VLIV OSOBNÍ ZODPOVĚDNOSTI ZAMĚSTNANCE NA FUNKCI INTEGROVANÉHO SYSTÉMU ZABEZPEČENÍ OBJEKTU

The Influence of Employees´ Personal Responsibility on the Functioning of a Site Integrated Security System

Bc. David Tomšů

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. David Tomšů**
Osobní číslo:	**A14387**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Vliv osobní zodpovědnosti zaměstnance na funkci integrovaného systému zabezpečení objektu**
Téma anglicky:	**The Influence of Employees' Personal Responsibility on the Functioning of a Site Integrated Security System**

Zásady pro vypracování:

1. **Popište základní systémy zabezpečení středních objektů a vliv lidského činitele na jejich funkci.**
2. **Charakterizujte integrované bezpečnostní systémy z pohledu spolehlivosti zabezpečení objektů.**
3. **Naznačte další vývoj v této oblasti.**
4. **Definujte problém aktivace PZTS ze strany zaměstnance, vycházející z vaší praxe.**
5. **Proveďte návrh řešení definovaného problému.**
6. **Popište a vysvětlete princip navrhovaného řešení průběžného hodnocení početního stavu zaměstnanců ve firmě.**
7. **Navrhněte postup řešení modelových situací v případě selhání zaměstnance při úkonech spojených s činností zabezpečovacího systému.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **VALOUCH, Jan. Projektování integrovaných systémů. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj, 152 s.. ISBN 978-80-7454-296-1. Dostupné také z: http://hdl.handle.net/10563/25814.**
2. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2011-, 1 sv. ISBN 978-80-87500-05-7.**
3. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management III: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2013-, 3 sv. ISBN 978-80-87500-35-4.**
4. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 3. aktualiz. S.l.: Cricetus, 2006, 313 s. ISBN 80-902938-2-4.**
5. **UHLÁŘ, Jan. Technická ochrana objektů. Vyd. 1. Praha: Policejní akademie české republiky, 2005, 229 s. ISBN 80-7251-189-0.**
6. **KINDL, Jiří. Projektování bezpečnostních systémů I. 2. vyd. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.**

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

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

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

Ve Zlíně dne 5. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Jméno, příjmení: David Tomšů

Název diplomové práce: Vliv osobní zodpovědnosti zaměstnance na funkci integrovaného systému zabezpečení ojektu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 1.5.2016

.....
podpis diplomanta

ABSTRAKT

V této diplomové práci chci čtenáře seznámit s problematikou vlivu osobní zodpovědnosti zaměstnance na funkci integrovaného systému zabezpečení objektu. Teoretická část práce se věnuje popisu základních systémů zabezpečení objektů, jako jsou EPS, PZTS, ACS a CCTV. Jednotlivé systémy zabezpečení jsou popsány obecně, a následně také z pohledu negativního vlivu uživatele na funkčnost systému. Samostatná kapitola je věnována integrovaným zabezpečovacím systémům. Zde je kladen důraz na případné problémy integrace. V praktické části se věnuji řešení konkrétního problému, který spočívá v neprovedení aktivace PZTS zaměstnancem při odchodu ze zaměstnání, kdy firma zůstává nezabezpečena. V práci je navrženo a popsáno konkrétní řešení problému. Modelové situace vyplývající z chování zaměstnance jsou podrobně popsány a řešeny. Práce je doplněna algoritmy chování zaměstnance v systému.

Klíčová slova: Základní bezpečnostní systémy, integrovaný bezpečnostní systém, přístupový systém, docházkový systém, aktivace PZTS, bezpečnost systému.

ABSTRACT

The Thesis focuses on the issues concerned with the impact of personal responsibility of employees on the functioning of the Integrated Safety System at a workplace. The theoretical part describes basic safety systems in company buildings, such as Fire Detection and Fire Alarm System (FDAS), Intruder and Hold-up Alarm System (I&HAS), Access Control System (ACS) and Close Circuit Television (CCTV). Each individual system is described in general, followed by the user's negative impact point of view on the functioning of the system. A separate section is dedicated to Integrated Safety Systems alone, in which possible problems of integration are emphasised. In the practical part of the section I focus on a concrete issue, which stems from not activating I&HAS by an employee when leaving a workplace, resulting in the company being unprotected. The Thesis then proposes and describes a concrete solution of the issue. It also details and solves model situations which arise from such behaviour of an employee. The Thesis is accompanied by employee's behaviour algorithms in the system.

Key words: Basic safety systems, integrated safety system, access control system, entry system, PZTS activation, system's safety.

Chtěl bych poděkovat Ing. Rudolfu Drgovi Ph.D., za poskytnutí cenných rad, informací a pomoci při zpracování mé diplomové práce.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

K vypracování této diplomové práce mne vedla praktická zkušenost s provozem integrovaného poplachového systému firmy, ve které jsem zaměstnán. Tato firma se zabývá výrobou elektrotechnických zařízení. V rámci výrobního areálu jsou nastavena pravidla a nařízení, pomocí kterých je řízen vstup a pohyb zaměstnanců. Je zde zaměstnáno zhruba sto zaměstnanců v několika odděleních, a vzhledem k charakteru jejich činnosti a časovému rozložení pracovní doby není možné využít například automatickou aktivaci PZTS objektu k určité hodině. Zastřežení objektu je proto spojeno s úkonem pracovníka, který opouští pracoviště jako poslední, tudíž s jeho konkrétní odpovědností. Často se však stane, že objekt, či jeho část opustí většina zaměstnanců a systém PZTS není aktivován. Rozhodl jsem se proto, vypracovat diplomovou práci, ve které se budu věnovat vlivu osobní odpovědnosti zaměstnance na funkci integrovaného bezpečnostního systému ve firmě, a zároveň se pokusím nalézt řešení konkrétního problému.

Odpovědnost zaměstnance, respektive jeho povinnost provést zastřežení objektu je zřejmá. V praxi však stále existuje mnoho důvodů a výmluv ze strany zaměstnanců, proč nebylo zastřežení provedeno. Může se jednat o zapomenutí úmyslné či neúmyslné, nevědomost nebo vypočítavost. Výmluv lze najít opravdu mnoho.

Začal jsem proto přemýšlet, jakým způsobem přimět zaměstnance, kteří opouští firmu, aby systém PZTS aktivovali, pokud jsou poslední. Chtěl jsem najít vhodný způsob, který by zaměstnance v podstatě přinutil k zastřežení. Při zvažování různých variant jsem si uvědomil, že cesta dalších nařízení a restrikcí ze strany zaměstnavatele vůči zaměstnancům není vhodná. Většinou se takové inovace setkají spíše s nevolí a odporem, než s kladným přijetím. Zvolil jsem tedy řešení, které by umožnilo činnost spojenou s aktivací PZTS zautomatizovat.

K řešení bych chtěl využít integrovaný bezpečnostní systém zabezpečení objektu firmy. Konkrétně se jedná o softwarovou integraci PZTS a ACS s nadstavbou docházkového systému. Právě s její pomocí lze dosáhnout pozitivního vlivu odpovědnosti zaměstnanců na funkci integrovaného systému zabezpečení objektu.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ SYSTÉMY ZABEZPEČENÍ OBJEKTŮ

Mezi základní systémy zabezpečení objektů, kterými se budeme v této práci zabývat, patří elektrická požární signalizace, poplachový zabezpečovací a tísňový systém a přístupový systém.

Elektronické zabezpečovací systémy jsou důležitou součástí zajištění bezpečnosti, zdraví a života. Jednotlivé typy senzorů dokážou plně nahradit, a ve většině případů i překonat lidské smysly jako je zrak, čich nebo sluch. Ve spojení s hardwarovým a softwarovým vybavením dokáže systém hrozbu vyhodnotit a zareagovat během zlomku vteřin. Chybovost těchto zařízení je velice nízká a systémy dokážou kontrolovat samy sebe, nebo v případě sabotáže upozornit obsluhu. Právě jednání člověka, který zasahuje do systému, je předmětem této práce.

Zabezpečovací systémy jsou součástí technických prostředků ochrany majetku. Při návrhu zabezpečení je vždy nezbytné provést analýzu rizik. S pomocí analýzy rizik lze nadefinovat bezpečnostní hrozby, vůči kterým navrhneme zabezpečovací systém.

Bezpečnostní hrozby lze obecně rozdělit na **intencionální** a **neintencionální.** Mezi intencionální (záměrné) hrozby v kontextu střední firmy můžeme zařadit:

- neoprávněný vstup do objektu
- vloupání
- krádež
- vandalismus
- počítačovou kriminalitu
- úmyslné přerušení dodávky energií

Naproti tomu neintencionální (neúmyslné) hrozby zahrnují především:

- požár
- živelní pohromy
- havárie
- katastrofy
- nedbalostní chování pracovníků firmy

Z výše uvedeného vyplývá přirozená potřeba monitorovat a detekovat tyto hrozby takovým způsobem, abychom mohli včas a adekvátně zasáhnout.

Tyto hrozby je možné dále rozčlenit podle priority ohrožení hodnot. Všeobecně je brána jako nejvyšší priorita újma na zdraví či životě člověka. Proto jsou vždy poplachové aplikace na ochranu života a zdraví funkčně nadřazeny ostatním aplikacím. Do této skupiny patří požární hlásiče (EPS) a tísňové systémy (SAS). V další skupině jsou poplachové systémy na ochranu majetku a detekci vniknutí do objektu. Teprve za tyto skupiny je možné zařadit ostatní poplachové i nepoplachové aplikace, které jsou součástí integrovaných poplachových systémů.

V dalších podkapitolách budou popsány základní systémy zabezpečení středních objektů a vliv lidského činitele na jejich funkci.

1.1 Legislativní rámec v oblasti zabezpečení objektů

Stejně jako v řadě jiných činností i v oblasti zabezpečení objektu je nutné postupovat podle závazných předpisů, norem a pravidel. Ve většině případů se totiž jedná o dodávku systému na objednávku. Dodávka může zahrnovat nejen vlastní technologii, ale i následný provoz systému, nebo servis. Ovšem, i v případě, kdy si majitel objektu instaluje a provozuje zabezpečovací systém vlastními prostředky, musí mít tento systém požadované vlastnosti a jeho provoz musí být v souladu s příslušnými normami a právními předpisy.

Právní předpis je normativní právní akt představující soubor obecně závazných právních norem, které tvoří součást právního řádu.

Mezi právní předpisy patří základní (zákonné) právní předpisy (Ústava a ústavní zákony, Zákony a zákonná opatření), podzákonné (prováděcí) právní předpisy (vládní nařízení, vyhlášky - ústředních správních úřadů, ministerstev, České národní banky, obecně závazné vyhlášky obcí nebo krajů, nařízení obcí nebo krajů). [1] Právní předpisy související s problematikou této práce můžeme uvézt např.:

- Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti.
- Zákon č.181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
- Zákon č. 360/1992 Sb. o výkonu povolání autorizovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě.
- Vyhláška č. 50/1978 Sb. o odborné způsobilosti v elektrotechnice.
- Vyhláška č. 246/2001 Sb. o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru - vyhláška o požární prevenci.

- Vyhláška č. 499/2006 Sb. o dokumentaci staveb.

Česká technická norma (ČSN) je dokument schválený pověřenou právnickou osobou pro opakované nebo stálé použití vytvořený podle tohoto zákona (Zákon č. 22/1997 Sb. o technických požadavcích na výrobky a o změně a doplnění některých zákonů) a označený písmenným označením ČSN, jehož vydání bylo oznámeno ve Věstníku Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví. Česká technická norma poskytuje pro obecné a opakované používání pravidla, směrnice nebo charakteristiky činností zaměřené na dosažení optimálního stupně uspořádání ve vymezených souvislostech. [1]

Příklady ČSN užitých v oblasti bezpečnostních technologií (Tab. 1).

Tab. 1. Základní členění ČSN EN v oblasti poplachových systémů. [1]

Číslo normy (řada)	**Název**
ČSN EN 50 130-x-y	Poplachové systémy (všeobecné požadavky).
ČSN EN 50 131-x-y	Poplachové systémy - PZTS.
ČSN EN 50 132-x-y	Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích.
ČSN EN 50 133-x-y	Poplachové systémy - systémy kontroly vstupů pro použití v bezpečnostních aplikacích.
ČSN EN 50 134-x-y	Poplachové systémy - systémy přivolání pomoci.
ČSN EN 50 136-x-y	Poplachové systémy - poplachové přenosové systémy.
ČSN EN 50 137-x-y	Poplachové systémy - systémy kombinované nebo integrované (viz ČSN CLC/TS 50398).

Mezi další dokumenty, se kterými se můžeme při tvorbě poplachového systému setkat, patří **technická norma (TN).** Tento dokument představuje jakákoliv technická pravidla, směrnice nebo charakteristiky činností nebo jejich výsledků. Technické normy nejsou součástí právního řádu.

Technická normalizační informace (TNI) je technický dokument informativního charakteru, který obsahuje technické údaje nebo technická řešení, která nejsou obsažena v platných normách.

Prohlášení o shodě je doklad, kterým výrobce zaručuje shodu vlastností a technických parametrů výrobků s požadavky právních předpisů a norem. Postup při posouzení shody stanoví zákon č. 22/1997 Sb. v platném znění a příslušná nařízení vlády (NV). Výrobek, kterému bylo vydáno prohlášení o shodě, nese povinně označení CE.

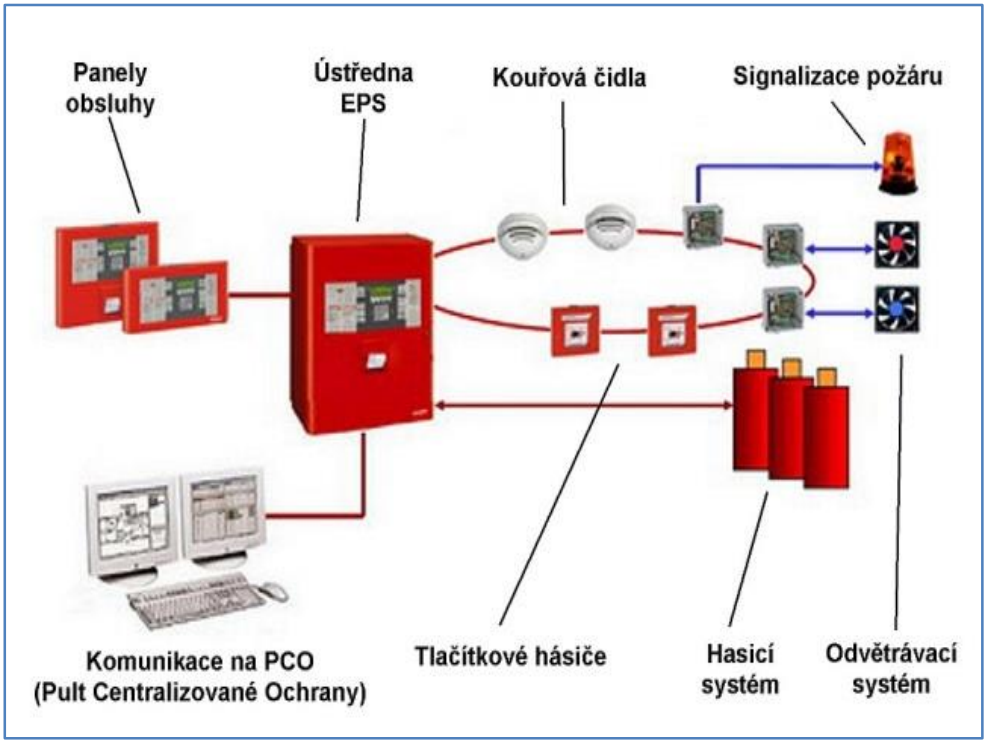
1.2 EPS - elektrická požární signalizace

Požáry způsobují každoročně značné ztráty na majetku a hlavně na lidských životech. V České republice jsou majetkové škody v řádu miliard korun a zahyne při nich více jak sto osob ročně. Jedním z opatření jak těmto škodám zabránit a zároveň zvýšit požární bezpečnost staveb, je využití požárně bezpečnostních zařízení. [2]

Elektrická požární signalizace pomáhá při včasném zjištění vznikajícího požáru. K tomuto účelu je využíváno několik druhů a typů požárních hlásičů, které jsou společně s dalšími komponenty zapojeny do systému EPS.

1.2.1 Obecný popis systému EPS

Základní EPS je sestaven z ústředny EPS, požárních hlásičů, tísňových hlásičů, signalizace požáru, panelu obsluhy a komunikačním rozhraním. Může být doplněn o hasící systémy, odvětrávací systém, atd. (Obr. 1).



Obr. 1. Základní schéma systému EPS. [3]

Tato diplomová práce se zabývá komponenty zabezpečovacích systémů, které může přímo ovlivnit uživatel. Proto se dále budeme soustředit především na tlačítkové hlásiče požáru.

Hlásiče požáru lze rozdělit dle dvou základních principů na samočinné a tlačítkové.

Samočinné hlásiče požáru dokážou vniklý požár identifikovat, lokalizovat a ohlásit. To vše bez nutné přítomnosti obsluhy. Podle způsobu detekce je rozdělujeme na:

- Hlásiče kouře ionizační a optické.
- Hlásiče teplot.
- Hlásiče plamene.
- Hlásiče plynu.
- Hlásiče multisenzorové. [2]

Tlačítkové hlásiče požáru (Obr. 2.) slouží k vyhlášení poplachu osobou, která zjistí požár nebo jiný nebezpečný jev. Kryt tlačítkového hlásiče požáru je vyhotoven vždy v červené barvě a nesmí umožňovat samovolné nebo náhodné spuštění poplachu. Po vyhlášení poplachu musí být zřejmé, který hlásič jej vyvolal. [4]

Obr. 2. Tlačítkový hlásič požáru. [5]

1.2.2 Specifika projektování elektrické požární signalizace EPS

Vyhláška č. 499/2006 Sb. o dokumentaci staveb ukládá povinnost vypracovat jako součást projektové dokumentace pro ohlášení stavby dle § 104 odst. 1 písm. a) až e) stavebního zákona, požárně bezpečnostní řešení. Tímto se návrh a provoz EPS odlišuje od ostatních systémů zabezpečení. Je zřejmé, že záchrana života a zdraví má jasnou prioritu.

