Moderní metody docházkových a přístupových systémů

Bc. Tomáš Groš

Diplomová práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. Tomáš Groš**
Osobní číslo:	**A15282**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Moderní metody docházkových a přístupových systémů**
Téma anglicky:	**Modern Methods of Access and Attendance Control Systems**

Zásady pro vypracování:

1. **Analyzujte technické normy a technologické trendy z oblasti docházkových a přístupových systémů.**
2. **Proveďte komparaci vybraných analytických a prognostických metod.**
3. **Navrhněte evaluační metodiku přístupových a docházkových systémů pro podmínky rozsáhlé výrobní společnosti.**
4. **Analyzujte soudobý přístupový a docházkový systém vybrané rozsáhlé výrobní společnosti.**
5. **Vytvořte studii přístupových a docházkových systémů pro podmínky rozsáhlé výrobní společnosti.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **VALOUCH, Jan a Martin HROMADA. Bezpečnostní futurologie. Zlín: Univerzita Tomáše Bati ve Zlíně, 2016. ISBN 978-80-7454-621-1.**
2. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV: Teorie a praxe ochrany majetku a fyzické bezpečnosti. 1. vyd. Zlín: VeRBuM, 2014. ISBN 978-808-7500-576.**
3. **RAK, Roman a kolektiv. Biometrie a identita člověka. Praha: Grada, 2008, 664 s.ISBN 978-80-247-6392-7.**
4. **ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy Část 11-1: Elektronické systémy kontroly vstupu Požadavky na systém a komponenty. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídicí znak 33 4593.**
5. **ČSN EN 60839-11-2 Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016. Třídicí znak 334593.**

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

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

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

Ve Zlíně dne 3. února 2017

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Jméno, příjmení: Bc. TOMÁŠ GROŠ

Název bakalářské/diplomové práce: MODERNÍ METODY DOCHÁZKOVÝCH A PŘÍSTUPOVÝCH SYSTÉMŮ

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 17.5.2017

.....
podpis diplomanta

ABSTRAKT

Diplomová práce je zaměřena na moderní metody docházkových a přístupových systémů. Teoretická část se zabývá analýzou technických norem a technologickými trendy z oblasti docházkových a přístupových systémů. Dále pak provedením komparace vybraných analytických a prognostických metod. Praktické část se zabývá návrhem evaluační metodiky přístupových a docházkových systémů pro podmínky konkrétní vybrané rozsáhlé výrobní společnosti. Analyzuje její soudobý přístupový a docházkový systém. Cílem diplomové práce je vytvoření studie přístupových a docházkových systémů pro podmínky zvolené konkrétní rozsáhlé výrobní společnosti.

Klíčová slova: systémy kontroly vstupu, biometrie, analýza, studie, rozsáhlá výrobní společnost

ABSTRACT

The diploma thesis is focused on modern methods of attendance and access systems. The theoretical part deals with the analysis of technical standards and technological trends in the field of attendance and access systems. Further, by comparing selected analytical and prognostic methods. Practical part deals with proposal of evaluation methodology of access and attendance systems for the conditions of particular selected large production company. It analyzes its current access and attendance system. The aim of the diopo work is to create a study of access and attendance systems for the conditions of a particular large-scale production company.

Key words: access control systems, biometrics, analysis, studies, extensive production community

Tímto bych chtěl poděkovat svému vedoucímu Ing. Jiřímu Ševčíkovi za jeho vedení, poskytnutý čas a cenné rady při vypracovávaní mé diplomové práce. Dále bych rád poděkoval mým rodičům, přátelům a kamarádům za podporu po celou dobu studia.

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

OBSAH

ÚVOD

Díky neustálému pokroku a vývoji nových technologií se objevují stále novější a sofistikovanější možnosti jak umožnit přístup do střeženého objektu. V současnosti se již téměř každá větší či menší firma snaží zabezpečit a kontrolovat přístup do svých objektů, ať už budov nebo pozemků. Dříve se tento vstup kontroloval pouze za pomoci lidských zdrojů, tzv. vrátných a každá vstupující osoba musela být tímto člověkem zkontrolována. S vývojem nových technologií se začaly pro tento účel používat přístupové a docházkové systémy. Tak jak šel pokrok stále kupředu, začaly se objevovat nové a nové metody. Dnes jsou největší inovací na tomto poli biometrické systémy. Ty se stále více začínají uplatňovat jak v zabezpečení osobního majetku, tak i v zabezpečení přístupu do firem.

Cílem této diplomové práce je zhotovení studie modernizace přístupových a docházkových systémů pro podmínky konkrétní zvolené rozsáhlé výrobní společnosti. Půjde zde především však o možnost aplikace těchto nadčasových systémů do prostředí rozsáhlé výrobní společnosti.

V teoretické části této diplomové práce se budeme nejprve zabývat samotnými systémy kontroly vstupu. Co vlastně jsou a jaké musí plnit základní funkce. Dále pak veškerými normami, které se vztahují k systému kontroly vstupu a jsou platné v České republice. Posléze současnými technologickými trendy, které se objevují v oblasti přístupových a docházkových systémů. V další části se zaměříme na analytické a prognostické metody. Jak se dané metody dělí a výčtem těch nejznámějších a nejpoužívanějších. Na závěr pak dojde k jejich jednotlivým srovnáním.

