehlednost byl v prvním kroku zvolen půdorys celého objektu. Při otevření vizualizace bude tedy zobrazen půdorys celého objektu, který bude odkazovat na 3 části objektu, a to chodby, přední část a zadní část. Zadní část bude následně ještě rozdělena na 2 patra. Pro implementaci těchto posloupností ve vizualizaci byly vytvořeny v programu Auto CAD 2016 půdorysy a bokorys jednotlivých částí a byly vloženy do C4.

Po vložení půdorysů byly do jednotlivých půdorysů přidány jednotlivé komponenty ProSYS Plus a Hikvisionu. Dále pro ProSYS Plus byly přidány i jednotlivé podsystémy pro jejich snadné ovládání.

5.3.9 Uživatelé

V posledním kroku byly vytvořeny uživatelské účty pro obsluhu. Nakonec byly požadovány 2 uživatelské účty, a to pro správce objektu a majitele firmy, která v objektu sídlí. První účet pro

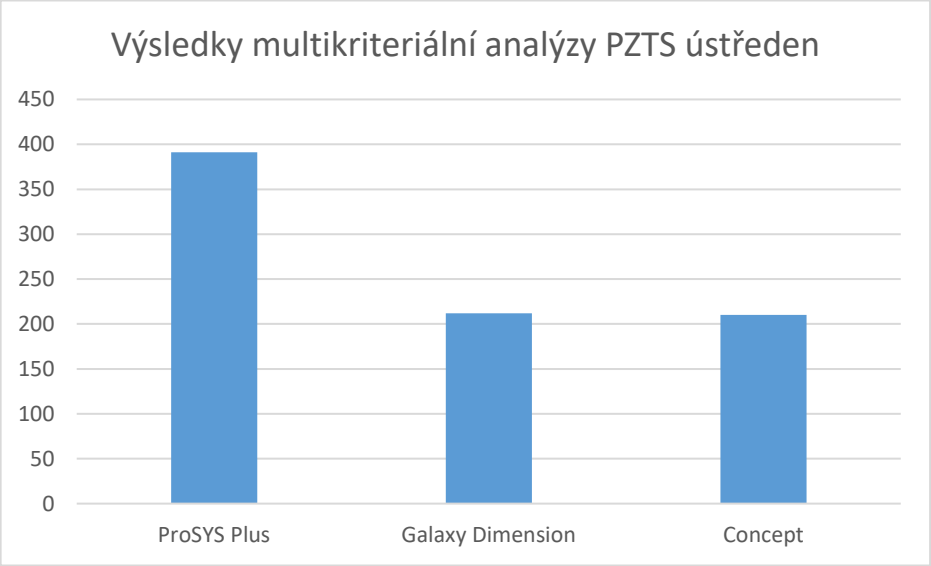
správce byl nastaven tak, aby mohl dohlížet na technologie a řešit události, např. poplachy, a ovládat technologii. Proto dostal automatické oprávnění Dispečer, které je v C4 předdefinováno. Druhý účet pro majitele firmy měl stejné možnosti jako účet pro správce objektu, ale byly mu přidány další oprávnění, například správa osob pro přidání případných dalších uživatelů.

Protože uživatelé ústředny PZTS byli vytvořeni již v ústředně a nebyl požadavek na jejich správu z C4, tak nebyli vytvořeni uživatelé technologie a na driveru byla zakázána správa uživatelů. Tím došlo k ponechání databáze uživatelů v zařízení bez změn z C4.