„Elektrická požární signalizace je dle vyhlášky č. 246/2001 Sb. (Vyhláška Ministerstva vnitra o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru -vyhláška o požární prevenci) vyhrazeným požárně bezpečnostním zařízením (PBZ). Proto musí projektovou dokumentaci pro instalaci požární signalizace vypracovat pouze kvalifikovaný projektant, způsobilý pro tuto činnost, který získal oprávnění k projektové činnosti podle zvláštního právního předpisu s autorizací v tomto oboru. Kvalifikace a autorizace musí být spolu s prohlášením projektanta o osobní odpovědnosti za kvalitu provedené činnosti a splnění podmínek stanovených právními předpisy, normativními požadavky a průvodní dokumentací výrobce konkrétního typu požárně bezpečnostního zařízení doložena v projektové dokumentaci.

Podkladem pro vypracování projektu elektrické požární signalizace je zejména projekt požárně - bezpečnostního řešení stavby, požární zpráva, kde jsou vzneseny požadavky na hlídání prostorů systémem požární signalizace EPS a také na funkci a návaznost na další zařízení, která jsou systémem EPS ovládána nebo monitorována. Dále je nutné zajistit projektové podklady od dodavatelů těchto návazných zařízení na systém elektrické požární signalizace a projednání technického řešení koordinace jejich funkcí s elektrickou požární signalizací.

Projekt elektrické požární signalizace je pak spolu s projektovou dokumentací ostatních požárně bezpečnostních zařízení PBZ, elektroinstalace a požárně - bezpečnostním řešením stavby předložen k vyjádření zástupci Hasičského záchranného sboru. Na základě takto schválené projektové dokumentace je nutné provést prováděcí projekt, podle kterého je pak EPS instalována.

Po instalaci a zprovoznění systému elektrické požární signalizace EPS je nutné zajistit dokumentaci skutečného provedení EPS, která je jedním z hlavních předpokladů plnohodnotné údržby a servisu zařízení elektrické požární signalizace.“ [6]

1.2.3 Vliv lidského činitele na systém EPS

Jedním z komponentů EPS, na který má přímý vliv člověk, je tlačítkový hlásič požáru. Je zde totiž nutná obsluha člověkem. Člověk je ten, kdo musí v první řadě vzniklý požár zjistit a následně použít tlačítkový hlásič. To ovšem předpokládá, že dotyčný člověk zachová rozvahu, dokáže hlásič rychle najít a správně použít.

Jiná situace může nastat, pokud bude tlačítkový hlásič zneužitý, nebo se stane předmětem vandalismu. Proti náhodnému použití je samotné tlačítko chráněno v pevném pouzdru. Navíc je kryto tenkým sklem, které je nutno před použitím rozbít. Toto funguje i jako psychologická bariéra, která může v prvním okamžiku vandala odradit od vyvolání planého poplachu.

U samočinných hlásičů se projeví vliv lidského činitele zejména při zanedbání a nedodržení základních požadavků montáže a provozu EPS. Samočinné hlásiče pracují automaticky, a pokud je systém kvalitně a odpovědně naprojektován, neměl by jej lidský faktor nějak významně ovlivňovat. Problémová situace může nastat po vyhlášení samotného poplachu. Systém správně vyhodnotí situaci a při vzniku požáru vyhlásí poplach. Pracovník dohledového centra podcení vzniklou situaci nebo nepostupuje dle závazných předpisů. V této situaci se projeví vliv jeho jednání na EPS jako celek.

Některé ze základních požadavků při realizaci EPS uvádím níže:

- Použití typu a principu hlásiče vhodného pro daný prostor.
- Správné umístění hlásiče s ohledem na povahu prostoru.
- Využití inteligentní analýzy signálu v hlásičích.
- Správné nastavení hlásiče v souladu s podmínkami prostředí.
- Vymezení času pro obsluhu na verifikaci místa požáru před odesláním hlášení na HZS.
- Kvalitně zpracované a důsledně dodržované předpisy pro chování v objektech.
- Realizace školení a osvěty techniků, projektantů, hasičských záchranných sborů a dalších osob, které spolupracují na vytváření EPS v objektech.
- Pravidelné testování funkčnosti a údržba systémů – správné provádění kontrol a zkoušek systémů EPS dle norem a nařízení.
- Pravidelná modernizace systému – zejména po uplynutí doby životnosti. [7]

1.3 PZTS – poplachový zabezpečovací a tísňový systém

Poplachový zabezpečovací a tísňový systém je kombinací poplachového zabezpečovacího systému a poplachového tísňového systému. Dříve se označoval tento systém jako EZS - **elektrický zabezpečovací systém**, či EZTS - **elektrický zabezpečovací a tísňový systém**. V současné době je jako poplachový zabezpečovací systém PZS označován systém pro detekci a signalizaci vniknutí narušitele nebo zloděje do objektu. Poplachový tísňový systém PTS pro případ nouze (přepadení, zdravotní potíže, únik plynu, zaplavení, …), umožňuje úmyslné vyvolání poplachu. PZTS lze instalovat jako autonomní, tzn. bez připojení na PPC. V takovém případě se při narušení objektu spustí signalizace, popřípadě je odeslána informace majiteli, který si sám řídí další postup.

Každý PZTS musí mít stanoven stupeň zabezpečení (Tab. 2) a klasifikaci prostředí (Tab. 3).

Tab. 2. Stupně zabezpečení komponentů PZTS (dle ČSN EN 50131-1). [8]

Stupeň 1	Nízké riziko (NR)	Předpokládá se, že narušitelé mají malou znalost PZTS, a že mají k dispozici omezený sortiment snadno dostupných nástrojů.
Stupeň 2	Nízké až střední riziko (NR/SR)	Předpokládá se, že narušitelé mají určité znalosti o PZTS, a že použijí základní sortiment nástrojů a přenosných elektronických přístrojů.
Stupeň 3	Střední až vysoké riziko (SR/VR)	Předpokládá se, že narušitelé jsou obeznámeni s PZTS a mají úplný sortiment nástrojů a přenosných elektronických přístrojů.
Stupeň 4	Vysoké riziko (VR)	Očekává se, že narušitelé mají podrobné informace pro zpracování podrobného plánu vniknutí, a že mají kompletní zařízení a prostředky umožňující nahradit rozhodující prvky PZTS.

Tab. 3. Klasifikace prostředí (dle ČSN EN 50131-1). [8]

Třída I	Prostředí vnitřní	Komponenty PZTS musí správně pracovat při působení vlivů prostředí, které se vyskytuje ve vytápěných místnostech. Předpokládají se změny teplot

		v rozmezí + 5 °C až + 40 °C, při střední relativní vlhkosti okolo 75 % bez kondenzace.
Třída II	Prostředí vnitřní všeobecné	Komponenty PZTS musí správně pracovat při působení vlivů prostředí, které se vyskytuje všeobecně v objektech, kde není udržována stálá teplota. Předpokládají se změny teplot v rozmezí - 10 °C až + 40 °C, při střední relativní vlhkosti okolo 75 % bez kondenzace.
Třída III	Prostředí venkovní chráněné	Komponenty PZTS musí správně pracovat při působení vlivů prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty nejsou vystaveny plně vlivům počasí. Předpokládají se změny teplot v rozmezí - 25 °C až + 50 °C, při střední relativní vlhkosti okolo 75 % bez kondenzace. V průběhu roku se po dobu 30 dnů předpokládají změny relativní vlhkosti v rozmezí 85 % až 95 % bez kondenzace.
Třída VI	Prostředí venkovní všeobecné	Komponenty PZTS musí správně pracovat při působení vlivů prostředí, které se vyskytuje všeobecně vně budov s tím, že komponenty jsou vystaveny plně vlivům počasí. Předpokládají se změny teplot v rozmezí - 25 °C až + 60 °C, při střední relativní vlhkosti okolo 75 % bez kondenzace. V průběhu roku se po dobu 30 dnů předpokládají změny relativní vlhkosti v rozmezí 85 % až 95 % bez kondenzace.

1.3.1 Požadavky na integraci poplachových zabezpečovacích a tísňových systémů

„Uvedené požadavky vychází z ustanovení řady technických norem ČSN EN 50131, především ČSN EN 50131-1 ed.2 a ČSN EN 50131-7. Požadavky na integraci poplachových zabezpečovacích a tísňových systému lze charakterizovat v následujících bodech:

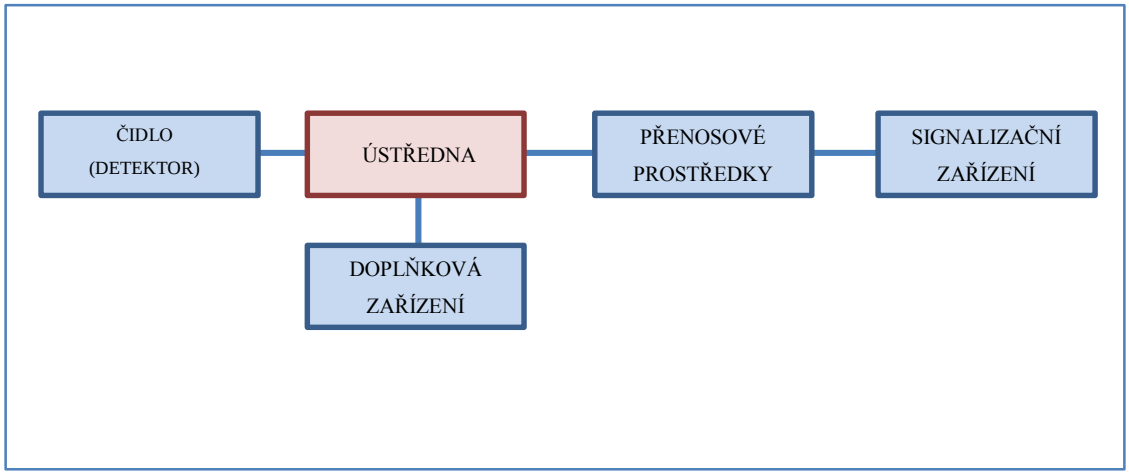
- PZTS mohou být rozšířeny o doplňková zařízení - zařízení použitá pro ovládací účely, která mohou představovat např. klávesnice, biometrické prvky, čtečky karet

nebo klíčenek atd. umístěná vně střeženého prostoru, pomocí kterých lze PZTS ovládat (uvádět do stavu střežení nebo klidu),

- pro PZTS jsou definovány přístupové úrovně s ohledem na možnost uživatelů k přístupu ke komponentům systému,
- pro PZTS jsou definovány požadavky na indikaci s ohledem na stupeň zabezpečení (např. v rámci integrace se systémem kontroly vstupu by bylo nutné zajistit indikaci jednotlivých vstupů do objektu i v systému PZTS),
- propojení komponent musí být navrženo tak, aby byla minimalizována možnost zpoždění, modifikace, záměny nebo ztráty signálů,
- propojení systémů musí být monitorováno,
- propojení komponent je klasifikováno na specifické (v rámci jedné aplikace) / nespecifické (mezi aplikacemi), kdy je třeba vzít v úvahu vliv jiných systémů, sdílejících společné vedení,
- požadavek na aplikaci prostředků, které zajistí, aby chyby obsluhy, které by mohly negativně ovlivnit funkce PZTS, byly eliminovány nebo indikovány,
- v systému PZTS je možné použít i komponenty, pro které neexistují technické normy, a které tudíž nemají stanoven stupeň zabezpečení, celkový stupeň zabezpečení PZTS pak odpovídá stupni zabezpečení komponentu nejnižšího stupně, u kterého je stupeň zabezpečení stanoven,
- jsou definovány požadavky na zpracování signálů (vniknutí, tíseň, sabotáž, porucha) - musí být vyhlášeny do 10 s,
- v rámci oblasti úpravy pod názvem „kompatibilita“ jsou stanoveny obecné požadavky na vzájemnou kompatibilitu výrobků, konzultace s výrobcem, distributorem, zkušebnou atd.,
- v rámci zpracování návrhu systému je nutné v případě integrace popsat vzájemné vazby jednotlivých systémů, a to v části dokumentu Návrh systému - konfigurace systému a rovněž tyto vazby a propojení jednotlivých aplikací schematicky znázornit v části dokumentu Návrh systému - seznam vybavení.“ [1]

1.3.2 Obecný popis PZTS

Základní struktura PZTS je v shodná s předchozím systémem EPS. Je tvořena detektory (vstupy), ústřednou PZTS, signalizačním zařízením (výstupy), přenosovou soustavou, napájením a ovládáním. Níže uvedený nákres (Obr. 3) zobrazuje obecné schéma poplachového systému PZTS.



Obr. 3. Blokové schéma PZTS. [9]

Prostory střežení

Jednotlivá čidla je možno pro ovládací účely soustřeďovat do skupin. Takto lze např. nastavit stav střežení (klidu) části systému, nebo pomocí jednoduchých příkazů zablokovat některá čidla (tzv. sektory střežení).

Základním prvkem PZTS z hlediska signalizace je smyčka. Podle Uhláře [9] „ Smyčkou rozumíme skupinu čidel nebo tísňových hlásičů či sabotážních kontaktů, která jsou propojena společným vedením a na výstupu ústředny vyhodnocována.“ Smyčku lze v oprávněných případech vyjímat ze střežení (přemostit). Elementárním prvkem z hlediska ovládání je podsystém. Zahrnuje jednu nebo více smyček se společným ovládáním. Smyčka může být společná pro více podsystémů, ale neměla by sdružovat čidla z odlišných prostor. Důvodem je ztížená identifikace místa narušení. Podle způsobu napojení smyček na ústřednu PZTS rozlišujeme připojení:

- smyčkové
- s přímou adresací čidel
- koncentrátorové – smíšené
- bezdrátové
- hybridní [9]

1.3.3 Prvky PZTS přímo ovládané uživatelem

Veřejné tísňové hlásiče jsou určeny pro vyvolání tísňového hlášení pro veřejnost. Zpravidla se umísťují na viditelných místech objektů (schodiště, chodby a haly), tak aby jejich použití bylo co nejjednodušší a nejrychlejší. Jejich konstrukce je podobná tlačítkovému požárnímu hlásiči. Pro jejich aktivaci je nutno překonat ochranné sklíčko. [9]

Speciální tísňové hlásiče slouží obsluze k nepozorovanému vyvolání poplachu v případě přímého ohrožení. Využívají se zejména v chráněných objektech (pokladny, banky, účtárny,…). Obsluha musí být předem zaškolena ve způsobu použití těchto zařízení. Konstrukčně jsou připraveny pro okamžité použití. Příklady speciálních tísňových hlásičů:

- lištové
- tlačítkové
- výklopné
- bankovková čidla
- osobní tísňové hlásiče [9]

Ovládací zařízení

Základní funkcí ovládacího zařízení je aktivace a deaktivace PZTS. Výběr vhodného typu zařízení usnadní ovládání uživatelům. Požadavky jsou kladeny zejména na omezení planých poplachů a dostatečnou ochranu proti překonání.

Další funkce ovládacího zařízení:

- Zadávání uživatelských kódů pro ovládání systému.
- Odstavení a resetování poplachů.
- Odpínání a připínání smyček (pro částečné střežení).
- Volbě speciálních funkcí (tísňové hlášení z klávesnice, vyvolání paměti aj.).
- Programování parametrů systému.

Klávesnice

„Nezbytnou součástí každého systému je alespoň jedna klávesnice. Slouží pro uvedení do stavu střežení a stavu klidu systému EZS (Obr. 4). Při programování systému se projeví komfort, který poskytuje LCD displej. Displej je užitečný také k prohlížení historie událostí. Rozdělení typů klávesnic:

- Klávesnice s LCD displejem.

- Klávesnice s podsvícením kláves (LED diody).

Obr. 4. LCD klávesnice (vlevo), klávesnice s podsvícením. [10]

U klávesnic s podsvícením kláves probíhá potvrzení a zobrazení hodnot prostřednictvím podsvícení kláves, což bývá velmi nepřehledné a pomalé. Propojení se systémem EZS je totožné, jako je tomu u rozšiřujících modulů. Často je využita společná komunikační linka. Některé klávesnice v sobě integrují vstupy a výstupy pro detektory a jiná zařízení. Pro instalaci a používání klávesnic platí určitá pravidla:

- Elektronika klávesnice musí být v samostatné skříni.
- Klávesnice musí být umístěna uvnitř střežených prostor.
- Klávesnice musí být umístěna tak, aby neoprávněné osoby nemohly sledovat její ovládání, není-li chráněna nebo ukryta.
- Je nutné pečlivě navrhnout přístupové a odchodové postupy s cílem minimalizovat plané poplachy.
- Zajistit potřebnou signalizaci pro účely identifikace poruch nebo poplachu. [10]

K dalším ovládacím zařízením patři **blokovací zámky**, které jsou z hlediska uživatele nejjednodušším a nejbezpečnějším druhem ovládacího zařízení. Montují se jako přídavné zámky dveří a jejich konstrukce zajišťuje bezchybné uvádění zabezpečovacího zařízení do stavu střežení (klidu). Na podobném principu pracují **spínací (propouštěcí) zámky.** Hlavní

rozdíl je v tom, že nevyužívají blokovací elektromagnetické západky. Využívají se k samostatnému odpojování smyček či odpojení pracovního kontaktu čidel. [9]

1.3.4 Vliv lidského činitele na systém PZTS

Problém veřejných tísňových hlásičů spočívá zejména v jejich zneužití, a to jak úmyslném tak i neúmyslném. Při úmyslném zneužití může jít o vandalismus nebo o použití hlásiče z nesprávného důvodu (např. požadavek na přivolání servisního vozu k nepojízdnému automobilu). Neúmyslné spuštění může nastat zejména při nehodě, stěhování, stavebních úpravách, atd.