V praktické části diplomové práce se budeme nejprve zabývat analýzou současného přístupového a docházkového systému vybrané rozsáhlé výrobní společnosti. Zde nejprve charakterizujeme zvolenou výrobní společnost a zjistíme, jaký přístupový a docházkový systém je zde využíván. Dojde k popisu jednotlivých způsobů, jak lze získat přístup do areálu firmy a co vše musí být splněno. Následně dojde k popsání jednotlivých vrátnic, které jsou určeny pro vstup do areálu společnosti. V závěrečné kapitole se budeme zabývat studií nových metod přístupových a docházkových systémů pro podmínky vybrané výrobní společnosti. Zde bude zmíněn zákon č. 101/2000 Sb., o ochraně osobních údajů. Dále pak budou uvedeny v současnosti nejpoužívanější metody přístupu, které by bylo možno co nejlépe aplikovat pro podmínky dané společnosti. Cílem je zhodnotit a určit, na které z vrátnic by bylo nejvhodnější metody aplikovat.

I. TEORETICKÁ ČÁST

1 SYSTÉMY KONTROLY VSTUPU

Systémy kontroly vstupu představují jeden z typů poplachových systémů, které je možné definovat jako určitý soubor opatření k zajištění a evidenci přístupu do námi zabezpečeného prostoru nebo objektu na základě jednoznačně přidělených přístupových práv. Tento soubor opatření můžeme rozdělit na fyzické (ostraha), mechanické (mříže), elektronické nebo systémové, ale nejúčinnější je kombinace všech. Pro vstup nebo odchod se zabezpečeného prostoru jsou danému zaměstnanci nebo uživateli přidělena přístupová práva na základě určitého časového harmonogramu profesní politiky nebo stupně oprávnění apod. Po této identifikaci a ověření je buď vstup povolen, nebo zamítnut. Složitější systémy pak sledují pohyb a přítomnost osob v jednotlivých úsecích a mohou popřípadě za běhu měnit přístupová práva. Obecně se systém kontroly vstupu popisuje do tří bodů:

KDO se dostane KAM a KDY.

Velmi nutné je také rozlišovat pojmy „přístupové“ a „docházkové“ systémy. Za docházkový systém lze považovat ten, který nejenom prokáže identitu uživatele, ale také monitoruje čas a důvod průchodu daným místem, aby bylo možno sledovat délku pracovní doby nebo povinné přestávky zaměstnanců. Úkolem přístupových systémů je řídit přístup k oblastem, které mají být chráněny zařízeními k ochraně firemních aktiv, informací a dat na základě předem určených pravidel. [1]

1.1 Funkce systémů kontroly vstupu

Systém kontroly vstupu musí splňovat základní funkce jejich výčet je obsáhnut v normě ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty. Jedná se o 11 základních funkcí, jejichž výčet je uveden následně:

- **zpracování** – porovnávání změn, které v systému nastaly s přednastavenými pravidly,
- **komunikace** – přenos signálu mezi komponenty systému kontroly vstupu,
- **konfigurace** (programování) – nastavení pravidel zpracování,
- **rozhraní míst přístupu** – aktivace a monitorovaní místa přístupu,
- **identifikace** – rozpoznání oprávněných uživatelů žádající o přístup,
- **oznámení** – funkce výstrahy zobrazení nebo záznamu událostí,

- **signalizace nátlaku** – tiché varování o stavu probíhajícího vynucovaného požadavku přístupu,
- **rozhraní pro spojení s ostatními systémy** – sdílení funkcí nebo změn, k nimž v systémech dochází,
- **vlastní ochrana systému** – slouží k prevenci, detekci nebo informování o úmyslném nebo náhodném zasahování do systému.
- **napájecí zdroj,**
- **uživatelské rozhraní** – žádost o přístup, indikace. [2]

1.2 Standardy v oblasti systémů kontroly vstupu

Do nedávné doby byly systémové a technické požadavky na systém kontroly vstupu upraveny technickými normami řady ČSN EN 50133. V současné době jsou ale tyto normy nahrazeny novými a to normou ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty. A posléze normou ČSN EN 60839-11-2 Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace, která je v platnosti současně s normou, kterou nahrazuje ČSN EN 50133-7 Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace jejich platnost skončí 13. 4. 2018. [1]

Dále je nutné v rámci jednotlivých procesů zřizování systémů kontroly vstupu dodržet i požadavky dalších technických norem. Mezi ně například patří normy upravující požadavky na komponenty v rámci procesu jejich uvádění na trh. Většina komponentů systému kontroly vstupu je z hlediska jejich konstrukce zařazena mezi tzv. stanovené výrobky, tj. výrobky, které by mohly ve zvýšené míře ohrozit zdraví nebo bezpečnost osob, majetek a životní prostředí, popřípadě jiný veřejný zájem. [1]