6 Zhodnocení výsledků

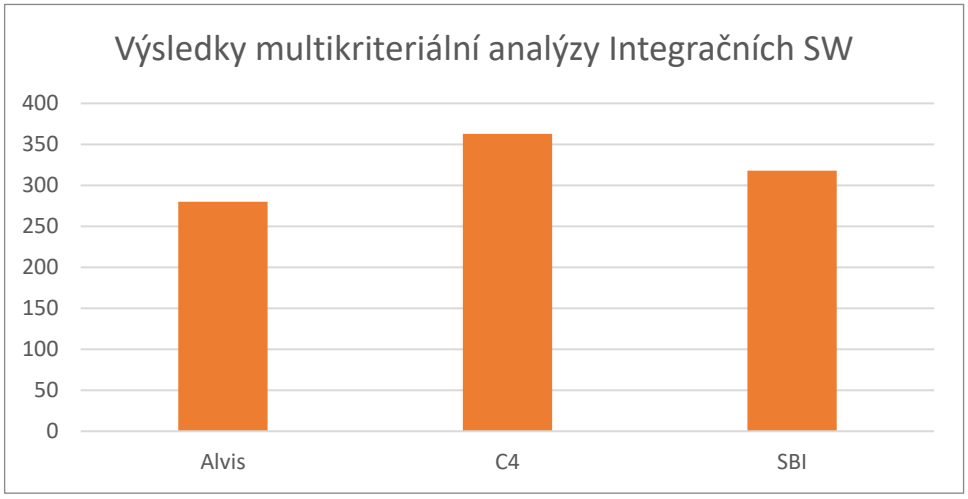
V multikriteriální analýze PZTS ústředen vyšlo, že nejvhodnější ústřednou je ProSYS Plus, která v multikriteriální analýze získala 391 bodů. Srovnání bodového zisku jednotlivých ústředen je v Tabulka 8 Výsledky multikriteriální analýzy PZTS ústředen.

Tabulka 8 Výsledky multikriteriální analýzy PZTS ústředen



V multikriteriální analýze integračních SW vyšlo, že nejvhodnější integrační SW je C4, který v multikriteriální analýze získal 363 bodů. Srovnání bodového zisku jednotlivých integračních SW je v Tabulka 9 Výsledky multikriteriální analýzy integračních SW.

Tabulka 9 Výsledky multikriteriální analýzy integračních SW



Na základě těchto analýz byla provedena výměna stávajícího poplachového, zabezpečovacího a tísňového systému za ProSYS Plus. Po úspěšné instalaci a nastavení systému byla provedena integrace do integračního softwaru C4 společně s kamerovým systémem Hikvision. Díky této integraci je možné ovládat a spravovat obě technologie z jednotného prostředí C4.

7 Závěr

V práci byl vytvořen přehled problematiky poplachových, zabezpečovacích a tísňových systémů, dále elektronické požární signalizace, kamerových systémů, elektronické kontrole vstupu a integračních softwarů. V rámci tohoto přehledu byly uvedeny komponenty těchto technologií. U integračních softwarů bylo uvedeno, jak obecně integrační softwary fungují a kde se nasazují.

V kapitole věnující se poplachovým, zabezpečovacím a tísňovým systémům bylo podrobně uvedeno, jak tento systém funguje, z jakých prvků se skládá, jakými možnostmi komunikace disponuje a jak se může ovládat.

V každé kapitole věnující se jednotlivé technologii bylo uvedeno, jaké nejčastější způsoby integrace do integračního SW jsou v současné době využívány.

V práci byly řešeny způsoby integrace jednotlivých technologií do integračních softwarů a následně v praktické části práce byly porovnány tři nejčastěji používané integrační softwary. Vzhledem k tomu, že integrační SW se používají spíše pro střední a velké objekty, byl pro praktickou část nalezen střední objekt a na něm byly aplikovány poznatky z rešeršní části a z multikriteriálních analýz.

V praktické části byla na daném objektu provedena demontáž staré PZTS ústředny a následná instalace nové, která byla vybrána v multikriteriální analýze. Tato instalace zahrnovala montáž sběrnicových prvků, instalaci kabeláže a následné oživení celé ústředny.

Po provedení instalace PZTS ústředny byla provedena integrace do vybraného integračního SW, díky čemuž bylo dosaženo jednotného uživatelského rozhraní pro ovládání a správu obou technologií.