Druhý extrém nastává v okamžiku, když chce uživatel oprávněně, v případě nouze použít tísňový hlásič, ale z nějakého důvodu jej nenajde. Typicky se může jednat o zakrytí hlásiče kusem nábytku, květináčem nebo plakátem. Pro **tísňové hlásiče** není vhodná autonomní instalace. Je to zejména kvůli charakteru systému, který má za úkol upozornit obsluhu PPC, že je někdo nebo něco v tísni. Pouze v takovém případě může obsluha PPC účinně zasáhnout, a poskytnout potřebnou pomoc. Řešení spočívající v odeslání zprávy např. na mobilní telefon majitele se zde jeví jako nedostatečné, jelikož je závislé na mnoha faktorech funkčnosti zařízení, dostupnosti mobilní sítě a samotného příjemce. V situacích, kdy je ohroženo zdraví a život je potřeba mít zajištěn kvalitní poplachový přenosový systém a spolehlivého příjemce.

U **speciálních tísňových hlásičů** je problém spíše s náhodným spuštěním obsluhou, nebo se může jednat o neodbornou manipulaci se zařízením. Zásadní nedostatek je obdobný jako u veřejných hlásičů. Je to nedostupnost hlásiče způsobená nedbalostí a nedodržením pravidel používání.

Vysoce rizikovým prvkem ovládání PZTS je za určitých okolností **kódová klávesnice**. Jejím prostřednictvím je možné aktivovat či deaktivovat celý systém střežení. Primární způsob zabezpečení tohoto prvku spočívá v nutnosti zadání hesla (PIN) na číselné klávesnici. To vyžaduje od obsluhy dodržování několika základních pravidel:

- Zapamatovat si PIN.
- Nesdělovat PIN ostatním osobám (PIN je osobní, nikoli veřejné číslo).
- Pokud si PIN musí zaznamenat, měl by být uložen pouze v trezoru, nebo v datovém úložišti, náležitě zašifrován.
- Dbát při zadávání do klávesnice na to, aby nebylo možné PIN odečíst. Klávesnice by měla být umístěna na objektu tak, aby toto co nejvíce znemožňovala.

- Měnit PIN minimálně jednou měsíčně. Důvodů je několik. V prvé řadě, s přibývajícím časem roste pravděpodobnost vyzrazení nebo prolomení kódu. Dále při opakovaném zadávání stejných číslic dochází k opotřebení klávesnice, což usnadňuje potencionálnímu pachateli útok.

Mezi výhody patří možnost použití tísňového kódu v rizikovém okamžiku vstupu do objektu.

Jedním z hlavních problémů souvisejících s obsluhou PZTS prostřednictvím kódové klávesnice ze strany zaměstnanců je neprovedení zastřežení objektu při odchodu. Touto problematikou se budu zabývat v praktické části diplomové práce.

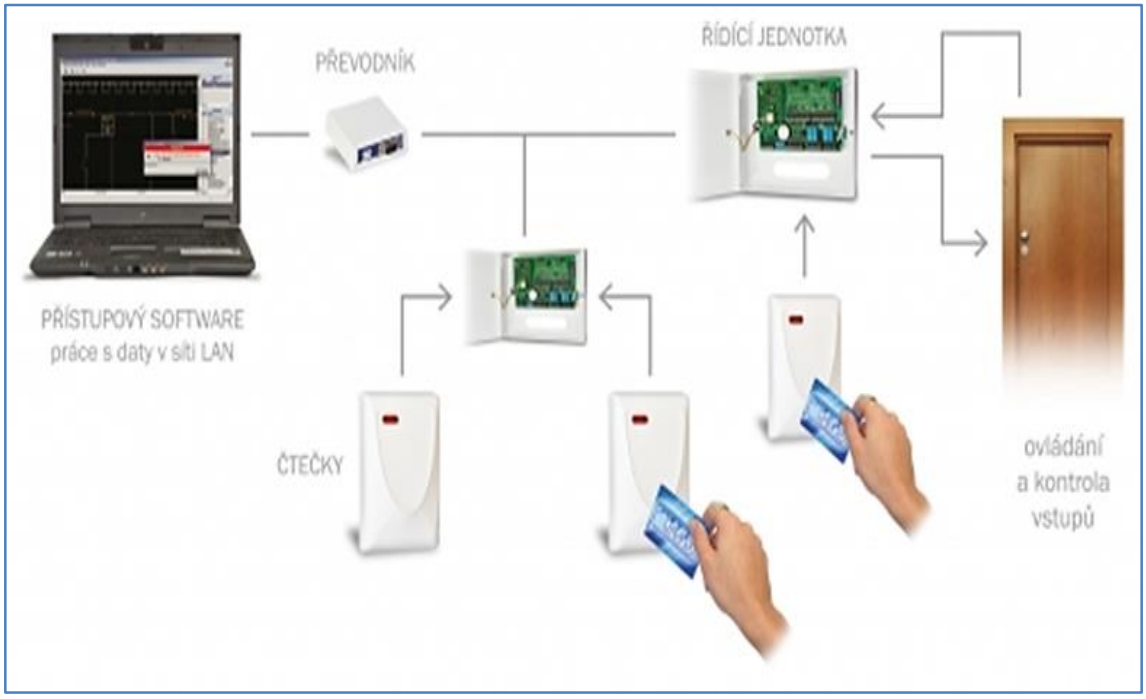
Při použití **blokovacích zámků** může být neoprávněnou osobou zneužit autorizovaný klíč, na kterém je celý systém závislý. [9]

Příčina selhání ochrany v PZTS může být i v **použití detektoru** využívajícího fyzikální jev, který může ve střeženém prostoru s velkou pravděpodobností vzniknout i z jiných důvodů. V takových případech dochází k vyhlašování planých poplachů a tento systém se stává nespolehlivým. Je tedy nezbytné již v přípravné fázi projektu zahrnout a zvážit všechny aspekty, které mohou ovlivnit funkci bezpečnostního systému.

„Detektory narušení by měly být odolné vůči planým a falešným poplachům. Za planý poplach se považuje každý poplach, který detektor vyhlásí na základě vyhodnocení změn v prostředí střeženého prostoru a nevznikne vlivem přítomnosti nebo pohybu narušitele. Kvalita detektoru narušení je určena jeho odolností vůči planým poplachům. Je přijatelné, vyhlásí-li detektor max. 1 planý poplach týdně. Falešný poplach naopak vzniká na základě technické nespolehlivosti obvodů detektoru. Přijatelnou hodnotou je 1 poplach za 2 roky.“ [11]

1.4 ACS – přístupový systém

Přístupový systém – ACS, lze „chápat jako soubor opatření k zajištění řízení a evidence přístupu do zabezpečeného objektu nebo prostor na základě jednoznačně přidělených přístupových práv.“ [11]



Obr. 5. Obecné schéma přístupového systému. [12]

Hlavní funkce přístupového systému:

- Zavedení definice snímač (kontrolované místo vstupu) a zóna (množina snímačů definující vstupy do určité oblasti).
- Definování množiny ID karet i s případným organizačním rozdělením.
- Definování práv jednotlivých ID karet pro vstup do zóny.
- Kontrola násobných vstupů – antipassback (APB).
- Zpřístupnění aktuálních stavů systému (kde se která ID karta nebo osoba nachází, stav zařízení, signalizace alarmových stavů) pomocí monitorovacích úloh.
- Definice a vyhodnocení nátlakových kódů.
- Funkce sledování překročení doby nutné k zavření dveří.
- Kontrola otevření dveří jiným způsobem, než ID kartou.
- Definice různých úrovní alarmových stavů systému (zejména z hlediska jejich vyhodnocování a potvrzování).

Vhodnou kombinací uvedených opatření je dosaženo maximální účinnosti systému. Princip fungování přístupového systému je takový, že každému uživateli jsou na základě personální politiky podniku přidělena přístupová práva, dle stupně oprávnění či časového harmonogramu.

Jednoduše lze popsat funkci: „Kdo, kdy a kam má povolený vstup?“

Tohoto lze dosáhnout při splnění několika podmínek. Je to zejména možnost jednoznačné identifikace uživatele, vytvoření místa přístupu a definice přístupových práv uživatelů.

Identifikace uživatele

Jednoznačná identifikace uživatele je zajištěna zejména přidělením ID prvku. Mezi ID prvky můžeme zařadit:

- kódové zámky
- kontaktní a bezkontaktní čipy (id karty)
- magnetické karty
- čárové kódy, kruhové kódy
- bluetooth identifikace
- biometrické prvky

Identifikace může proběhnout v zásadě třemi způsoby:

- heslo, PIN, kontrolní otázka,…, něco, co subjekt zná
- karta, čip, ovladač,…, něco, co má subjekt u sebe
- biometrie (papilární linie, oční duhovka, hlas,…), něco, co má fyzicky pouze subjekt [13]

Proces identifikace probíhá v několika logických krocích:

1. Zadání vstupní informace ze strany subjektu přes **snímací zařízení.**
2. Porovnání vstupních informací s databází ACS (ověření identity subjektu).
3. Ověření přístupových práv subjektu (v prostoru, v čase,…).
4. Povolení vstupu.

Identifikaci lze podle požadavků na zabezpečení rozdělit do čtyř tříd (Tab. 4).

Tab. 4. Třídy identifikace. [11]

Třída klasifikace	Identifikace na základě	Příklad identifikačního média/kombinační bezpečnost
0	není přímá identifikace	Tlačítko, kontakt, detektor pohybu (prostý požadavek pohybu).
		Pro vstup se předpokládá namátková kontrola dokladu nebo pověření fyzickou osobou (ostraha).
1	dat uložených v paměti	Heslo, číslo zaměstnance.
		Poměr počtu uživatelů k počtu všech kombinací kódů musí být alespoň 1:1000. Min. počet kombinací 10 000.
2	identifikačních prvků nebo biometrie	ID karta, přívěšek, čip, otisk prstu, oční duhovka, 3D model obličeje.
		Min. 1 mil. kombinací, jednoznačná identita uživatele, chybovost max. 0,01%. Identifikační číslo prvku nesmí být přímo zobrazeno.
3	kombinace třídy 1 a 2	Jednoznačný token/otisk prstu + heslo.
		Alespoň kombinace tříd 1 a 2.

Přístupový bod

je významnou součástí přístupového systému, a díky identifikačnímu procesu, který zde probíhá, odlišuje ACS od ostatních bezpečnostních systémů. Přes přístupový bod totiž dochází ke kontrolovanému prostupu do chráněných oblastí. Prvky tvořící přístupový bod jsou v zásadě tyto:

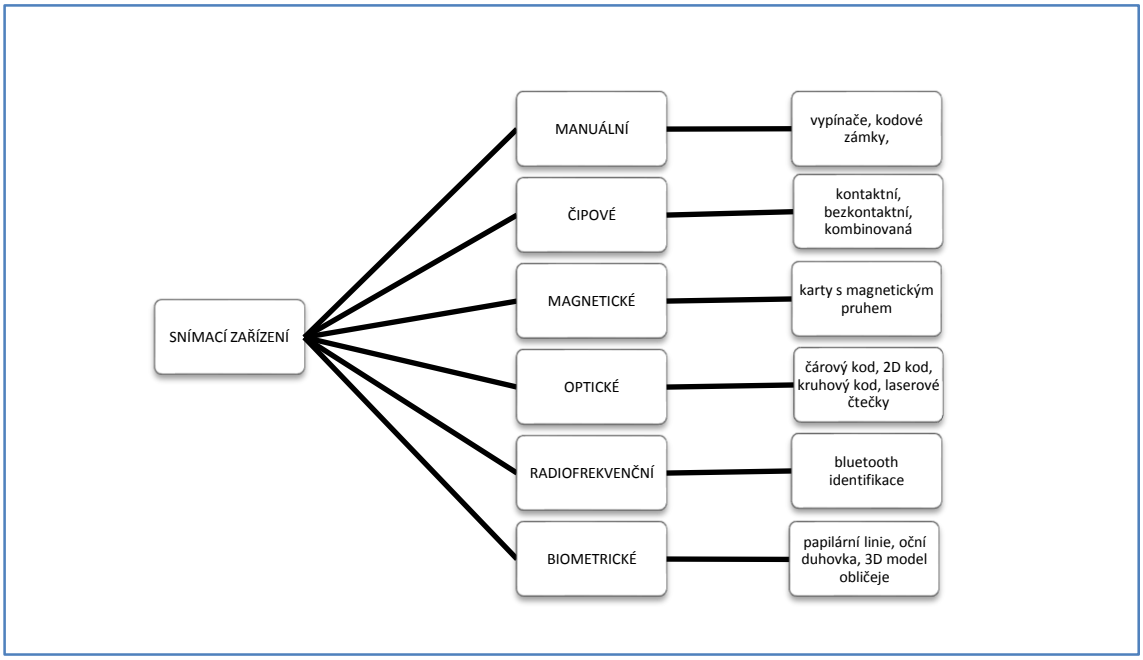
- místo přístupu (dveře, brána, turniket,…)
- rozhraní místa přístupu – ovládá otevření nebo zabezpečení místa přístupu (kontroler)
- snímače místa přístupu, slouží k identifikaci (čtečka, klávesnice,…)
- APAS – ovládací prvky a senzory přístupového místa

Podle způsobu a místa vyhodnocení vstupních informací lze snímací zařízení rozdělit na tři kategorie:

- **Základní (neinteligentní)** – tato čtečka umí „pouze“ přečíst číslo identifikátoru a popř. zadat PIN kód. Zjištěné údaje poskytuje dále řídící jednotce, která provede porovnání a ověření subjektu.
- **Polointeligentní** – dokážou ovládat všechny vstupy a výstupy místa prostupu. Vlastní rozhodnutí o vstupu subjektu provádí řídící jednotka.
- **Inteligentní** – stejně jako předchozí snímač, dokáží ovládat vstupy a výstupy a zároveň je v jejich paměti uložena databáze přístupových údajů a definice práv vstupu. Rozhodují samostatně a nezávisle. Řídící jednotka pouze aktualizuje údaje v zařízení. [11]

1.4.1 Obecný popis ACS

Obecná struktura přístupového systému se skládá z **ovládacích** a **ovládaných prvků**. K ovládacím prvkům patří hlavní řídící jednotka (pokud to systém vyžaduje), napájení systému, komunikační síť (RS-485, LAN, proudová smyčka, bezdrátová komunikace), řídící a obslužné pracoviště a snímací zařízení. Tento prvek je primárně ve styku s uživatelem, který svým jednáním může zásadně ovlivnit činnost systému. Jedná se např. o čipové nebo magnetické karty, čárové kódy, biometrické prvky (Obr. 6).



Obr. 6. Rozdělení snímacích zařízení dle identifikačních prvků. [11] a [vlastní]

Mezi **ovládané prvky**, které slouží k odblokování, nebo otevření prostupu řadíme například:

- elektromagnety
- elektromagnetické otvírače
- elektromechanické/elektromotorické zámky
- elektromotorické/elektrohydraulické otvírače
- motory
- přídržné elektromagnety
- vstupně/výstupní moduly

1.4.2 Topologie systému

Autonomní systém umožňuje provozovat nejjednodušší způsob ACS. Čtecí moduly nejsou připojeny na sběrnici. Je vhodný zejména do nejmenších firem nebo do bytových domů, ve kterých není nutná častá aktualizace údajů. Programování přístupových oprávnění se provádí přímo na přístupovém bodu systému. [14]

Druhou variantou jsou **modulární systémy,** které se využívají u rozsáhlejších systémů. Jsou tvořeny větším počtem přístupových míst, řídícími jednotkami spolu s řídícím pracovištěm. Centrálním prvkem systému je ústředna, ve které probíhá ověření a rozhodnutí o přístupu. V modulárních systémech se nejčastěji využívá sběrnicové nebo hvězdicové topologie.

1.4.3 Vliv lidského činitele na činnost ACS

Lidský činitel ovlivňuje ACS zásadním způsobem. Jeho prostřednictvím je řízen přístup uživatelů do objektu. V závislosti na nastavení systému a volbě vhodných komponentů můžeme dosáhnout téměř dokonalé nepropustnosti objektu. Pokud ovšem nebudou jednotlivé prvky dokonale sladěny, může se do objektu dostat v podstatě kdokoli.

Vzhledem ke skutečnosti, že v ACS hraje hlavní roli uživatel (např. zaměstnanec), je v tomto systému mnoho prostoru pro jeho jednání, které je z hlediska zabezpečení nepřípustné a nebezpečné. Nabízí se zde několik pohledů na daný problém.

Jako první bych uvedl pohled ze strany správce systému. V jeho zájmu, respektive v zájmu jeho zaměstnavatele je, aby ACS plnil dokonale svoji funkci. K tomu je nutné splnit několik zásadních požadavků. Jsou to zejména:

- Ve spolupráci s personálním oddělením (administrátorem) vést a pravidelně aktualizovat seznamy zaměstnanců.

- Aktualizace je důležitá zejména při propuštění zaměstnance (vrácení ID prvků, vymazání ze systému).
- Evidence a blokace ztracených ID prvků.
- V případě ovládání místa přístupu pomocí GSM brány, autorizovat každé telefonní číslo. Nevpustit do systému číslo cizí.

Je zde také pohled ze strany zaměstnance, který ACS využívá. Jedná se například o:

- Prostup místem přístupu více jak jednoho subjektu najednou za použití jediného ID prvku.
- Poskytnutí ID prvku i s potřebnými údaji druhé osobě (úmyslně i neúmyslně).
- Uživatel při prostupu nevyčká na dokonalé uzavření místa prostupu (pokud není toto prováděno fyzickou ostrahou)
- Uživatel provede úmyslně úpravu na ovládaném zařízení, která znemožní jeho funkci. Průchod je pak možný i bez použití ID prvku.

Výše uvedené příklady jednání jsou pouze jedny z mnoha možných variant, kterými mohou zaměstnanci zkoušet oklamat ACS.

1.5 CCTV kamerové systémy

V současnosti zaznamenávají kamerové systémy rozvoj, který je způsobený zejména dynamickým vývojem v oblasti informačních a komunikačních technologií, audiovizuální technologie, ale i ve filmovém a herním průmyslu.

Původně byl kamerový systém určený na identifikaci, rekognoskaci a detekci osob. Dnešní sofistikované systémy umožňují daleko širší použití například na detekci podezřelého jednání, při biometrické verifikaci, sledování osob, sledování tělesné teploty osob, nebo při řešení dopravní situace.

Zařazení systému CCTV a jeho komponentů do bezpečnostní struktury je prováděno na základě vyhodnocení míry rizika a podle požadovaného stupně zabezpečení.