S ustanovením zákona č. 22/1997 Sb. o technických požadavcích na výrobky musí být před uvedením stanovených výrobků na trh provedeno posouzení shody parametrů s požadavky technických předpisů. Na základě splnění úspěšného posouzení shody je nutné ze strany výrobce označit výrobek značkou CE a vydat ES prohlášení o shodě. Požadavky pro jednotlivé typy stanovených výrobků jsou podle zákona č. 22/1997 Sb. upřesněny v nařízeních vlády. Na elektronické a elektrické komponenty systému kontroly vstupu se vztahují ustanovení nařízení vlády č. 616/2006 Sb. (elektronická kompatibilita) a NV č. 17/2003 Sb. (elektrická bezpečnost). Vybraných komponentů, převážně komunikačních

respektive bezdrátových prvků, se týká ustanovení NV č. 426/2000 Sb. opět se spojením s NV č. 17/2003 (elektrická bezpečnost). [1]

V následující tabulce bude uveden přehled aktuálních norem v rámci problematiky požadavků na systémy kontroly vstupu jako součásti poplachových systémů.

Tab. 1. *Základní technické normy v oblasti systémů kontroly vstupu* [1]

p.č.	Číslo technické normy	Název technické normy
1.	ČSN EN 60839-11-1	Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty.
2.	ČSN EN 60839-11-2	Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace.
3.	ČSN EN 50133-7	Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace.
4.	ČSN EN 50130-4 ed.2	Poplachové systémy – část4: Elektronická kompatibilita – Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci.
5.	ČSN EN 50130-5 ed.2	Poplachové systémy – Část 5: Metody zkoušek vlivu prostředí.
6.	ČSN CLC/TS 50389	Poplachové systémy – Kombinované a integrované systémy – všeobecné požadavky.

V procesu návrhu, projektování a instalace systémů kontroly vstupu je potřeba dodržet i požadavky technických norem, které se vztahují na elektrické instalace nízkého napětí, mezi ně patří například:

- ČSN 33 2000-4-41 ed.2 Elektrické instalace nízkého napětí – část 4-41: Ochranná opatření pro zajištění bezpečnosti – Ochrana před úrazem elektrickým proudem.
- ČSN 33 2000-5-51 ed. 3 Elektrické instalace nízkého napětí – Část 5-51: Výběr a stavba elektrických zařízení – Všeobecné předpisy.
- ČSN 33 2000-6 Elektrické instalace nízkého napětí – Část 6: Revize. [1]

1.2.1 ČSN EN 60839-11-1

Technická norma byla vydána v únoru 2014. Jak již bylo řečeno, úplné účinnosti ale nabyla až od 11. 6. 2016 kdy úplně nahradila původní normu ČSN EN 50133-1. Řeší nové standardy pro systémy kontroly vstupu, a to v následujících oblastech:

- terminologie,
- architektura systému,
- stupně klasifikace,
- požadavky na funkčnost systému,
- požadavky na odolnost proti vlivům prostředí,
- způsoby zkoušek.

Oproti předchozí technické normě ČSN EN 50133-1 zde zejména dochází k následujícím změnám:

- je nově stanovena klasifikace zabezpečení, ta již není založena na třídách identifikace a třídách přístupu, ale je podobně jako u poplachových zabezpečovacích a tísňových systémů rozdělena na úrovně rizika, přičemž jsou stanoveny čtyři klasifikační stupně,
- zvýšil se rozsah a podrobnost zpracování funkčních požadavků,
- dále se zvýšila míra volnosti a inspirace funkčních požadavků pro jednotlivé aplikace systému kontroly vstupu, kdy část požadavků je pouze volitelná,
- byla rozšířena terminologie o nové názvy jako např. EACS – Electronic Access Control Systems, FAR – False Acceptance Rate, portál atd. [2]

1.2.2 ČSN EN 60839-11-2

Technická norma byla vydána v březnu 2016. Úplné účinnosti ale nabude až 13. 4. 2018, kdy nahradí normu ČSN EN 50133-7. V současné době obě normy platí souběžně. V této normě jsou upraveny problematiky spojené s postupem návrhu projekce, instalace, revize, provozu a údržby systémů kontroly vstupu, které vychází z nových požadavků stanovené ČSN EN 60839-11-1. Jsou zde řešeny nové standardy v následujících oblastech:

- terminologie,
- požadavky na odolnost proti vlivům prostředí a EMC,
- plánování systémů a analýza rizik,

- montáž systému,
- uvedení do provozu a předání,
- provoz a údržba,
- dokumentace. [3]

1.2.3 ČSN EN 50130-4 ed.2

Technická norma stanovuje společné požadavky na komponenty různých typů poplachových systémů, a to na zkoušky elektromagnetické odolnosti. Jsou zde definovány podmínky a úrovně testování pro zkoušky vyzařovaným elektromagnetickým polem, poklesy a přerušení napětí, rázové impulsy rychlé přechodové děje, elektrostatické výboje atd.