8 Seznam použitých zdrojů

1. ABUS August Bremicker Söhne KG [online] [cit. 8.9. 2017], dostupné z WWW: <https://www.abus.com/eng/Guide/Break-in-protection/Alarm-systems/History-of-the-alarm-system>
2. VinTech Systems [online] [cit. 8.9. 2017], dostupné z WWW: <http://vintechnology.com/2011/04/08/back-to-basics-where-did-the-burglar-alarm-come-from/>
3. UHLÁŘ, Jan. Technická ochrana objektů 2. díl. Praha: Vydavatelství PA ČR, 2005. 229 stran. ISBN 80-7215-189-0
4. UHLÁŘ, Jan. Technická ochrana objektů 3. díl. Praha: Vydavatelství PA ČR, 2006. 246 stran. ISBN 80-7215-235-8
5. KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Blatná: Cricetus, 2002. 350 stran. ISBN 80-9029-382-4
6. Česká agentura pro standardizaci [online] [cit. 12.9. 2017], dostupné z WWW: <https://csnonline.agentura-cas.cz/Detailnormy.aspx?k=78248>
7. Kim, S.H.. Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition. Sunchon: Elsevier Ltd, 2018. ISSN 03064549
8. Alarmsecurity.cz [online] [cit. 12.9. 2017], dostupné z WWW: <https://www.alarmsecurity.cz/www-alarmsecurity-cz/5-TECHNICKA-PODPORA/5-Co-je-zabezpecovaci-system>
9. Talbot, C.M.. Detecting rogue attacks on commercial wireless Insteon home automation systems. Dayton: Elsevier Ltd, 2017. ISSN 01674048 >
10. Topinfo s.r.o. [online] [cit. 14.9. 2017], dostupné z WWW: http://www.tzb-info.cz/provoz-technologii/10735-charakteristika-falesnych-poplachu-z-hlediska-pricin-vyvolani-a-popis-moznych-reseni-1-dil
11. Mishra, V.P.. Analysis of alarms to prevent the organizations network in real-time using process mining approach. New York: Amity University, 2018. ISSN 13867857
12. ELKOV elektro a.s. [online] [cit. 15.9. 2017], dostupné z WWW: <http://www.ladinn.cz/ostatni/technika/princip-EZS.html>

13. KRUEGLE, Herman. CCTV Surveillance. Oxford: Elsevier, 2007. 641 stran. ISBN 0-7506-7768-6
14. Rohrschneider, K.. Closed-circuit television systems: Current importance and tips on adaptation and prescription. Germany: Springer Verlag, 2017. ISSN 0941293X
15. Vel'As, A.. Influence of changing the parameters of the camera system on video-based motion detection. London: Institute of Electrical and Electronics Engineers Inc., 2017. ISSN 10716572
16. Christie Intruder Alarms [online] [cit. 12.10. 2017], dostupné z WWW: <https://ciaalarms.co.uk/cctv/closed-circuit-television-overview/>
17. Kaenzig, R.. Videosurveillance and urban insecurities: Study of the preventive effectiveness of the cameras installed in the Pâquis neighborhood in Geneva. Neuchâtel: Copernicus GmbH, 2018. ISSN 00167312
18. Wickes, J.. CCTV: an open door into enterprise and national infrastructure. Cloudview: Elsevier Ltd, 2018. ISSN 13534858
19. ELKOV elektro a.s. [online] [cit. 17.10. 2017], dostupné z WWW: <http://www.ladinn.cz/ostatni/technika/kamerovy_system.html>
20. Téma: Provedení CCTV. Rozhovor s Pavlem kounovským (manažer CCTV ve firmě Alarm Absolon s.r.o.) dne 19.10. 2017
21. Lee, D.. De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment. New York: Springer New York LLC, 2018. ISSN 19366442
22. Úřad pro ochranu osobních údajů [online] [cit. 22.10. 2017], dostupné z WWW: <https://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf>
23. Topinfo s.r.o. [online] [cit. 1.11. 2017], dostupné z WWW: <http://www.tzb-info.cz/elektricka-pozarni-signalizace>
24. Topinfo s.r.o. [online] [cit. 2.11. 2017], dostupné z WWW: <http://www.tzb-info.cz/pozarni-bezpecnost-staveb/16573-aktualni-evropske-trendy-v-oblasti-pozarne-bezpecnostnich-zarizeni>
25. Gay, L.. Effects of cable fire smoke on electronic boards. Villeurbanne: International Association for Fire Safety Science, 2014. ISSN 18174299
26. Nemlaha, E.. Minimization of EPS polyfunctional buildings testing. Hong Kong: Hong Kong Industrial Technology Research Centre, 2013. ISSN 16609336