Podle zařazení systému CCTV do některé z úrovní rizika jsou na něj kladeny různé nároky a požadavky. Jsou to např.:

- ukládání dat (rychlost reprodukce záznamu po incidentu,…)
- archivace a zálohování dat
- záznam událostí (poplach, řízení funkcí kamery, tisk,…)

- monitorování přepojení (čas oznámení poruchy operátorovi, ověřování spojení,…)
- detekce sabotáže (úmyslné zatemnění, změna pozice kamery,…)
- identifikace dat (lokalita, zdroj obrazu, datum, čas,…) [15]

1.5.1 Základní komponenty CCTV systému

Mezi základní komponenty systému CCTV patří:

- zařízení na snímání obrazu - kamera
- příslušenství kamery
- přenosová soustava
- zařízení na zpracování videosignálu
- zařízení na zpracování a záznam obrazu

1.5.2 Digitální systémy – IP kamery

Novým trendem v kamerových systémech je využití IP kamer. Původní CCTV systém pracuje s analogovým signálem. Tento systém využívá přenosový standart CCIR[1], jehož rozlišovací schopnost je cca 440 000 pixelů. Naproti tomu umožňují digitální systémy přenos digitálního signálu při využití kompresních algoritmů. Za pomocí těchto algoritmů jsou z obrazu odstraněny redundantní a irelevantní informace, které by v opačném případě neúměrně zatěžovaly přenosový systém. Nejznámější kompresní algoritmy jsou MPEG-2, H.263 a Wavelet. Základní prvky digitálního systému CCTV jsou **IP kamery, IP videoservery, IP dekodéry, IP záznamová zařízení.**

Princip snímání IP kamery je shodný s analogovou kamerou (pomocí CCD nebo CMOS senzoru). Rozdíl je ve zpracování získaných dat. Tato data jsou digitalizována a příslušným algoritmem kompresována, před vlastní vysláním do sítě.

[1] CCIR - Evropský standard pro televizní signál -625 řádků, 50 půlsnímků/s (z fr. Comite Consultatif International des Radiocommunications)

Síťové propojení IP kamery s ostatními prvky využívá tzv. **skupinové adresování,** které umožňuje uživateli sledovat, popř. řídit zařízení na několika přijímačích současně (PC, tablet, smartphone).

Jednou z hlavních výhod přenosu digitálních dat je prakticky nulová degradace digitálního signálu v přenosových systémech.

1.5.3 Vliv lidského činitele na funkci systému CCTV

Možnost ovlivnění činnosti CCTV ze strany uživatele (zaměstnance) není nijak zásadní. Kamerový systém je spouštěn většinou automaticky a při pokusu o manipulaci s vlastní kamerou je vyhlašován sabotážní poplach.

Negativní vliv se může projevit při nesprávném nastavení kamery ze strany obsluhy. Jedná se například o nevhodné umístění kamery (protisvětlo, překážky ve výhledu, nepodstatná oblast snímání,…). Problém při provozování CCTV nastává, pokud není systém používán dle zákona č. 101/2000 Sb. o ochraně osobních údajů (sledování osob, zneužití záznamu z kamery,…)

Tab. 5. Vliv chování zaměstnance na funkci zabezpečovacích systémů. [vlastní]

Bezpečnostní systém	**Zařízení**	**Událost**	**Možný následek**
PZTS	Zadávací klávesnice.	Odkrytá manipulace.	Vyzrazení PIN kódu neoprávněné osobě.
		Neprovedení aktivace PZTS.	Objekt zůstává nezastřežen.
	Tísňové tlačítko.	Zneužití úmyslné/neúmyslné.	Marný poplach.
		Tlačítko není použito.	Poškození zdraví, nebo majetku.
EPS	Tísňový hlásič.	Zneužití úmyslné/ neúmyslné.	Marný poplach.

		Tlačítko není použito.	Poškození zdraví, nebo majetku.
ACS	Identifikační zařízení.	Použití jednoho ID prvku k průchodu více osob.	Neoprávněné vniknutí cizí osoby.
			Pokus o oklamání docházkového systému.
		Použití více ID prvků jednou osobou.	Pokus o oklamání docházkového systému.
		Odcizení, ztráta ID prvku.	Neoprávněné vniknutí cizí osoby.
	Přístupové body.	Blokace přístupového místa-znemožnění uzavření.	Pokus o oklamání docházkového systému. Neoprávněné vniknutí cizí osoby.
CCTV	Kamera.	Zakrytí kamery, otočení kamery	Pokus o znemožnění sledování chráněného prostoru.
	Záznamové zařízení.	Neoprávněné sledování osob.	Porušení zákona č. 101/2000 Sb.
	Monitor.	Neoprávněné sledování osob.	Porušení zákona č. 101/2000 Sb.

2 INTEGROVANÉ POPLACHOVÉ SYSTÉMY

Integrované poplachové systémy (IPS) jsou dle Valoucha [1] „definovány jako systémy mající jedno nebo více společných zařízení, alespoň jedním, z nichž je poplachová aplikace."

„Integrace poplachových systému představuje moderní způsob využití současných technologických možností prvků zabezpečovacích, kamerových, přístupových, tísňových systémů a systémů přivolání pomoci. Uvedené aplikace je možno integrovat navzájem nebo doplnit o systémy nepoplachové a tím zabezpečit efektivní aplikaci automatizačních procesů v rezidenčních, komerčních i průmyslových objektech." [1]

Mezi nepoplachové aplikace řadíme:

- osvětlení, vytápění
- klimatizace, ventilace
- zavlažování, vysoušení
- správa budov, řízení energetických systémů
- dopravní aplikace
- zemědělské aplikace (např. automatizované krmení) atd.

K rozvoji integrovaných systémů dochází z několika důvodů. Mezi hlavní důvody můžeme zařadit **zvýšení bezpečnosti**. Zde vycházíme z jednoduchého pravidla „Více očí, více vidí". V praxi jde většinou o kombinaci poplachových systémů EPS, CCTV, PZTS a ACS, s jejichž pomocí lze při jejich správném nastavení reagovat téměř okamžitě na vzniklé hrozby.

Dalším z důvodů zvyšující se poptávky po integrovaných systémech je **komfort ovládání a řízení.** Tyto systémy se využívají zejména v rezidenčních sídlech. Jako příklad můžeme uvést ovládání dveřních zámků, žaluzií, osvětlení, zavlažování, přívodů elektřiny, atd.

Nemůžeme opomenout také **ekonomické důvody** a s tím spojenou snahu o redukci spotřeby energie. V současné době lze systém například naprogramovat tak, že po odchodu z objektu a zapnutí zabezpečovacího systému dojde automaticky k vypnutí všech světel a sníží se teplota na předem definovanou hodnotu.

Při popisu důvodů, proč dochází k integraci zabezpečovacích systémů, jsem vycházel spíše z výhod, které systém nabízí. K objektivnímu posouzení je nutno uvést i některé nevýhody integrace.

2.1 IPS z pohledu spolehlivosti

Spolehlivost

Spolehlivost můžeme vyjádřit jako pravděpodobnost bezporuchového provozu, což je pravděpodobnost, že objekt může plnit požadovanou funkci v daných podmínkách a v daném časovém intervalu. Spolehlivost integrovaných poplachových systémů je závislá na následujících faktorech:

- jakost výrobku
- správný návrh systému
- kvalita zpracování projektové dokumentace
- kvalita provedení instalace
- způsob nastavení vzájemných vazeb v systému
- vlivy okolního prostředí
- správný způsob obsluhy
- údržba systému
- servis [1]

Spolehlivost systému je jedním ze základních požadavků. Žádný zákazník nepřijme integrovaný bezpečnostní systém, který sice „ovládá“ dům, ale zároveň vyžaduje servisní zásah několikrát do měsíce.

Jak bylo popsáno výše, jsou IPS velmi komplikované a sofistikované systémy. Jsou složeny z mnoha elektronických i mechanických součástí, které neustále ovlivňují vnitřní i vnější vlivy, včetně člověka jako uživatele.

Jeden z důvodů snížení spolehlivosti IPS je právě vyšší počet zařízení v systému. Jedná se o integraci bezpečnostních systémů (např. PZTS, EPS, ACS a CCTV) a nepoplachových aplikací jako zavlažování, topení a řízení energetických systémů. V celém systému je zařazeno mnoho komponentů. Každý komponent vykazuje nějakou chybovost, a zvyšováním jejich počtu v systému se zvyšuje i pravděpodobnost selhání.

Dalším z důvodů selhání integrovaného poplachového systému je integrace zařízení od různých výrobců. Toto hledisko lze rozdělit na dva úhly pohledu. Za prvé je to kombinace zařízení rozdílných generací. Pokud vztáhneme problematiku na ČR, můžeme říci, že jsou v některých objektech poplachové systémy více než 20 let staré. Proto se z hlediska spolehlivosti jeví kombinace těchto starších systémů se zařízeními několik generací modernějšími

jako problematická. Existuje samozřejmě možnost, že výrobce pokračuje ve vývoji nových systémů a garantuje uživateli při splnění určitých podmínek rozšíření systému. Většinou se jedná o doplnění dalších zařízení jako převaděčů, adaptérů a redukcí, které mají za úkol propojit staré s novým.

Druhý úhel pohledu je použití systémů stejné generace, avšak odlišných výrobců. Na trhu je skupina výrobců, kteří vyvíjí svá zařízení tak, aby byla kompatibilní s ostatními systémy, a ta druhá, která kompatibilní nejsou. Na základě toho vzniká problém jak jednotlivé subsystémy integrovat. Opět je zapotřebí doplnit další zařízení a nadstavby, které integraci pomohou. V této chvíli se můžeme odvolat na předchozí odstavec, který hovoří o spolehlivosti v souvislosti s počtem zařízení v systému.

Značný vliv na spolehlivost IPS má centralizace řízení systému. Je nutné si uvědomit, že v případě selhání centrální řídící jednotky z důvodu přerušené komunikace, dodávky elektrické energie nebo výpadku SQL serveru je funkce systému a tím i bezpečnost objektu ohrožena. Při projektování uvažujeme o záložním zdroji a využití autonomních koncových zařízení v největší možné míře (např. inteligentní čtečky).

3 TRENDY V IPS

V této kapitole se pokusím nastínit směr vývoje v oblasti IPS. Každým rokem je pořádáno několik veletrhů a výstav na téma bezpečnostních technologií. Níže je popsáno několik možných trendů pro nejbližší období.

3.1 Trendy ACS

V přístupových systémech je snaha do budoucna využívat autonomní plně inteligentní snímače (čtečky), které budou schopny samy vyhodnocovat a ovládat přístupové body. Tento krok má za následek zjednodušení architektury ACS, kdy samotné čtečky budou připojeny k terminálovému serveru kvůli aktualizaci dat v definovaných intervalech.

Na úrovni samotných snímačů vývoj směřuje k duálním čtečkám, které kombinují RFID snímač ID karet s biometrickým snímačem. V současné době je vcelku běžné využití snímače papilárních linií prstu ruky. Jedná se o cenově přístupnou metodu ověřování. Jeden z problémů biometrie je uchování a ochrana biometrických dat. Jedná se o citlivé údaje, které je potřeba zabezpečit před zneužitím. Zajímavé řešení nabízí například biometrická čtečka otisků prstů 4G V-Flex™ iClass® (výrobce Safran Morpho), která vyčítá vzory otisků přímo z ID karty. Kapacita systému je v podstatě neomezená a citlivá data jsou uložena na ID kartě. Další možností je využití snímače oční duhovky a sítnice. Zde narážíme při snaze o větší uplatnění zejména na pořizovací cenu systému a způsob snímání dat. Infračervený paprsek sejme data ze vzdálenosti zhruba dva centimetry od oka, což mnohým uživatelům není příjemné. Na druhou stranu je v duhovce uloženo zhruba 260 identifikačních znaků a přesnost identifikace se uvádí v poměru 1 : 6 milionům (například u verifikace otisků prstů je to cca 1 : 1 milionu). Ostatní biometrické údaje, jako je geometrie ruky, dynamika stisku kláves či charakteristika hlasu, nelze zatím využít v masovém měřítku, vzhledem k jejich nízké přesnosti porovnání. [16]

3.2 Drony jako fyzická ostraha objektů

V posledních několika letech zažívají drony nebývalého rozmachu. Původně byly jako většina moderních technologií využívány především v armádě, ale s postupem doby se dostaly i do veřejného sektoru. Jejich komerční využití v oblasti prevence kriminality chce zahájit japonská bezpečnostní agentura, která plánuje nasazení dronů ke sledování podezřelých vozidel a osob v průmyslových a obchodních areálech či jiných objektech většího rozsahu.

V souvislosti s jejich provozem je však potřeba nejdříve legislativně vymezit jakým způsobem, a za jakých podmínek mohou být použity.

Praktické použití dronu může být následující. Pokud je v místě aplikace detekován poplachovým systémem pohyb mimo dosah fixních a PTZ kamer, dron se automaticky přiblíží k místu spuštění poplachu a pořídí snímky i s videozáznamem podezřelého objektu, které v reálném čase odešle do dohledového centra. V případě zjištění přítomnosti vozidla ve střeženém prostoru se dron zaměří na záznam poznávací značky vozu, u osob se dron pokusí zaznamenat jejich obličeje. [17]

Obr. 7. Dron- bezpilotní letoun. [17]

3.3 Video dohledové systémy

V oblasti video dohledových systémů se přepokládá rozšíření IP kamer v oblasti podnikových bezpečnostních systémů u malých a středně velkých organizací. Pozornost uživatel se obrací k využití cloudového uložiště[2], které nabývá na významu zejména díky své jednoduchosti, snadné instalaci a správě.

„Zvyšuje se postupně popularita širokoúhlých fish-eye kamer na úkor PTZ kamer[3]. Multisenzorové panoramatické kamery s širokým úhlem záběru jsou schopny pokrýt velký prostor ve vysokém rozlišení. Došlo k odstranění problémů s kvalitou obrazu, jako tomu bylo u prvních modelů tohoto typu kamer. Nová technologie s sebou přinesla snížení výrobních nákladů. Odborníci na bezpečnost si proto pomalu začínají uvědomovat schopnosti těchto kamer odstranit nedostatky PTZ kamer, zejména jejich „nešťastné“ tendence být natočen v jiném směru než je právě potřeba. Očekává se plynulý přechod na 4K rozlišení, zejména v momentě, kdy dojde ke snížení ceny a zvýšení dostupnosti pro většinu běžných uživatelů. Ke zvyšování rozlišení již nebude tak často docházet, spíše se očekává vývoj v oblasti zpracování a komprese videa (Tom Cook, viceprezident prodeje pro Severní Ameriku, Samsung).“ [18]

Kvůli teroristickým hrozbám dochází k preventivním bezpečnostním opatřením v rámci video dohledu nad objekty kritické infrastruktury, vládními a vojenskými objekty a včetně dopravních aplikací a ochrany státních hranic. Trend v oblasti IP kamer směřuje k vysokému rozlišení multisenzorových panoramatických kamer. [18]

---

[2] „Cloud (také cloud computing /cloud hosting) je způsob poskytnutí výpočetního výkonu a funkcí coby služby, nikoliv produktu, pomocí sítě (nejčastěji přímo pomocí internetu). Cloud obvykle poskytuje výpočetní výkon, aplikace, přístup k datům a jejich management, případně i ukládání a zálohování dat.“ [19]

[3] PZT kamera- PTZ (angl. pan–tilt–zoom) je zkratka pro otáčení, naklánění a zoom, a odráží možnosti dálkového ovládání kamery.

II. PRAKTICKÁ ČÁST

4 DEFINICE PROBLÉMU S AKTIVACÍ PZTS ZE STRANY ZAMĚSTNANCE

V následující podkapitole je uveden konkrétní příklad integrace poplachových systémů. V našem případě se jedná o firmu střední velikosti, která se zabývá elektrotechnickou výrobou. Pro zajištění bezpečnosti využívá PZTS a ACS (Access) s nadstavbou docházkového systému (Passport).

Ve firmě pracuje 96 zaměstnanců, jejichž pracovní doba je stanovena vnitřním předpisem jako pružná. Není proto možné využít automatického způsobu aktivace a deaktivace zastřežení s časovým parametrem.