Veškeré zkoušky a zkušební hodnoty jsou společné pro vnitřní i venkovní aplikace, pro pevná, přenosná i přemístitelná zařízení. Nejsou zde ale nastaveny extrémní případy, které mohou nastat např. v blízkosti výkonných zdrojů elektromagnetického vyzařování. Testovaná zařízení jsou navržena tak, aby spolehlivě fungovala v rámci elektromagnetických podmínek v místě instalace v prostředí obytném, lehkého průmyslu a prostředí průmyslovém. [4]

1.2.4 ČSN EN 50130-5 ed.2

Podobně jako u ČSN EN 50130-4 stanovuje tato norma společné požadavky na komponenty různých typů poplachových systémů. Uvedená norma definuje požadavky na jednotlivé typy zkoušek vlivu prostředí, které jsou aplikovatelné na komponenty poplachových systémů. Jde např. o provozní a odolnostní zkoušky proti vlivům jako jsou suché teplo, vlhké teplo, vniknutí vody, údery, rázy, vibrace atd.[5]

1.2.5 ČSN CLC/TS 50389

Jedná se v současné době o jedinou technickou normu řešící vzájemné propojení poplachových a nepoplachových aplikací. Mezi poplachové aplikace jsou zařazeny všechny poplachové systémy a dále rovněž i systémy elektrické požární signalizace a poplachové systémy výtahů. K nepoplachovým aplikacím patří například systémy:

- osvětlení, vytápění,
- klimatizace, ventilace,
- zavlažování, vysoušení,

- správa budov, řízení elektrických systémů,
- dopravní aplikace,
- zemědělské aplikace.

Norma řeší následující problematiku:

- definice základních pojmů,
- popis základních typů konfigurací integrovaných poplachových systémů,
- systémové požadavky,
- dokumentace a školení,
- použití, montáž a spolehlivost integrovaných poplachových systémů. [6]

1.3 Klasifikace systémů kontroly vstupu

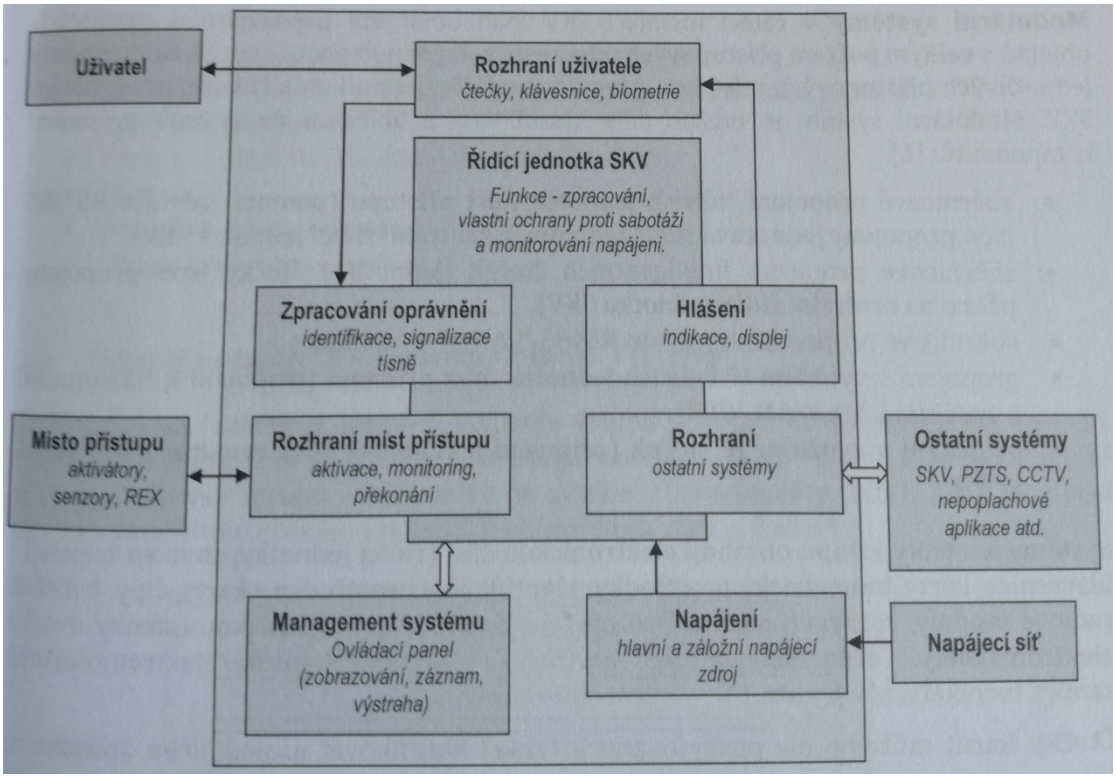
Veškeré požadavky na činnost zařízení systémů kontroly vstupu musí být konstruovány podle stupňů, odpovídajících úrovní ochrany. Toho je dosaženo pomocí klasifikací funkcí majících vztah k bezpečnosti ve vztahu k úrovni rizika. Klasifikace systémů kontroly vstupu jsou určeny jedním ze čtyř stupňů, kde stupeň 1 je nejnižší a stupeň 4 nejvyšší. Klasifikace je definována individuálně pro každé místo přístupu pro vstup i výstup. V celé instalaci je možné pro rozhraní přístupových míst použít různé stupně pokud funkce poskytování systémem kontroly vstupu a ověřovací prostředky splňují alespoň požadavky nejvyšší bezpečnostní klasifikace přístupových míst kontrolovaným tímto systémem. Úroveň rizika je stanovena na základě hodnoty majetku, který má být chráněn a odhodláním a způsoby útoku osob, zamýšlející obejít systém kontroly vstupu. V následující tabulce budou zobrazeny všechny stupně klasifikace. [2]