27. D3Soft s.r.o. [online] [cit. 5.11. 2017], dostupné z WWW: <http://www.alcamprofi.cz/elektricka-pozarni-signalizace-eps-evakuacni-rozhlas-er.html>
28. Association Convener [online] [cit. 12.11. 2017], dostupné z WWW: <https://www.scdf.gov.sg/content/scdf_internet/en/building-professionals/fire-safety-manager/download_slides_forfsmbriefing-26may09to9jul09/_jcr_content/par/download_1/file.res/FSMAS_Overview_of_Fire_Alarm_Systems_%26_Maintenance.pdf>
29. Santos, J.F.C.. Potentials and limitations of remote fire monitoring in protected areas. Viçosa: Elsevier B.V., 2017. ISSN 00489697
30. Téma: Základy EPS. Rozhovor s Vladimírem Černým (manažer EPS a EVAK ve firmě Alarm Absolon s.r.o.) dne 7.10. 2017
31. Cech elektrické požární signalizace České Republiky [online] [cit. 18.11. 2017], dostupné z WWW: <http://cecheps.cz/cz/zakony-a-normy.html>
32. Silva Consultants [online] [cit. 24.11. 2017], dostupné z WWW: <http://www.silvaconsultants.com/introduction-to-access-control-systems.html>
33. Kisi [online] [cit. 7.12. 2017], dostupné z WWW: <https://www.getkisi.com/components>
34. The balance [online] [cit. 9.12. 2017], dostupné z WWW: <https://www.thebalance.com/introduction-to-electronic-access-control-394578>
35. Lopez, J.. Access control for cyber-physical systems interconnected to the cloud. Malaga: Elsevier B.V., 2018. ISSN 13891286
36. Alonso-Ayuso, A.. Risk management for forestry planning under uncertainty in demand and prices. Philadelphia: Elsevier B.V., 2018. ISSN 03772217
37. Ing.Radek Zezula, UTKO FEKT VUT [online] [cit. 12.12. 2017], dostupné z WWW: <http://www.elektrorevue.cz/clanky/02054/index.html>
38. Téma: Fungování ACS. Rozhovor s Liborem Šimkem (manažer EZS a ACS ve firmě Alarm Absolon s.r.o.) dne 17.12. 2017
39. Česká agentura pro standardizaci [online] [cit. 12.9. 2017], dostupné z WWW: <https://csnonline.agentura-cas.cz/Detailnormy.aspx?k=58303>
40. C.G.C., a.s. [online] [cit. 22.12. 2017], dostupné z WWW: <http://www.cgc.sk/www.cgc.sk/sk/>

41. Gamanet a.s. [online] [cit. 22.12. 2017], dostupné z WWW: <https://wiki.gamanet.com/a/1768/main-article/c4-sdk-2017/general-overview>
42. S P I R I T - informačné systémy, a.s. [online] [cit. 23.12. 2017], dostupné z WWW: <http://www.alvis.sk/vlastnosti.php>
43. ABBAS, a.s. [online] [cit. 25.12. 2017], dostupné z WWW: <http://www.dominus.cz/software/c4/>
44. ABBAS, a.s. [online] [cit. 26.12. 2017], dostupné z WWW: <http://www.abbas.cz/produkty-a-sluzby/integrace/>

9 Seznamy

9.1 Seznam obrázků

9.2 Seznam tabulek