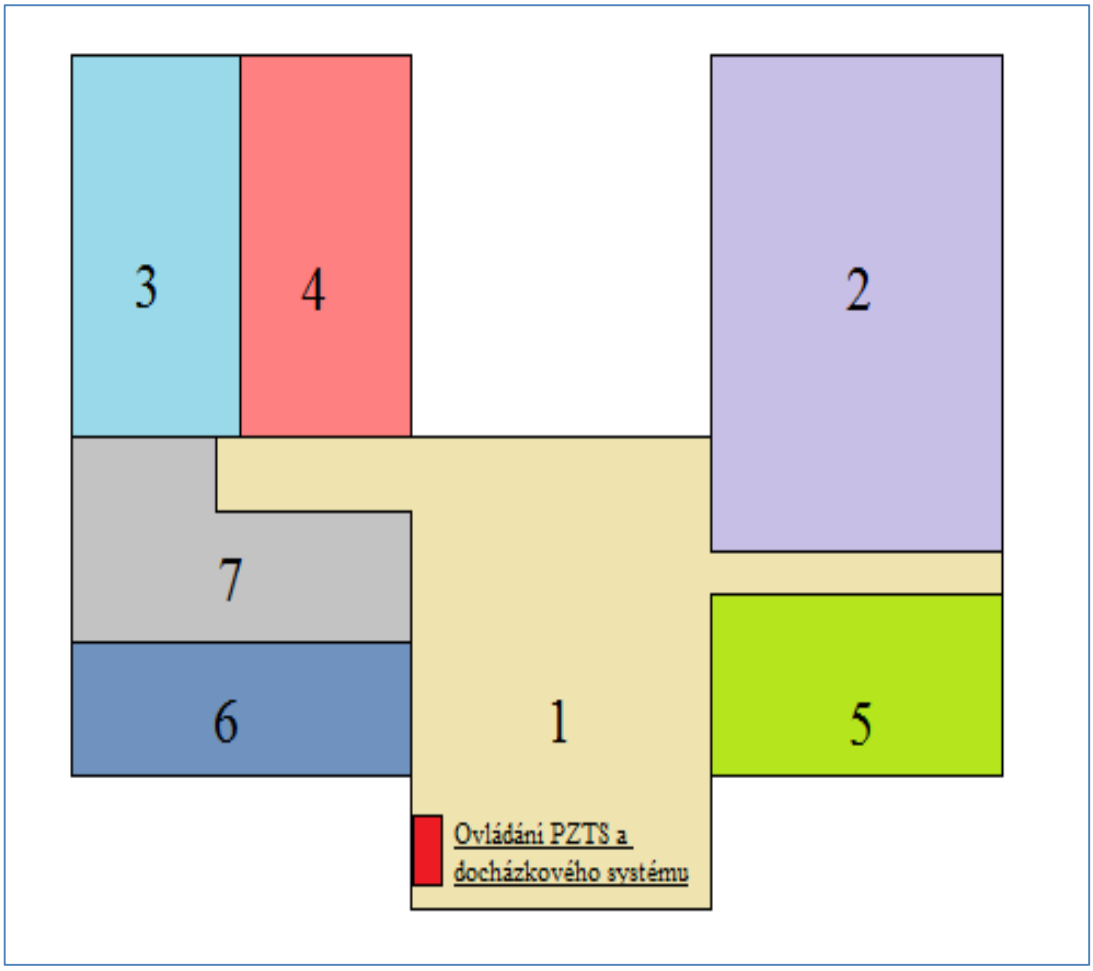
4.1 Realizovaný IPS firmy

Povinností každého zaměstnance je při příchodu do zaměstnání zaznamenat svůj příchod do docházkového systému pomocí ID karty, kterou získá v přijímacím řízení do zaměstnání. Pokud přijde na pracoviště první, musí také deaktivovat PZS pomocí přiděleného PIN kódu. Opačný postup provádí zaměstnanec při odchodu ze zaměstnání. V této chvíli by se měl přesvědčit o tom, že je skutečně poslední, kdo firmu opouští a je tedy jeho povinností aktivovat zastřežení objektu.

Technické řešení PZTS firmy je provedeno následovně. Areál firmy tvoří několik objektů, ve kterých jsou umístěna jednotlivá oddělení (Obr. 8). Podle těchto oddělení je rozdělen systém střežení do sedmi zón (Tab. 6). Systém je řízen centrální ústřednou, která je napojena na PCO.

Tab. 6. Rozdělení areálu firmy do střežených zón. [vlastní]

Budova A	zóna 1 zóna 5 zóna 6 zóna 7	společné prostory účtárna obchodní oddělení vedení firmy
Budova B	zóna 3 zóna 4	dílny vývojové centrum
Budova C	zóna 2	sklad



Obr. 8. Rozdělení areálu firmy na jednotlivé zóny zabezpečení. [vlastní]

V každé zóně jsou podle potřeby umístěny pohybové PIR detektory, které jsou k centrální ústředně připojeny přes koncentrátory.

Jako doplnění plášťové ochrana objektů jsou využity detektory tříštění skla.

Poplachový tísňový systém resp. EPS je realizován pomocí tlačítkových hlásičů požáru, které jsou umístěny na klíčových místech firemního areálu.

Pohyb zaměstnanců a ostatních uživatelů po firmě je řízen ACS. Samotný objekt je rozdělen do několika sekcí, ve kterých jsou definována práva a podmínky ke vstupu. K identifikaci uživatele slouží opět ID karta.

Obr. 9. Univerzální snímací hlava. [20]

Obr. 9 zobrazuje snímací hlavy určené pro použití bezkontaktních ID karet. Tyto „čtečky“ mohou pracovat na kmitočtu 13,56 MHz resp. 125 kHz. Pro komunikaci využívá např. protokol WIEGAND. Čtení karet probíhá na vzdálenost 5-10 cm.

Snímací hlavy představují jednu z možností identifikace uživatele. Většinou jsou v jednoduchém provedení (čtečka vlevo), které pomocí LED indikátorů zobrazuje stav přístupového bodu – červená LED zamčeno, zelená LED odemčeno. Čtečka vpravo je kombinována s numerickou klávesnicí, která umožňuje zadání číselného kódu. Tento krok doplňuje vlastní identifikaci o autentizaci uživatele.

Dalším komunikačním prvkem mezi uživatelem a ACS může být multiaplikační identifikační terminál, který umožňuje uživateli získat mnohem více informací (Obr. 10).

Tento terminál disponuje grafickým barevným displejem 7,0 “ , 800 x 480 bodů s dotykovým panelem. Díky jeho technickým vlastnostem je možné ovládat několik systémů a aplikací.

Obr. 10. Multiaplikační identifikační terminál. [21]

Jedná se například o EZS, EPS, řízení zámků, turniketů, zobrazovačů a tiskáren.

Základní parametry terminálu:

- Komunikační rozhraní (Ethernet, USB, RS485, Wiegand).
- Rozsah vnitřní paměti dovoluje pracovat s desítkami tisíc identifikačních prvků (karty, tagy, čárové kódy).
- Integrovaný univerzální RFID snímač (125 kHz nebo 13,56 MHz), podporující desítky typů RFID čipů.
- Možnost integrace vysoce výkonného vícesměrového snímače čárového kódu.
- Možnost rozšíření až do 16 vstupních signálů s galvanickým oddělením.
- Možnost rozšíření až do 16 bezpotenciálových výstupů.
- PoE (Power Over Ethernet). [21]

SQL databáze

Nedílnou součástí systému ACS je SQL databázový stroj. Zde popisovaný systém vychází plně z architektury klient/server. Jako SQL servery jsou podporovány MS SQL Server (verze 2008 až 7.0) včetně MS SQL 2005 EXPRESS, Oracle a Informix. U modulů komunikací se snímači ID karet je volitelné i prostředí UNIX, LINUX. [22]

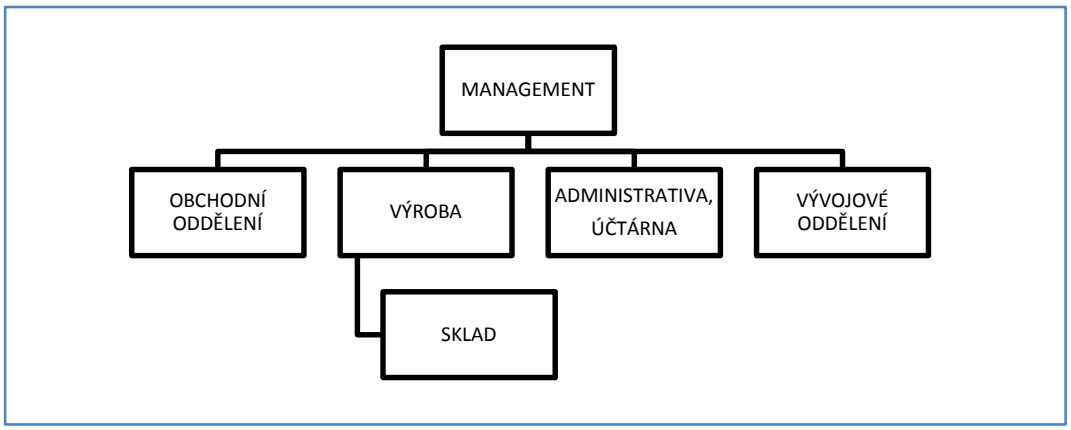
„Model klient-server je forma distribuovaného zpracování výpočetního výkonu mezi koncovým zařízením (klientem) a serverem, kteří mezi sebou komunikují a předávají si vzájemně data. **Klient** překládá uživatelův požadavek tak, aby byl srozumitelný **serveru**, čeká od něj odpověď, kterou překládá zpět tak, aby byla srozumitelná **klientovi**, který ji na obrazovce prezentuje uživateli. V architektuře klient-server tedy server zpracovává dotazy v databázi a klient je prezentuje, zajišťuje aplikační logiku a zprostředkovává rozhraní pro uživatele.“ [23]

Vstup a vjezd do areálu

Vstup a vjezd do areálu firmy je zabezpečen bránou a závorou, kterou lze ovládat několika způsoby. Je to:

- GSM brána (telefonní číslo získá zaměstnanec).
- ID karta zaměstnance.
- Dálkové ovládání z recepce na výzvu (určeno pro návštěvy).

Výše uvedené systémy zabezpečení jsou integrovány společně s CCTV systémem. Část CCTV kamer je rozmístěna z důvodu ochrany perimetru vně objektu. Zbytek kamer je instalován převážně ve výrobní části firmy a ve vývojovém centru. Struktura firmy je naznačena níže.



Obr. 11. Struktura firmy. [vlastní]

4.2 Popis konkrétního problému v zabezpečení firmy

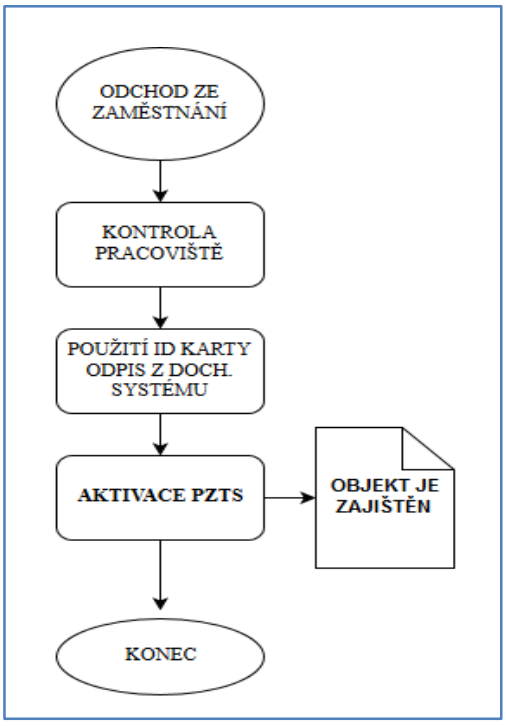
V následující části je popsána problémová situace, se kterou jsem se setkal v praxi. Tato situace, dle mého názoru, zásadně ovlivňuje funkci PZTS ve firmě.

4.2.1 Aktivace PZTS zaměstnancem při odchodu z pracoviště

Problém aktivace zastřežení vychází z praxe při užívání PZTS. Jako aktéři zde vystupují na jedné straně vlastníci firmy, kteří mají zájem o zabezpečení svého majetku, a na straně druhé zaměstnanec. Povinností každého zaměstnance, kterému bylo uděleno právo vstupu do střežené zóny (PIN kód), je systém při vstupu deaktivovat a při odchodu aktivovat. Samozřejmostí by mělo být, že svěřené kódy a ostatní identifikační prostředky uchová v tajnosti pouze pro vlastní potřebu.

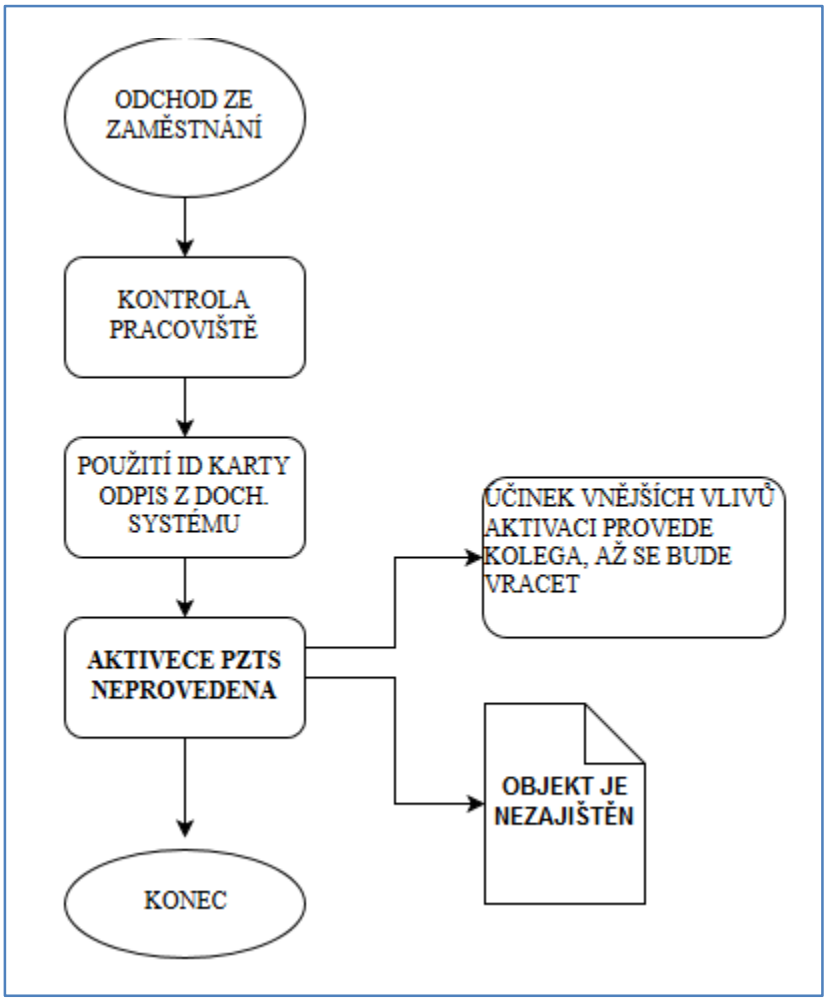
Varianty postupů zaměstnance při odchodu ze zaměstnání.

1. SPRÁVNÝ POSTUP. Zaměstnanec před odchodem ze zaměstnání zkontroluje pracoviště dle vnitřního řádu firmy, a přesvědčí se, že je opravdu poslední, kdo danou zónu opouští. ODEPÍŠE SE pomocí docházkového systému, AKTIVUJE (zastřeží) svoji zónu a opouští pracoviště (Obr. 12).



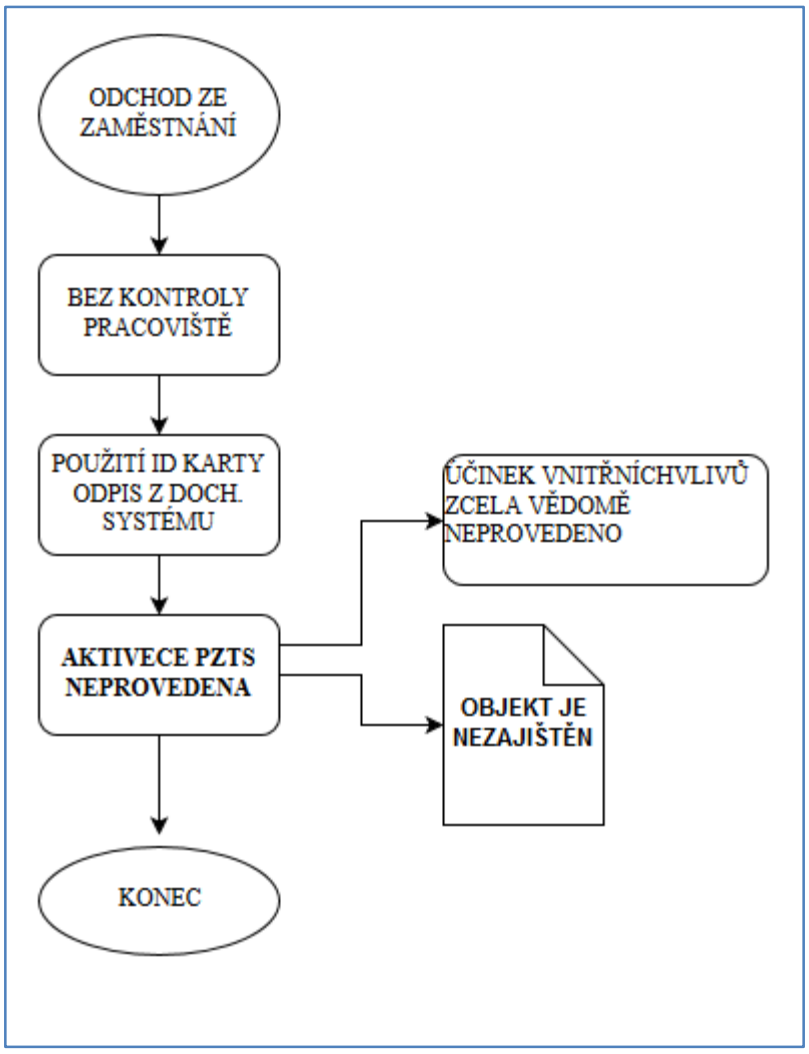
Obr. 12. Správný postup zaměstnance při odchodu ze zaměstnání. [vlastní]

2. NESPRÁVNÝ POSTUP I. Zaměstnanec před odchodem ze zaměstnání zkontroluje pracoviště dle vnitřního řádu firmy, a přesvědčí se, že je opravdu poslední, kdo danou zónu opouští. ODEPÍŠE SE z docházkového systému.
   Kolega, který odchází zároveň s ním, ho požádá, aby systém neaktivoval, protože se bude během 15 minut vracet, a sám pak systém aktivuje. Kolega se bohužel z nějakého důvodu nevrátí, a **objekt zůstává nezajištěn.** Možných kombinací tohoto jednání je více (Obr. 13).



Obr. 13. Nesprávný postup I. zaměstnance při odchodu ze zaměstnání. [vlastní]

3. NESPRÁVNÝ POSTUP II. Zaměstnanec bez jakékoli kontroly odchází z pracoviště, ODEPÍŠE SE z docházkového systému. **Objekt zůstává nezajištěn** (Obr. 14).



Obr. 14. Nesprávný postup II. zaměstnance při odchodu ze zaměstnání. [vlastní]

Jednání zaměstnance uvedené v bodu 2 a 3 má zásadní vliv na zabezpečení firmy. Veškeré investice do pořízení a inovace PZTS přicházejí nazmar. V případě napadení objektu (krádeže, vloupání, …) čeká majitele složité jednání a vysvětlování s dotčenými organizacemi, jako je pojišťovna nebo policie ČR.

4.2.2 Definice problému

Zaměstnanec má k dispozici veškeré potřebné prostředky a znalosti k tomu, aby provedl aktivaci PZTS, avšak v některých případech bez objektivních příčin aktivaci PZTS při odchodu ze zaměstnání neprovede.