Tab. 2. *Stupně klasifikace* [2]

Stupeň	1	2	3	4
Úroveň rizika	Nízké	Nízké a střední	Střední až vysoké	Vysoké
Aplikace	Organizační prostředky, ochrana majetku nízké hodnoty	Organizační prostředky, ochrana majetku nízké a střední hodnoty	Méně organizačních prostředků, ochrana komerčních prostředků střední až vysoké hodnoty	Zejména ochrana komerčních prostředků velmi vysoké hodnoty nebo kritické infrastruktury.
Dovednosti / znalosti pachatelů	Malá dovednost, malá znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií, malé finanční prostředky pro napadení	Střední dovednosti a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií, malé až střední finanční prostředky pro napadení	Velká dovednost, malá znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií, střední finanční prostředky pro napadení	Velmi vysoká dovednost a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií, velké finanční prostředky pro napadení
Typické příklady	Hotel	Obchodní kanceláře, malé firmy	Průmysl, administrativní prostory, finanční instituce	Vysoce citlivé prostory (vojenské zařízení, vládní budovy, výzkum a vývoj, kritická infrastruktura

1.4 Struktura systémů kontroly vstupu

Struktura systémů kontroly vstupu je v podstatě odvozena z jeho základních funkcí, které se vztahují k uživatelskému systému, managementu systému, místům přístupu a k ostatním systémům. Zahrnuje všechny konstrukční a organizační prostředky a zařízení, které jsou požadovány po systémech kontroly vstupu. Základní architektura je na obrázku níže, kde je blokově zobrazeno její základní složení. [1]



Obr. 1. *Architektura systémů kontroly vstupu* [1]

S poskytovanými funkcemi a v souladu s architekturou je struktura systémů kontroly vstupu tvořena následujícími prvky:

- místa přístupu (portály) včetně senzorů a aktivátorů,
- zařízení pro vyžádání odchodu,
- rozhraní místa přístupu,
- rozhraní uživatele (čtečky, klávesnice, biometrie),
- řídící jednotka kontroly vstupu,
- napájení (lokální, centrální),
- komunikační síť (bezdrátová smyčková, sběrnicová),
- management systému (řídící a obslužné pracoviště). [1]

Podle velikosti a topologie lze systém kontroly vstupu rozdělit na dva typy a to autonomní a modulární systémy. [1]

- **Autonomní systémy** slouží k zabezpečení řízení a kontroly vstupu nebo výstupu z jednoho přístupového místa. Obsahem je jedno nebo dvě snímací zařízení např. (klávesnice, čtečka, biometrie) a řídící jednotka (dveřní jednotka). Tato jednotka bývá integrována uvnitř snímacího zařízení, nebo může tvořit samostatný modul.

Autonomní systémy jsou vhodné pro nízký počet samostatných míst přístupu v objektech, kde je zároveň nižší četnost pohybu osob. [1]

- **Modulární systémy** mají uplatnění v rámci instalací systémů kontroly vstupu především u rozsáhlých objektů s velkým počtem přístupových míst nebo velkým počtem uživatelů. Jednotlivé komponenty různých přístupových míst jsou propojeny s řídící jednotkou a řídícím pracovištěm. Dále je možno systém rozdělit podle způsobu propojení na:
    - sběrnicové propojení řídících jednotek míst přístupu pomocí např. RS 485,
    - sběrnicové propojení inteligentních čteček,
    - sběrnicové propojení s využitím RS485/LAN převodníků,
    - propojení s využitím IP řídících jednotek míst přístupu,
    - propojení s využitím IP čteček. [1]

Systémy kontroly vstupu obsahují také elektrickou část (řídící jednotky, snímací zařízení – klávesnice, karty, biometrické prostředky, identifikační prostředky – karty, čipy, kabeláž, rádiové moduly, rozhraní, napájecí zdroje) a část elektro-mechanickou (zámky dveří – elektromagnety, elektromagnetické otvírače, elektromechanické/elektromotorické zámky, turnikety, závory atd.) [1]

Dále pak můžeme rozdělovat čtečky karet podle způsobu poskytovaných funkcí na základní čtečky, polointeligentní čtečky, inteligentní čtečky.[1]

V rámci procesu identifikace uživatele se rozděluje do tří skupin a to:

- znalosti (heslo, kód, kontrolní otázka),
- vlastnictví (karta, čip, ovladač atd.),
- biometrické charakterizace.

Podle identifikačních prvků a tím zároveň i čteček rozlišujeme následující typy na manuální, čipové, magnetické, optické, radiofrekvenční, biometrické. [1]

1.5 Dílčí závěr

Systémy kontroly vstupu jsou složeny z mnoha prvků a můžeme je rozdělit na systémy autonomní a modulární. Jejich složení je v základu odvozeno z jeho základních funkcí. V současné době jsou systémy kontroly vstupu ošetřeny technickými normami ČSN EN 60839-11-1 a ČSN EN 60839-11-2, které jsou přejaty z evropských norem. Tyto normy stanovují některé nové podmínky pro tyto systémy. Další normy, které se týkají systému kontroly vstupu, se vztahují k integraci s jinými systémy a posléze na technické podmínky jednotlivých prvků.

2 TECHNOLOGICKÉ TRENDY

U systémů kontroly vstupu se největší technologický posun odehrává ve stylu identifikace daného uživatele a jejího ověření. Identifikace daného uživatele se dá rozdělit do tří oblastí. Na identifikaci pomocí hesla nebo PINu, tedy podle toho, co si daný uživatel zapamatuje. Dále na identifikaci pomocí předmětu a posléze na biometrickou identifikaci. Samozřejmě vždy je nejúčinnější kombinace všech tří. Další technologický posun se odehrává s vývojem IT technologií. To lze nejvíce vidět tak, že při instalaci se přechází z drátového na bezdrátové zapojení. Nelze také opomenout, že v současné době probíhá integrace s ostatními systémy, a to jak hardwarová tak softwarová.

2.1 Identifikace pomocí hesla a PINu

Jedná se o nejstarší a nejrizikovější, ale také o nejjednodušší metodu identifikace. Ta je jasně vázána na paměť nositele. Jde o posloupnost znaků, kterou je nutno zadat do přístupové jednotky (klávesnice). U klávesnic jde většinou o číselné kombinace pevně dané délky. Porovnává se shoda zadaného s databází povolených přístupů. [7]

Heslo bývá typicky řetězec dlouhý 6-10 znaků. V ideálním případě netriviální, ale uživatelem snadno zapamatovatelný. Zadává systému heslo společně se svou identifikací, tzv. uživatelským jménem. Systém dané údaje kontroluje s daty uloženými k určitému uživateli. Obyčejní uživatelé si většinou neuvědomují (ne)bezpečnosti, kterou jejich hesla představují. Moderní systémy proto umožňují kontrolu bezpečnosti vkládaných hesel, příp. vygenerují heslo s požadovanými parametry. Negativní stránkou ale je, že uživatel si heslo bude obtížněji pamatovat a často zapomínat. Jako bezpečné heslo považujeme takové heslo, jehož prolomení obvyklými technikami je časově náročné. Obvykle se proto jedná o řetězec s délkou 8-12 znaků, který musí obsahovat znaky z více různých skupin (malá i velká písmena, číslice, další tisknutelné znaky) Důležité pro taková hesla je, že není v dostupných slovnících. [7]

PINy poskytují jinou možnost přístupu. Zde se omezuje počet pokusů, které má daný uživatel k dispozici pro zadání hodnoty PINu. Pokud se v určeném počtu pokusů netrefí, tak systém PIN zablokuje. Pro odblokování je nutné použít nějaký složitější mechanizmus, a tím vynulovat počet chybných pokusů. Tento druhý mechanizmus může mít mnohem delší PIN (PUK), nebo v mnoha případech nejpoužívanější časový úsek, po kterém lze

znovu PIN zadat. Proto je možné značně zjednodušit délku a formu PINu oproti heslu. Klasický PIN je složen pouze z číslic a bývá dlouhý 4-8 znaků. [7]

Identifikaci podle hesla a PINu můžeme také rozdělit do dvou skupin, a to podle toho že:

- **Heslo, PIN je přidělen skupině lidí**, kteří získávají oprávněný přístup do objektu. Může se jednat o zaměstnance jednoho pracoviště, obyvatele domu, apod. Značnou nevýhodou je, že nelze provést zpětně kontrolu, kdy který zaměstnanec vstoupil nebo odešel z objektu. [8]
- **Každá oprávněná osoba má přiděleno heslo, PIN**, díky němuž lze zpětně zjistit příchod a odchod jednotlivých osob. [8]

2.2 Identifikace předmětem

Může jít o kartu, přívěšek apod., tedy o jisté identifikační medium, kterým se jednotliví uživatelé prokazují identifikačnímu systému. Vždy je toto medium jedinečně přiřazeno určité osobě. Pro výběr typu nosiče informací v kombinaci se snímacím zařízením je potřeba dbát na následující aspekty, a to na:

- bezpečnost vložené informace,
- bezpečnost přenosu,
- spolehlivost identifikace,
- mechanická trvanlivost, životnost, opotřebení,
- kapacita pro případné uložení informace. [8]