.

5 NÁVRH ŘEŠENÍ PROBLÉMU S AKTIVACÍ PZTS ZE STRANY ZAMĚSTNANCE

V předchozí kapitole byl definován problém s aktivací zastřežení jednotlivých zón v chráněném objektu. V tomto konkrétním případě je nutné, aby zastřežení aktivoval poslední zaměstnanec, který zónu opouští. Je to zejména z důvodu pružné pracovní doby většiny zaměstnanců. Příchody a odchody těchto zaměstnanců jsou v rozmezí dvou hodin. Mnozí zaměstnanci pracují nepravidelně, v různou denní dobu. Jedná se například o vývojové a servisní oddělení. Z těchto objektivních důvodů nelze zvolit automatické časové zastřežení objektu.

K aktivaci PZTS je potřeba ze strany zaměstnance splnit několik podmínek:

1. Znalost bezpečnostního kódu (PIN).
2. Ochota provést zabezpečení.
3. Povědomí o tom, že odchází ze zóny jako poslední.

Znalost bezpečnostního kódu se předpokládá. Zaměstnanec jej získal při nástupu do zaměstnání. Může dojít k situaci, kdy kód zapomene. V tom případě by měl kontaktovat svého nadřízeného, který zajistí zastřežení objektu.

Ochota provést zabezpečení. Z vnitřního předpisu firmy vyplývá provedení zabezpečení jako povinnost. Zaměstnanec je povinen zastřežení provést. Pokud tak neučiní bez objektivních příčin, jedná se o hrubé porušení pracovní kázně s následným postihem. Neprovedení aktivace PZTS může mít dva důvody. Z nedbalosti – neúmyslně, nebo úmyslně. V tomto případě se může jednat o napomáhání k trestnému činu, nebo přípravu trestného činu.

Povědomí o tom, že je v zóně poslední, je podmínka zřejmě nejsložitější. Vyžaduje totiž od zaměstnance aktivitu. V případě pracoviště, kde zónu zastřežení tvoří dvě kanceláře a chodba, je kontrola početního stavu otázka několika vteřin. Jiná situace nastává, když se jedná o rozlehlé výrobní haly s několika kancelářemi, sociálním zařízením atd. Zde se od zaměstnance očekává, že celý prostor osobně projde a zkontroluje. Tato činnost může zabrat i několik minut, a je nezbytné, aby se zaměstnanec osobně přesvědčil, že jeho kolega například pouze zapomněl zhasnout a vypnout rádio v kanceláři. Ode dveří tato situace vypadá, jako kdyby pokračoval v práci, a není proto nutné aktivovat PZTS. Ve skutečnosti už na pracovišti nikdo není, a objekt zůstane nezabezpečený celou noc.

Návrh řešení problému

Řešení problému spočívá v získání informace o aktuálním početním stavu zaměstnanců v jednotlivých zónách PZTS. Tyto informace můžeme získat pomocí softwarové úpravy docházkového systému. Každé ID kartě bude přiřazen nový atribut – číslo zóny PZTS. Dále je nutno vytvořit nástroj - počítadlo, do kterého se budou načítat příchody a odchody zaměstnanců z jednotlivých zón. Aplikace průběžně vyhodnocuje aktuální stav zaměstnanců v jednotlivých zónách. V případě, že vyhodnotí odchozího zaměstnance jako posledního (hodnota 0), vyšle příkaz řídící jednotce PZTS k zastřežení příslušné zóny. Přístup do objektu a deaktivace jeho zabezpečení je podmíněno zadáním PIN.

6 PRINCIP PRŮBĚŽNÉHO HODNOCENÍ POČETNÍHO STAVU ZAMĚSTNANCŮ VE FIRMĚ

V následující kapitole je podrobně popsán princip navrhovaného řešení. Jednotlivé podkapitoly se zabývají počítáním zaměstnanců a jejich rozdělení do příslušných zón PZTS.

6.1 Počítání zaměstnanců

Prvním krokem k řešení je výpočet aktuálního stavu zaměstnanců v jednotlivých zónách. K tomuto lze využít softwarově upravený docházkový systém (Tab. 8). Jeho součástí je databáze pracovníků a přidělených ID karet. Systém mj. ukládá údaje o příchodu a odchodu zaměstnance ze zaměstnání.

Předpoklad pro stanovení aktuálního počtu zaměstnanců.

- Každý zaměstnanec má u sebe ID kartu, která je jedinečná.
- Každý zaměstnanec je povinen zaznamenat v docházkovém systému příchod a odchod z pracoviště, tzn., MUSÍ ID kartu používat denně.

Princip počítání je takový, že při použití ID karty, je provedena akce příchod/odchod, která vyvolá změnu stavu (Tab. 7). Tyto hodnoty jsou průběžně zaznamenávány pro jednotlivé zóny, do kterých byli zaměstnanci zařazeni.

Tab. 7. Příklad IDACTION. [vlastní]

IDACTION	NAME	ENTER
0	Odchod	0
1	Příchod	1
2	odchod dovolená	0
3	příchod dovolená	1
4	odchod lékař	0
5	příchod lékař	1
6	ochod služ. cesta	0
7	příchod služ. cesta	1

Tab. 8. Příklad přidělení atributu – číslo zóny. [vlastní]

CRDNUM	ATRIBUT				
	jméno	přijmení	středisko	číslo zóny PZTS	pracovní zařazení

123456789	Radim	Svoboda	50	4	32
987654321	Helena	Malá	20	6	12

6.2 Rozdělení zaměstnanců

Celý systém je založený na povinnosti a nutnosti použití ID karty zaměstnance. Vycházíme z předpokladu, že každému zaměstnanci byla při nástupu do zaměstnání přidělena ID karta, a bylo mu určeno pracoviště. V našem případě zóna číslo dva až sedm.

Zóna číslo jedna (společné prostory) se deaktivuje automaticky s první zónou toho dne. Zároveň slouží jako „odkládací zóna“ pro zaměstnance pracující toho dne na jiném pracovišti. Tato situace bude vysvětlena později.

Při použití ID karty, provede aplikace docházkového systému výpočet aktuálního stavu zaměstnanců v jednotlivých zónách PZTS (Tab. 6).

Přístup do jednotlivých zón je řízen jednak přidělením PIN kódu zaměstnanci oprávněnému k deaktivaci zastřežení (Tab. 9) a také pomocí ACS (Tab. 10).

Tab. 9. Přehled práv k deaktivaci PZTS. [vlastní]

Kam / Kdo	Zóna						
	7	**6**	**5**	**4**	**3**	**2**	**1**
Vedení firmy	ANO	X	X	X	X	X	ANO
Obchodník	X	ANO	X	X	X	X	ANO
Účetní	X	X	ANO	X	X	X	ANO
Pracovník vývoje	X	X	X	ANO	X	X	ANO
Dělník	X	X	X	X	ANO	X	ANO
Skladník	X	X	X	X	X	ANO	ANO
Návštěva firmy	X	X	X	X	X	X	X

Tab. 10. Přehled povolení vstupu ACS. [vlastní]

Kam / Kdo	Zóna						
	7	**6**	**5**	**4**	**3**	**2**	**1**
Vedení firmy	ANO	ANO	ANO	ANO	ANO	ANO	ANO
Obchodník	X	ANO	ANO	ANO	ANO	X	ANO
Účetní	X	ANO	ANO	X	X	X	ANO
Pracovník vývoje	X	X	ANO	ANO	ANO	X	ANO
Dělník	X	X	ANO	ANO	ANO	X	ANO
Skladník	X	X	ANO	X	ANO	ANO	ANO
Návštěva firmy[4]	(ANO)	(ANO)	(ANO)	(ANO)	(ANO)	(ANO)	(ANO)

1 - společné prostory
2 - sklad
3 - dílny
4 - vývoj
5 - účtárna
6 - obchodní oddělení
7 - vedení firmy

Z výše uvedených tabulek je zřejmé, že každý pracovník firmy má povolen vstup a deaktivaci PZTS přinejmenším na svém pracovišti.

Je tedy zodpovědný za to, že pokud odchází z pracoviště (bezpečnostní zóny) jako poslední, bude PZTS v dané zóně aktivován.

[4] (ANO) s doprovodem zodpovědného pracovníka

7 ŘEŠENÍ MODELOVÝCH SITUACÍ PŘÍCHODU A ODCHODU ZAMĚSTNANCŮ

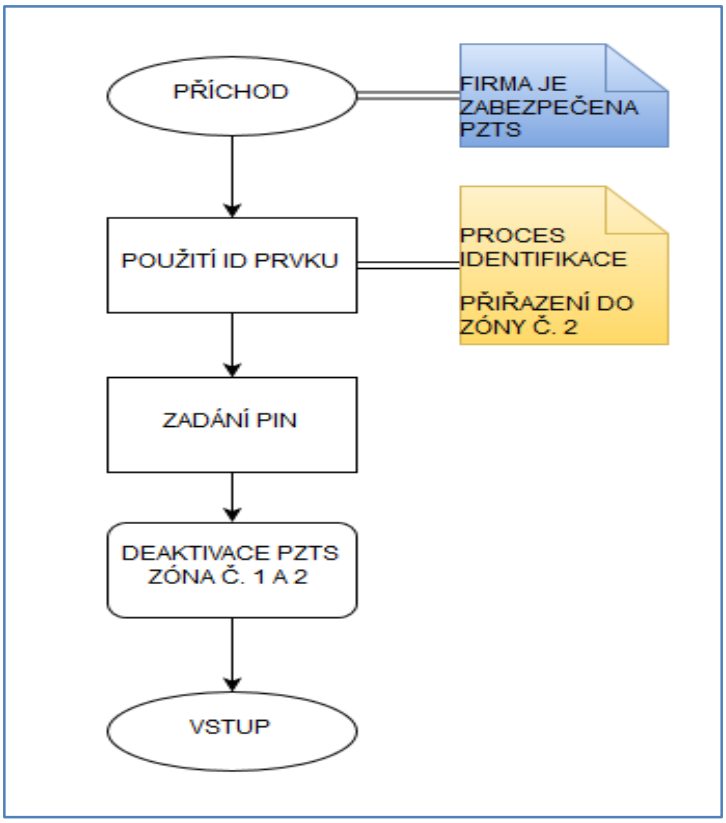
Při příchodu, resp. odchodu zaměstnance může nastat několik variant jeho chování. Systém musí umět na tyto varianty, které jsou níže popsány, adekvátně zareagovat.

7.1 Příchod do firmy

I. první zaměstnanec (zóna č. 2) otevírá firmu.

Zaměstnanec přichází jako první do firmy. Odemyká firmu a musí deaktivovat svoji zónu (společná „volná“ zóna č. 1 se deaktivuje automaticky).

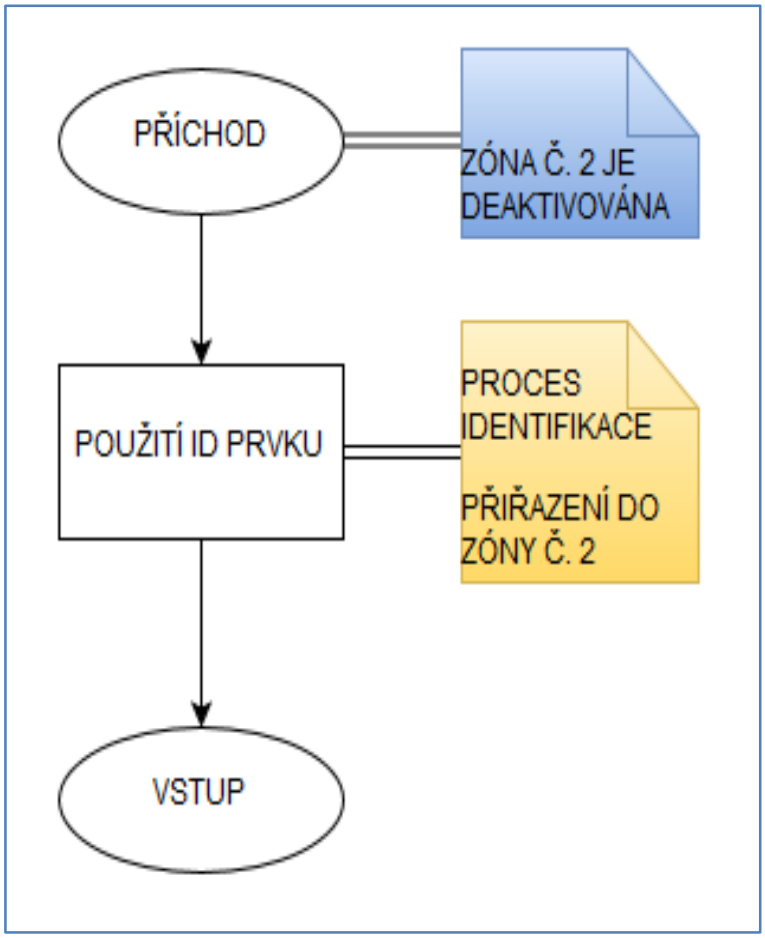
- PZTS je aktivován v celém objektu.
- Při použití ID karty dojde k identifikaci zaměstnance. Systém vyzve k zadání PIN kódu. Po ověření se deaktivuje PZTS v zóně č. 1+2.
- V docházkové aplikaci dojde k přičtení zaměstnance do zóny č. 2
- ACS uvolní místo přístupu (Obr. 15).



Obr. 15. Diagram: první zaměstnanec (zóna č. 2) otevírá firmu. [vlastní]

II. druhý zaměstnanec (zóna č. 2) přichází na své pracoviště.

- PZTS je deaktivován v zóně č. 1 a 2.
- Použitím ID karty dojde v docházkové aplikaci k identifikaci, ověření a ke kontrole stavu počítadla zaměstnanců v zóně č. 2 (aktuální stav = 1).
- Přičtení zaměstnance do zóny č. 2 (nový stav = 2).
- Zaznamenání času příchodu na pracoviště.
- ACS uvolní místo přístupu (Obr. 16).



Obr. 16. Diagram: druhý zaměstnanec (zóna č. 2) přichází na své pracoviště. [vlastní]

Varianta A - I. zaměstnanec (zóna č. 5) přichází na své pracoviště.

- Systém PZTS je deaktivován v zóně č. 1 a 2.
- Použitím ID karty dojde v docházkové aplikaci k identifikaci, ověření a ke kontrole stavu počítadla zaměstnanců v zóně č. 5 (aktuální stav = 0).

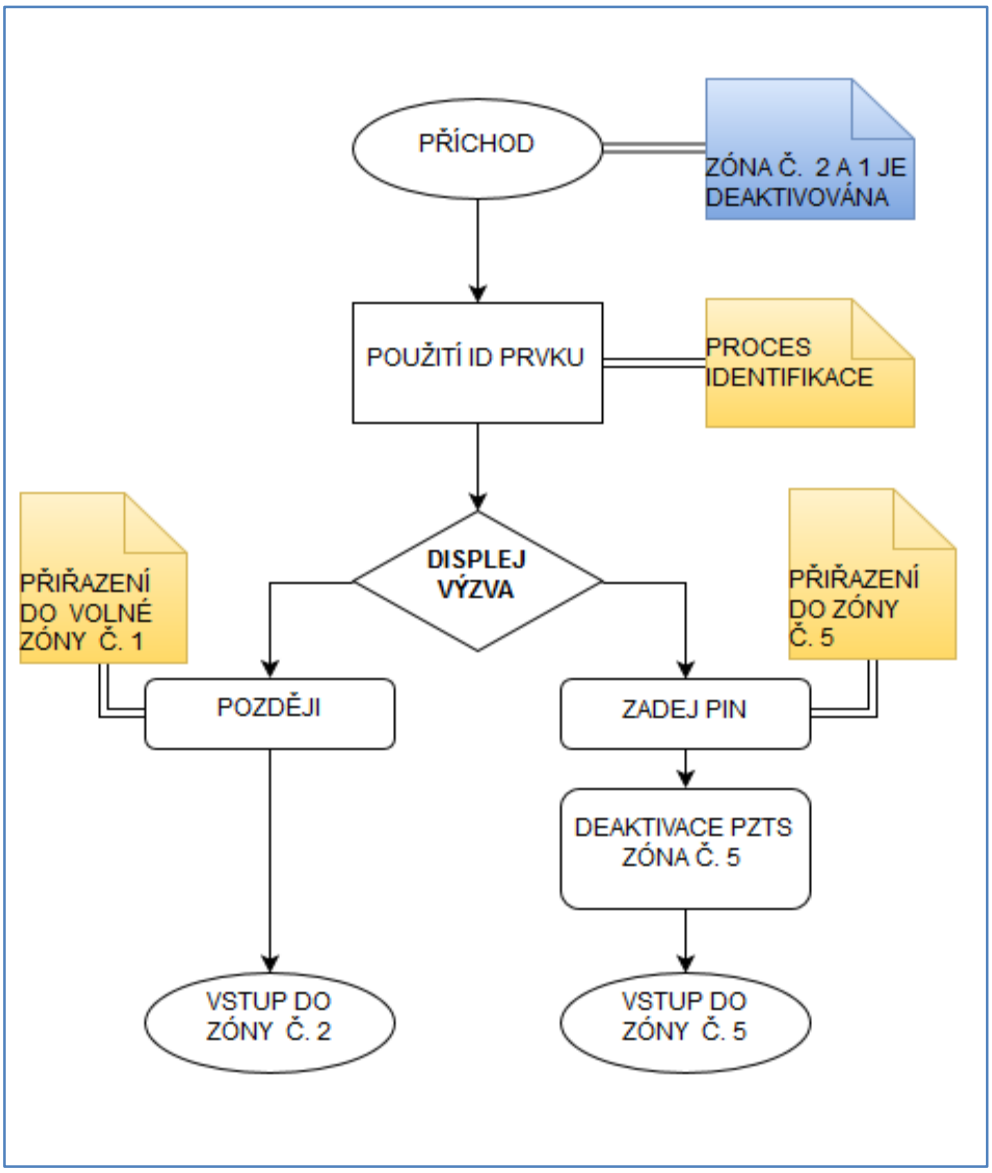
- Aplikace vyzve zaměstnance k deaktivaci PZTS v zóně č. 5 pomocí PIN. [hlášení: „ZADEJTE PIN“ nebo „POZDĚJI“]
- Zadáním PIN kódu, zaměstnanec deaktivuje zónu č. 5.
- Přičtení zaměstnance do zóny č. 5 (nový stav = 1).
- Zaznamenání času příchodu na pracoviště.
- ACS uvolní místo přístupu.

Varianta B – I. zaměstnanec (zóna č. 5) přichází na cizí pracoviště (zóna č. 2).

V zóně č. 2 je přítomen zaměstnanec s oprávněním k deaktivaci PZTS.

- Systém PZTS je deaktivován v zóně č. 1 a 2.
- Použitím ID karty dojde v docházkové aplikaci k identifikaci, ověření a ke kontrole stavu počítadla zaměstnanců v zóně č. 5 (aktuální stav = 0).
- Aplikace vyzve zaměstnance k deaktivaci PZTS v zóně č. 5 pomocí PIN. [hlášení zobrazené na terminálu: „ZADEJTE PIN“ nebo „POZDĚJI“]
- Volbou „POZDĚJI“ dojde k přičtení zaměstnance do společné zóny č. 1 (nový stav = 1)[5].
- Zaznamenání času příchodu na pracoviště.
- ACS uvolní místo přístupu (Obr. 17).

[5] Pokud bude během dne zóna č. 5 deaktivována jiným zaměstnancem, přeřadí systém automaticky Zaměstnance III. B z volné zóny do zóny č. 5.



Obr. 17. Diagram: Varianta A - I. zaměstnanec (zóna č. 5) přichází na své pracoviště. Varianta B – I. zaměstnanec (zóna č. 5) přichází na cizí pracoviště (zóna č. 2). [vlastní]

Modelové situace jsou přehledně znázorněny v diagramu příloha (P 1)

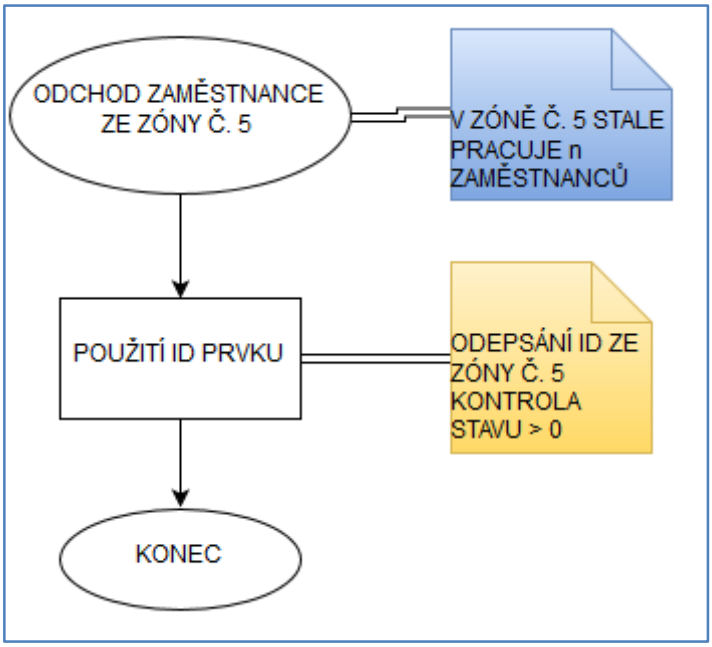
7.2 Odchod z firmy

Při odchodu ze zaměstnání může vzniknout několik variant chování zaměstnance. Stejně jako u příchodu jsou jednotlivé varianty popsány a vysvětleny.

I. zaměstnanec (zóna č. 5) odchází z pracoviště.

V zóně č. 5 je více než jeden zaměstnanec. V ostatních zónách se pracuje.

- PZTS je deaktivován v celém objektu.
- Použitím ID karty dojde v docházkové aplikaci k identifikaci, ověření a ke kontrole stavu počítadla zaměstnanců v zóně č. 5 (aktuální stav = 2).
- Odečtení zaměstnance ze zóny č. 5 (nový stav = 1).
- Zaznamenání času odchodu z pracoviště (Obr. 18).

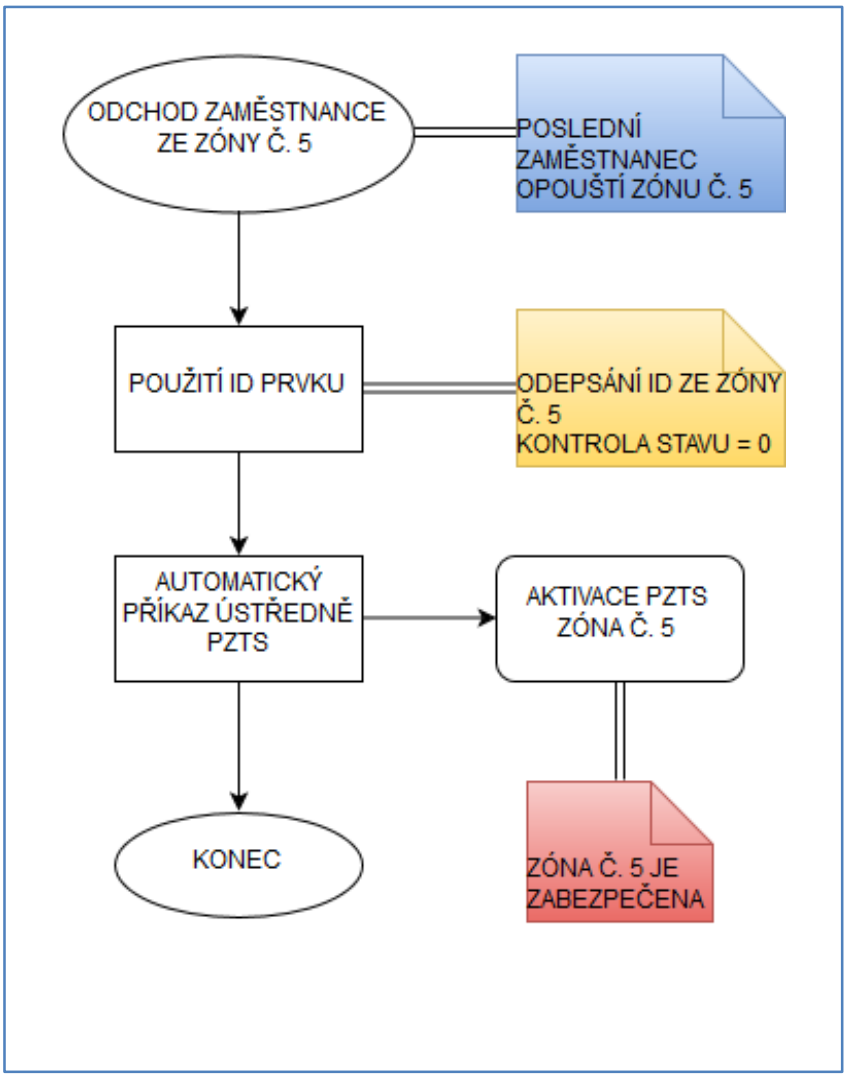


Obr. 18. Diagram: zaměstnanec (zóna č. 5) odchází z pracoviště. [vlastní]

POSLEDNÍ zaměstnanec (zóna č. 5) odchází z pracoviště.

V ostatních zónách se pracuje.

- PZTS je deaktivován v celém objektu.
- Použitím ID karty dojde v docházkové aplikaci k identifikaci, ověření a ke kontrole stavu počítadla zaměstnanců v zóně č. 5 (aktuální stav = 1).
- Odečtení zaměstnance ze zóny č. 5 (nový stav = 0).
- Aplikace vydá příkaz PZTS k aktivaci zóny č. 5.
- PZTS je aktivován v zóně č. 5.
- Zaznamenání času odchodu z pracoviště (Obr. 19).

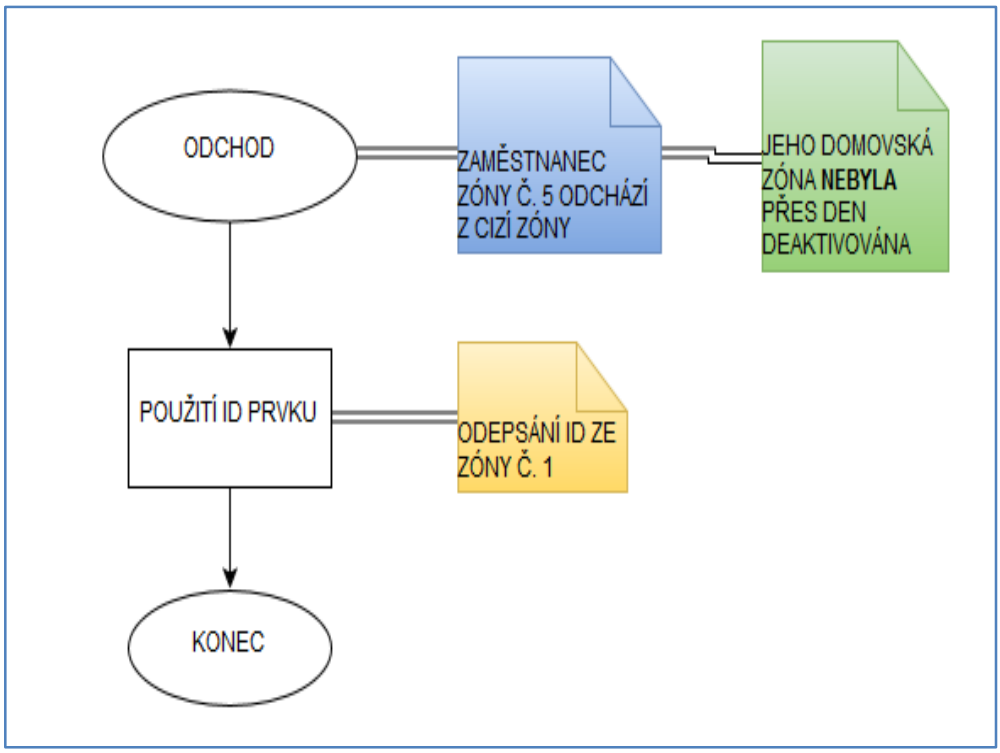


Obr. 19. Diagram: POSLEDNÍ zaměstnanec (zóna č. 5) odchází z pracoviště. [vlastní]

Varianta A - Zaměstnanec (zóna č. 5) odchází z cizího pracoviště (například zóna č. 2).

V zóně č. 2 je přítomen zaměstnanec s oprávněním k deaktivaci PZTS. Zaměstnanec zóny č. 5 zvolil při příchodu do zaměstnání volbu [POZDĚJI]. Aplikace jej zařadila do „volné“ zóny č. 1. Zóna č. 5 **nebyla** během dne deaktivována.

- PZTS je deaktivován v celém objektu.
- Použitím ID karty dojde v docházkové aplikaci k identifikaci, ověření a ke kontrole stavu počítadla zaměstnanců v zóně č. 1 (aktuální stav = 1).
- Odečtení zaměstnance ze zóny č. 1 (nový stav = 0).
- Zaznamenání času odchodu z pracoviště (Obr. 20).



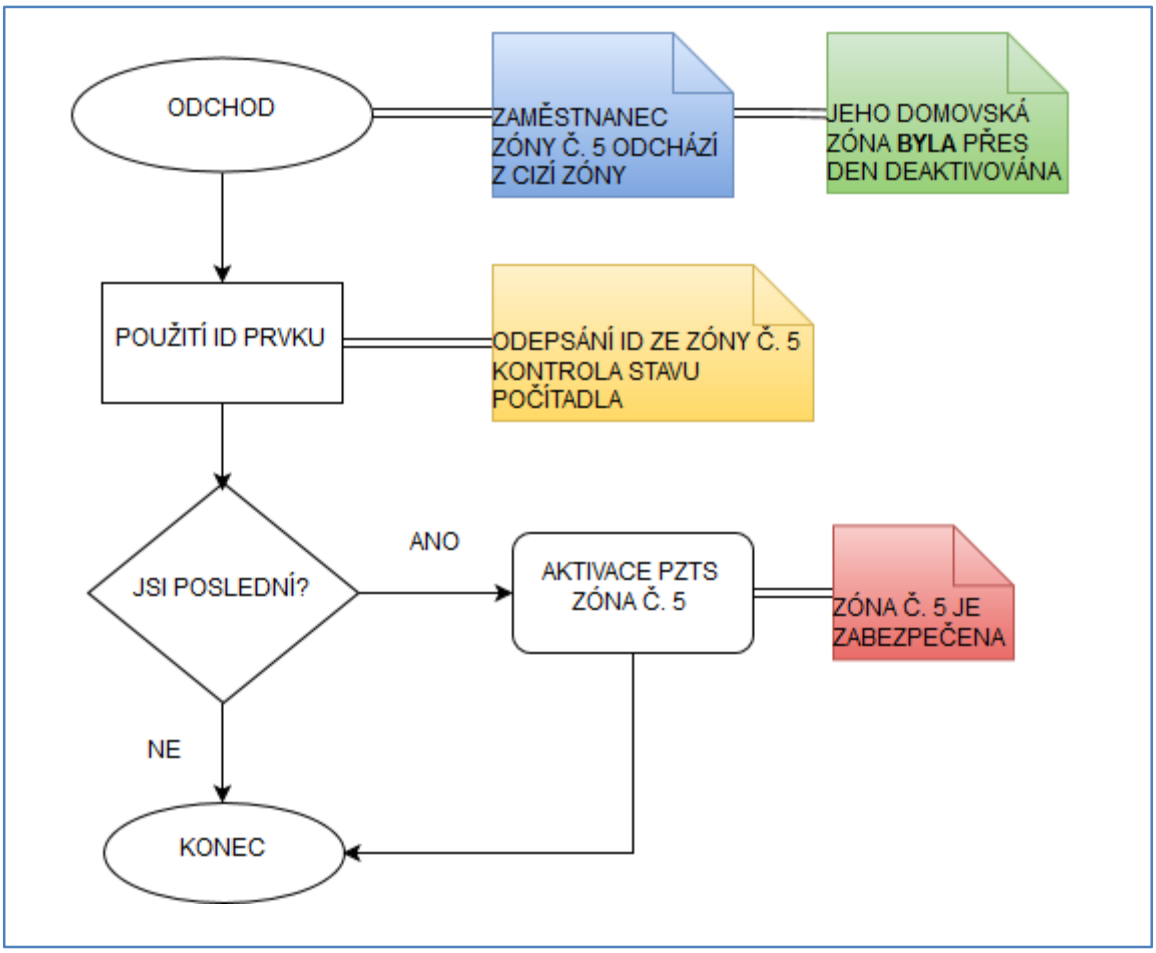
Obr. 20. Diagram: Varianta A - Zaměstnanec (zóna č. 5) odchází z cizího pracoviště (například zóna č. 2). [vlastní]

Varianta B - zaměstnanec (zóna č. 5) odchází z cizího pracoviště (například zóna č. 2)

V zóně č. 2 je přítomen zaměstnanec s oprávněním k deaktivaci. Zóna č. 5 **byla** deaktivována v průběhu dne jiným zaměstnancem. Při deaktivaci zóny č. 5 došlo automaticky k přesunu početního stavu „volného“ zaměstnance ze zóny č. 1 do zóny č. 5.

Aplikace se dále chová dle algoritmu:

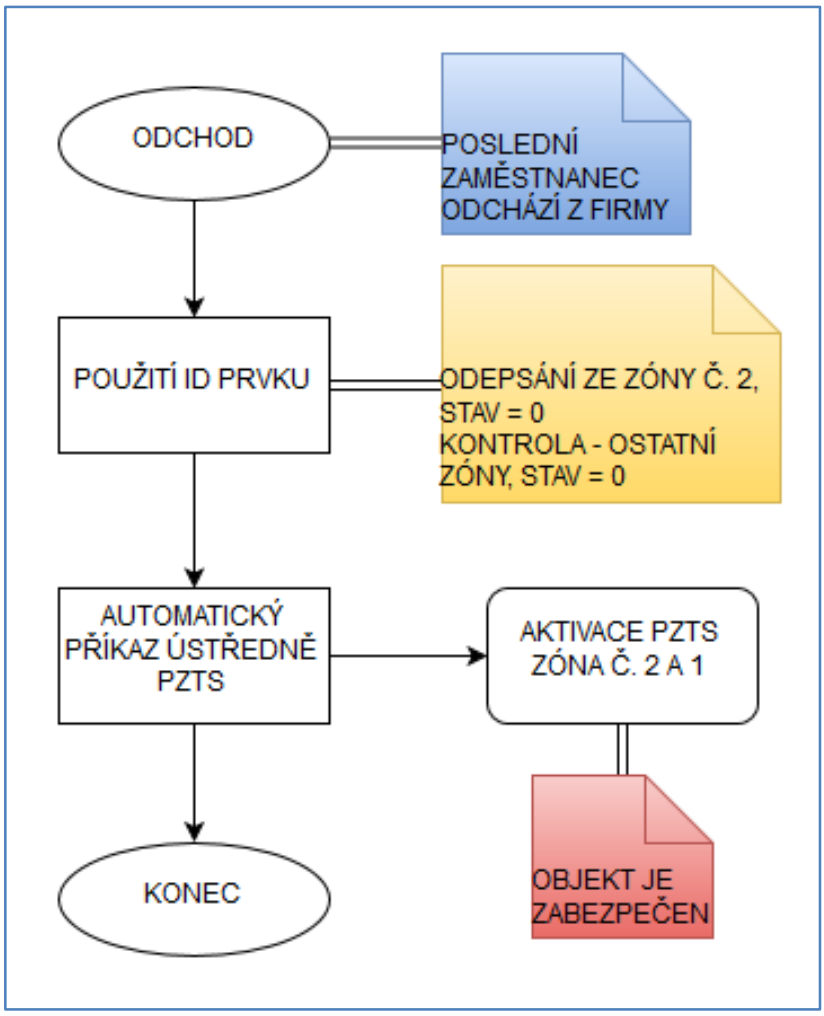
5.4.1 Zaměstnanec (zóna č. 5) odchází z pracoviště nebo 5.4.2 POSLEDNÍ zaměstnanec (zóna č. 5) odchází z pracoviště (Obr. 21).