2.2.1 Magnetický systém

Používají se karty o velikosti standardních kreditních karet. Jiný tvar zde není prakticky možný, protože při čtení dat musí být karta protažena čtecí hlavou. Karta je tvořena magnetických proužkem, který obsahuje údaje o kartě a uživateli. Tyto karty mají informace uložené na magnetické pásce, která zároveň slouží jako paměťová karta. Při protažení karty čtečkou dochází nejprve ke zmagnetizování, vytvoří se množství malých permanentních magnetů, a poté stav těchto magnetů tvoří jednoduché binární rozhodování. A to tak, že zmagnetizování tvoří logická 1, nezmagnetizování tvoří logická 0. [9,10]

a) Karty s magnetickým pruhem HiCo (High Coercivity)
   Umožňuje vysokou hustotu záznamu. Magnetické karty s tímto pruhem se používají jako věrnostní nebo slevové, jelikož se na tyto karty dají nahrávat určité informace. Také slouží jako identifikační médium pro systémy elektronické kontroly vstupu. Nespornou výhodou je především nízká pořizovací cena a snadná identifikace. Zápornou stránkou těchto karet je jejich snadná zničitelnost, možnost poškození magnetického pruhu. [9]
b) Karty s magnetickým pruhem LoCo (Low Coercivity)
   Mají nízkou hustotu záznamu. Jsou stejné jako karty s magnetickým pruhem HiCo. Lze nahrávat informace, které se týkají uživatele karty. Kartu je možno nahrát podle přání uživatele. [9]

Podle normy ISO 7811, existují 3 stopy magnetického záznamu:

- **1 stopa** (IATA) - má 79 znaků, dají se na ní nahrát jen alfanumerické znaky.
- **2 stopa** (ABA) - má 40 znaků, dají se na ní nahrát jen číslice 0-9 a rovnítko.
- **3 stopa** (THRIFT) - má 107 znaků, využívá se k bankovním účelům pro uchování PIN, dají se nahrát jen číslice 0-9, rovnítko, dvojtečka. [9]

Výhodou je, že data jsou dynamická, uložená data jdou kdykoli přepsat nebo aktualizovat. Životnost je poměrně vysoká, udává se 5 až 6 let. Další výhodou je jejich ekonomická nenáročnost. Mezi nevýhody lze určitě zařadit možnost poškození dat při vystavení silnému magnetickému poli, nebo při poškrábání magnetické vrstvy. Karta se stane nečitelnou a je nutné ji vyměnit. Velkou nevýhodou magnetických karet je jejich bezpečnost, protože ji lze bez velkých problémů přečíst a vyrobit duplikát. Čtečky se rozdělují podle toho, ze které stopy je informace sejmuta, a to pro první, druhou nebo třetí stopu. Podle toho se dělí čtečky na jednostopé, dvoustopé a třístopé. [9,10]

2.2.2 Optický systém

Používá se zde jako identifikační prvek běžný čárový kód. Cena těchto karet s čárovým kódem je v podstatě zanedbatelná. Nevýhodou je, že pro okopírování karty stačí obyčejná kopírka, nelze tedy hovořit o jakémkoliv zabezpečení. Mechanicky opotřebit kartu je velmi malá šance. Cena snímače, jeho umístění a použití je stejné jako u magnetického systému. Principem identifikace je, že v kódu je uložena číselná hodnota, která je posléze nalezena v databázi. Čtení kódů probíhá za pomoci laserového paprsku. Šířka v podélném směru ukazuje pro čtečku logickou informaci. Snímač vyšle světelný paprsek a sledu-

je, zda je odražen na bílém pozadí nebo pohlcen černým proužkem. První a poslední proužky slouží k synchronizaci. Nejpoužívanějšími typy čárového kódu jsou EAN 8, EAN 13, CODE 39, CODE 128, CODABAR, atd. Čárové kódy mohou být zamaskovány speciální barvou, pak je čitelný pouze infračerveným paprskem. Podle principu snímání čárového kódu rozlišujeme snímače na laserové a digitální. Klasické laserové snímače pracují na výše popsaném principu. V nedávné době se ale začaly používat snímače digitální. Ty fungují na podobném principu jako digitální fotoaparáty. Nejdříve dojde k vyfocení čárového kódu. Následně se jeho obsah dekóduje pomocí dekodéru, který je součástí snímače. Velkou výhodu u digitálních snímačů je, že umožňuje více směrné čtení jak 1D, tak i 2D symbolů. [9]

2.2.3 Kontaktní systém

Při provádění autentizace je potřeba kontaktu identifikačního média a čtečky. Mívají nejčastěji podobu kovového pouzdra nebo kreditní karty, které jsou opatřeny kontaktním polem. Při kontaktu dojde k zapojení čipu do obvodu, a poté může probíhat obousměrná komunikace. [9]