Obr. 21. Diagram: Varianta B - zaměstnanec (zóna č. 5) odchází z cizího pracoviště (například zóna č. 2). [vlastní]

POSLEDNÍ zaměstnanec odchází z firmy.

- PZTS je deaktivován v zóně č. 1 a 2.
- Použitím ID karty dojde v docházkové aplikaci k identifikaci, ověření a ke kontrole stavu počítadla zaměstnanců v zóně č. 2 (aktuální stav = 1).
- Kontrola stavu v ostatních zónách (3, 4, 5, 6 a 7 – NS = 0)
- Odečtení zaměstnance ze zóny č. 5 (nový stav = 0).
- Aplikace vydá příkaz PZTS k zastřežení celého objektu.
- Zaznamenání času odchodu z pracoviště (Obr. 22).



Obr. 22. Diagram: POSLEDNÍ zaměstnanec odchází z firmy. [vlastní]

Modelové situace jsou přehledně znázorněny v diagramu příloha (P 2).

7.3 Dílčí shrnutí

Popisem možných variant příchodů a odchodů zaměstnanců do firmy, resp. z firmy bylo potvrzeno, že softwarová úprava docházkového systému, popsaná výše, umožňuje dostatečnou kontrolu aktivace zastřežení příslušné zóny. Přístup do zaměstnání je podmíněn použitím ID karty, resp. PIN kódu.

Při příchodu a odchodu je zaměstnanec nucen použít ID kartu v docházkovém systému.

Tímto krokem umožní systému provést minimálně dva důležité úkony:

1. Zahájení a ukončení pracovní doby, a započítání odpracovaného času do výkazu práce. Tento krok je v jeho vlastním zájmu, a poslouží jako motivační prvek pro zaměstnance, pokud chce dostat za práci zaplaceno.
2. Provedení výpočtu stavu zaměstnanců v jednotlivých zónách, resp. ve firmě, a tím umožní vyhodnocení aktuálního stavu zaměstnanců a následnou automatickou aktivaci PZTS.

Celý proces je automatizován, a tím se eliminuje chyba zaměstnance při aktivaci PZTS. Toto opatření by mělo dostatečně zamezit nezodpovědnému jednání zaměstnance pracujícího ve firmě, která zastává povolnou politiku bezpečnosti (je povoleno vše, co není výslovně zakázáno).

ZÁVĚR

V této diplomové práci seznamuji čtenáře s problematikou jednání zaměstnance vůči zabezpečovacím systémům firmy a jeho vlivu na zajištění celkové bezpečnosti. V úvodu práce bylo stanoveno několik úkolů. Jedním z nich je vypracování rešerše základních zabezpečovacích systémů a popsání možných problémů při používání systémových komponentů zaměstnanci. Jedná se například o komunikátory a klávesnice, tedy o ty části systému, se kterými přijde zaměstnanec bezprostředně do styku. Zpracováním této části jsem dospěl k závěru, že nejzranitelnější součástí bezpečnostního systému je lidský činitel. V dnešní době lze vcelku bez problémů zálohovat hardwarové i softwarové prostředky tak, aby byla možná chyba eliminována v co největší míře. Pokud však zařadíme do systému člověka s možností rozhodování, je zde vždy riziko špatného nebo chybného rozhodnutí. Člověk podléhá při rozhodování mnoha vnitřním i vnějším vlivům. V těchto konkrétních případech jde spíše o negativní jednání.

Řídící jednotka přístupového systému je naprogramovaná tak, aby každý den v devět hodin zamkla všechny vstupy do budovy. Pokud není v programu další podmínka, tak daný příkaz provede, i když bude venku pršet nebo na stole zvonit telefon. Tentýž příkaz není fyzická ostraha schopna splnit, a to minimálně z časového hlediska. Najednou nedokáže jeden člověk uzamknout desatero dveří. Toto je samozřejmě pouze jednoduchý příklad. Mohou následovat další vlivy - pracovník ostrahy zapomene, zaspí, zazvoní mu telefon nebo u něj nastane zdravotní indispozice. V tomto ohledu se jeví přenesení odpovědnosti na zabezpečovací systém jako přínos. Proto je potřeba při projektování zabezpečovacích systémů brát v úvahu nejen technické řešení, ale také možnost jeho ovlivnění lidským faktorem.

Úkolem této práce bylo zjistit jaký vliv má osobní odpovědnost zaměstnance na zabezpečení firmy. Zaměstnanec je běžný uživatel zabezpečovacích systémů, pracující v kanceláři nebo v dílně. K jeho povinnostem patří i zajištění zabezpečení firmy při odchodu. Z vlastního pozorování v konkrétní firmě jsem zjistil, že tento úkol není často splněn, a proto jsem se rozhodl pro vypracování této práce, a nalezení řešení této bezpečnostní hrozby.

Provedl jsem návrh způsobu rozdělení jednotlivých oddělení firmy na zóny zabezpečení, které budou přiřazeny jako nové atributy každému ID prvku. Pomocí nástroje počítadla lze zaznamenat aktuální stav zaměstnanců v každé zóně zabezpečení. Díky této softwarové úpravě je možné provést automatickou aktivaci PZTS bezprostředně poté, co poslední zaměstnanec opustí příslušnou zónu.

Modelové situace popsané v práci řeší i případy, kdy jde zaměstnanec pracovat do jiné zóny, než je mu přidělena. Tyto situace jsou popsány a vyjádřeny pomocí vývojových diagramů. Automatizace zabezpečení se týká pouze odchodu zaměstnance z firmy. Z hlediska bezpečnosti jsem při příchodu zaměstnance do firmy zachoval nutnost použití druhého stupně identifikace - zadání PIN kódu. V opačném případě by se stala firma (konkrétní zóna) propustná pro kohokoliv, kdo kartu najde, než bude vymazána ze systému.

Využitím navrhovaného řešení dochází ke zvýšení zabezpečení firmy, a to zejména z důvodu minimalizace vlivu zaměstnance na zabezpečovací systém. Při odpovědném nastavení systému, a dodržování pravidel pro používání ID prvků jak ze strany zaměstnanců tak i zaměstnavatele, může navrhované řešení zlepšit zabezpečení i dalším firmám s podobnou charakteristikou provozu.

Na úplný závěr se chci zmínit o integraci zabezpečovacích systémů, která je v dnešní době velmi diskutovaná. Celosvětově jsou zřejmé tendence k využití a propojení moderních technologii do tzv. Smart Systems. Tyto systémy mají za úkol vytvořit jednodušší, pohodlnější, bezpečnější a rychlejší prostředí pro život. Na druhou stranu mohou také umožnit jeho řízení na dálku, kontrolu a přenesení odpovědnosti za vlastní rozhodnutí na „chytrý systém“. Tímto se mnozí lidé stávají, dle mého názoru, závislí na těchto technologiích, a zároveň i zranitelnějšími. Nelze opomenout fakt, že celý systém je závislý na elektrické energii. Nabízí se otázka, co se stane se stotisícovým „Smart City“, když nastane Black Out, trvající několik dní?

SEZNAM POUŽITÉ LITERATURY

[1] VALOUCH, Jan. *Projektování integrovaných systémů*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj (152 s.). ISBN 978-80-7454-296-1. Dostupné také z: http://hdl.handle.net/10563/25814

[2] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management III: [teorie a praxe ochrany majetku a fyzické bezpečnosti]*. 1. vyd. Zlín: VeRBuM, 2013-, 3 sv. ISBN 978-80-87500-35-4.

[3] Požární signalizace. *Interkonnect: Na stejné vlně* [online]. [cit. 2016-01-25]. Dostupné z: http://www.interconnect.cz/ostatni-sluzby/bezpecnostni-systemy/pozarni-signalizace

[4] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 3. aktualiz. S.l.: Cricetus, 2006, 313 s. ISBN 80-902938-2-4.

[5] *Protipozarni - systemy. com: Konvenční tlačítkový hlásič - detail produktu* [online]. [cit. 2016-01-26]. Dostupné z: http://www.protipozarni-systemy.com/konvencni-tlacitkovy-hlasic/

[6] Projektování elektrické požární signalizace EPS. *Delnet: elektromontáže inteligentní elektroinstalace* [online]. 2014 [cit. 2016-01-30]. Dostupné z: http://www.delnet.cz/projekcni-cinnost/projektovani-systemu-eps.html

[7] Falešné požární poplachy v budovách a jejich příčiny, 2013. *Inteligentní budovy: Moderní technologie pro inženýry* [online]. [cit. 2016-01-20]. Dostupné z: http://inbudovy.cz/artykul/article/falesne-pozarni-poplachy-v-budovach-a-jejich-priciny/

[8] KINDL, Jiří. *Projektování bezpečnostních systémů I*. 2. vyd. Zlín: Univerzita Tomáše Bati, 2007, 134 s. ISBN 978-80-7318-554-1.

[9] UHLÁŘ, Jan. *Technická ochrana objektů*. Vyd. 1. Praha: Policejní akademie české republiky, 2005, 229 s. ISBN 80-7251-189-0.

[10] EZS. In: *Střední škola, Havířov-Šumbark, Sýkorova 1/613, příspěvková organizace: Elektrotechnika & strojírenství* [online]. [cit. 2016-02-07]. Dostupné z: outech-havirov.cz/skola/files/knihovna_eltech/ete/ezs.pdf

[11] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I: [teorie a praxe ochrany majetku a fyzické bezpečnosti]*. 1. vyd. Zlín: VeRBuM, 2011-, 1 sv. ISBN 978-80-87500-05-7.

[12] Přístupový systém. *ACS line: Elektronický identifikační systém* [online]. [cit. 2016-03-21]. Dostupné z: http://www.acsline.cz/cs/pristupovy-system

[13] JUŘÍK, Pavel. *Encyklopedie platebních karet: historie, současnost a budoucnost peněz a platebních karet*. 1. vyd. Praha: Grada, 2003, 312 s. ISBN 8024706857.

[14] Topologie systému: Autonomní systém. *Techfass: český výrobce identifikačních systémů* [online]. [cit. 2016-01-03]. Dostupné z: http://www.techfass.cz/aps-mini-plus-topology-cz.html

[15] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II: [teorie a praxe ochrany majetku a fyzické bezpečnosti]*. 1. vyd. Zlín: VeRBuM, 2012-, 2 sv. ISBN 978-80-87500-19-4.

[16] Skenování otisků, duhovky, obličeje - biometrie proniká i do mobilů: Využití biometrického způsobu snímaní. *Česká televize* [online]. 2015 [cit. 2016-03-02]. Dostupné z: http://www.ceskatelevize.cz/ct24/domaci/1507374-skenovani-otisku-duhovky-obliceje-biometrie-pronika-i-do-mobilu

[17] *Security guide.cz: Drony jako fyzická ostraha objektů* [online]. 2016 [cit. 2016-03-02]. Dostupné z: https://www.securityguide.cz/security/viewArticle/drony-jako-fyzicka-ostraha-objektu

[18] Trendy 2016: Jaké myslíte, že budou nejvýznamnější trendy v oblasti video dohledových systémů v roce 2016? *Security guide.cz* [online]. 2016 [cit. 2016-03-02]. Dostupné z: https://www.securityguide.cz/security/viewArticle/trendy-2016

[19] Cloud. *Bluebord.cz: Nápověda a znalostní báze* [online]. [cit. 2016-03-02]. Dostupné z: https://hosting.blueboard.cz/napoveda/cloud

[20] Bezkontaktní čtečky: Dokumenty ke stažení. In: *Cominfo Security First: Váš partner pro bezkontaktní identifikaci a vstupní zařízení* [online]. [cit. 2016-02-13]. Dostupné z: http://www.cominfo-trade.com/cz/produkty/komponenty-a-hardware/bezkontaktni-ctecky

[21] Terminál REA Touch: Dokumenty ke stažení. In: *Cominfo Security First: Váš partner pro bezkontaktní identifikaci a vstupní zařízení* [online]. [cit. 2016-02-13]. Dostupné z: http://www.cominfo-trade.com/cz/produkty/komponenty-a-hardware/terminal-reatouch

[22] Přístupový systém - ACCESS: Systém Infos. In: *Cominfo Security First: Váš partner pro bezkontaktní identifikaci a vstupní zařízení* [online]. [cit. 2016-02-13]. Dostupné z: http://www.cominfo-trade.com/cz/reseni/pristupovy-system

[23] Architektura klient-server. *Management mania* [online]. 2015 [cit. 2016-02-13]. Dostupné z: https://managementmania.com/cs/architektura-klient-server

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Access Control System (přístupový systém)
APAS	Výstupní ovládací prvky a senzory místa přístupu
EPS	Elektronický požární systém
ETHERNET	Podniková informační síť
GSM	Groupe Spécial Mobile (globální systém pro mobilní komunikaci)
HAS	Hold-up Alarm System (poplachový tísňový systém)
HZS	Hasičský záchranný sbor
I&HAS	Intruder and Hold-up Alarm System (poplachový zabezpečovací a tísňový systém)
IAS	Intruder Alarm System (poplachový zabezpečovací systém)
INFORMIX	Systém řízení báze dat
IPS	Integrovaný poplachový systém
LAN	Local Area Network (lokální, místní síť)
LCD	Liquid Crystal Display (displej z tekutých krystalů)
LED	Light-Emitting Diode (dioda emitující světlo), polovodičová elektronická součástka
LINUX	Druh operačního systému
MS SQL server	Systém řízení báze dat
ORACLE	Systém řízení báze dat
PCO	Pult centralizované ochrany
PIR	Passive Infra Red (detektor pohybu)

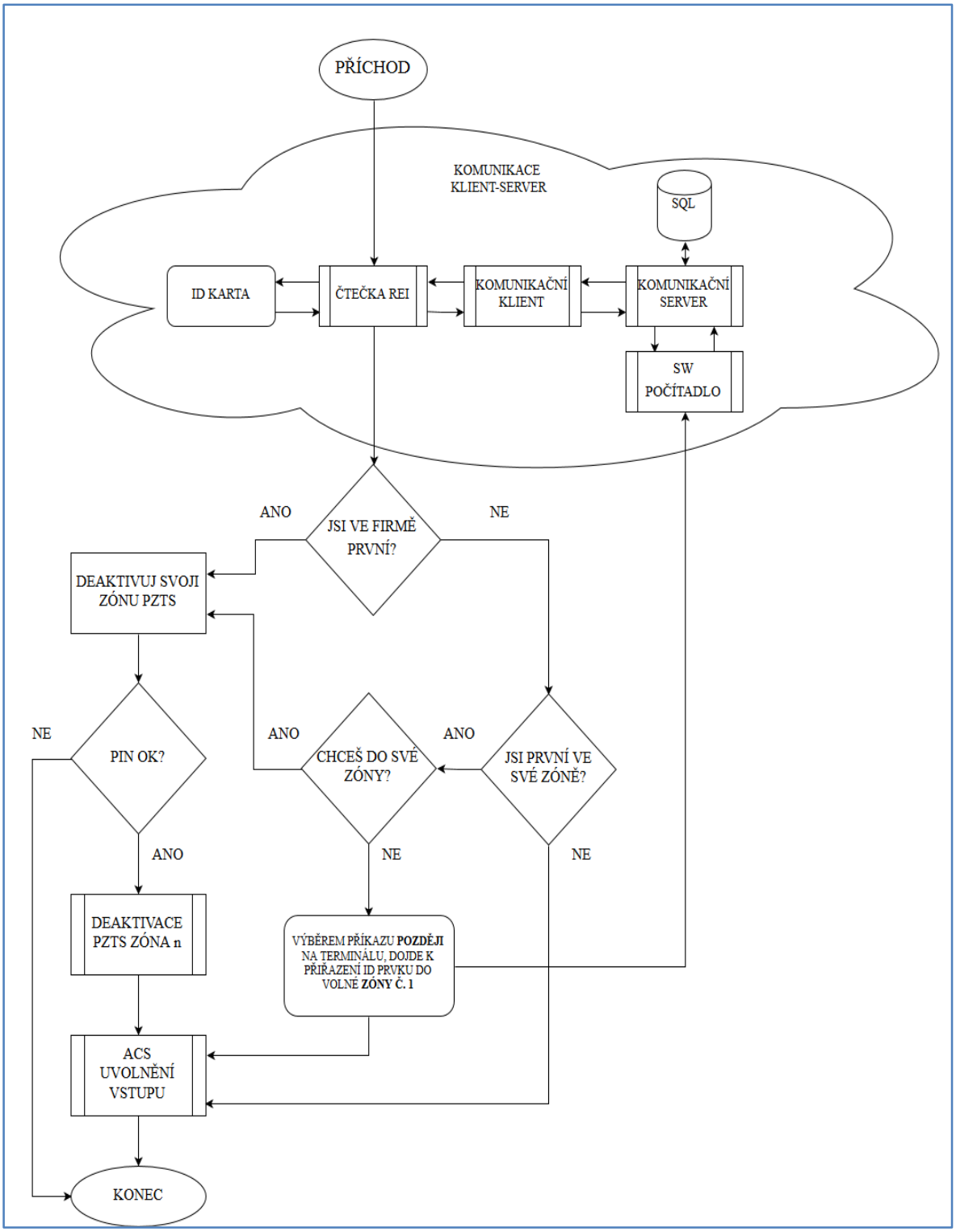
PoE	Power ower Ethernet (napájení po datovém síťovém kabelu)
PPC	Poplachové, přijímací centrum
PTS	Poplachový tísňový systém
PZTS	Poplachový, zabezpečovací a tísňový systém
RFID	Radio Frequency Identification (identifikace na rádiové frekvenci)
RS-485	Datová sběrnice
SAS	Social Alarm Systém (systém přivolání pomoci)
SQL server	Structured Query Language (strukturovaný dotazovací jazyk), Databázový stroj
UNIX	Operační systém
USB	Universal Serial Bus (univerzální sériová sběrnice)
WIEGAND	Komunikační protokol

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DIAGRAM PŘÍCHODU ZAMĚSTNANCŮ DO FIRMY



PŘÍLOHA P II: DIAGRAM ODCHODU ZAMĚSTNANCŮ Z FIRMY