2.2.3.1 Čipové karty

Používají se jako kontaktní médium. Může se jednat o jednoduché paměťové karty pro autentizaci nebo předplacené telefonní karty až po multiaplikační kartu s mikroprocesorem a kryptoprocesorem pro náročné aplikace. Čipové karty jsou velmi bezpečné a spolehlivé médium, které uchovává přístup k informacím uložením na čipu karty. Tyto karty umožnují uložit velké množství dat, a proto na těchto čipech může probíhat více aplikací najednou. U systémů kontroly vstupu jsou méně používané, ale častěji se využívají v informačních technologiích (přihlašování k počítačové síti, k PC, apod.). V dnešní době se zásadně využívají standardní karty splňující požadavky ISO 7816-1. Jsou vyráběny ve dvou provedeních. Tím větším jsou běžné platební karty a malý rozměr mají SIM karty mobilních telefonů. Je zde možnost vytvořit tzv. hybridní kartu, která umožňuje různě kombinovat datová média na kartě, a tak využívat výhody každého z nich. Příkladem může být karta s kontaktním a bezkontaktním čipem nebo karta s kontaktním čipem a magnetickým proužkem, atd. [9,10]

Na světovém trhu existuje celá řada výrobců kontaktních čipů, které lze implementovat do plastové karty. Tyto čipy jsou vyráběny s různými parametry podle druhu a náročnosti aplikace. Paměťové karty se mohou používat jako identifikační karty, předplacené telefonní karty, elektronická peněženka, přístupové systémy, karty zdravotních pojišťoven, elektronické jízdné, členské a klubové karty. Mikroprocesorové karty se používají jako bankovní karty, elektronické peněženky, GSM karty, ve zdravotnictví, předplacené TV a satelit, multifunkční karty. Výhodou použití čipové karty je velká rozšířenost systému a podpora řady výrobců, vysoká bezpečnost, možnost uložení značného množství dat, možnost běhu více aplikací na jednom čipu. Nevýhodou použití čipové karty je, že se v podstatě jedná o kontaktní řešení, a také možnost mechanického poškození čipu. [9]

2.2.4 Bezkontaktní systém

V současné době se jedná o nejpoužívanější metodu autentizace osob před vstupem do objektu. Je založena na radiovém přenosu dat mezi identifikačním médiem a čtečkou. Technologie, kterou se radiofrekvenční komunikace provádí, se jmenuje RFID (Radio-Frequency Identification). Informace jsou ukládány v elektronické podobě do malých čipů neboli tagů či transpondérů, ze kterých následně může probíhat čtení pomocí radiových vln. V podstatě jde o bezkontaktní paměťové prvky, které se vyznačují tím, že nepotřebují při identifikaci pevný kontakt se čtečkou, komunikace probíhá pouhým přiblížením. Obvykle je vzdálenost potřebná k přečtení informace z média asi 5 – 10 cm, lze dosáhnout i větší vzdálenosti. Čtečky jsou standardně napájeny 12 V, pro čtení na větší vzdálenost mohou vyžadovat i 24 V. Celý systém pracuje jako dvouanténní, jedna anténa je umístěna v transpondéru a druhá je připojena ke snímači. Transpondéry bývají v různém provedení, většinou jsou ale podle charakteru aplikace (např. karty velikosti kreditních karet, přívěsky, plastové disky, atd.). [9,10]

Princip spočívá v tom, že čtečka neustále vysílá na svém nosném kmitočtu elektromagnetickou vlnu, která je přijata anténou transpondéru za dodržení podmínky, že obě antény, čtečky i transpondér jsou naladěny na stejnou frekvenci. Indukované napětí posléze vyvolá elektrický proud, který je usměrněn a nabíjí kondenzátor v transpondéru. Přibližně tato akce trvá cca 50 milisekund. Uložená energie je použita pro napájení logických a rádiových obvodů transpondéru. Po dosažení minimální potřebné úrovně napětí na kondenzátoru, transpondér začne odesílat odpověď čtečce. Čtečka signál upraví na plně digitální

elektrický signál a předá do systému k dalšímu zpracování, kde se rozhodne v našem případě o vpuštění osoby do objektu. Doba identifikace obvykle netrvá déle než 100 – 120 milisekund. [9,10]

Transpondéry mohou být vyrobeny v mnoha provedeních lišících se jak tvarem, tak i funkcí. Co se týče funkce, existují typy určené pouze pro čtení uloženého kódu (R/O transpondéry), stejně jako typy s možností naprogramování kódu vlastního o délce 64 bitů do interní EEPROM (R/W transpondéry). [9,10]

- **R/O transpondéry** jsou užívány jako jedinečné a nekopírovatelné. Obsahují unikátní kód, neexistují tedy dva stejné transpondéry. Tyto prvky jsou široce použitelné u všech aplikací zabývajících se velkými databázemi s nezáměnnými položkami. [9,10]
- **R/W transpondéry** mají možnost také mimo jiné ukládat data. Mohou být programovány, čteny a měněny prakticky neomezeně. Programování se provádí rovněž bezkontaktně. Uživatel si tak může sám tvořit kódy ke snadné integraci s jeho počítačovým systémem zpracování dat. [9,10]

Pro systémy kontroly vstupu se nejčastěji používá kmitočtu 125kHz a 13,56MHz. Transpondéry, které obvykle pracují s kmitočtem 13,56 MHz, mají rychlý cyklus čtení. Zápis je rychlý přibližně 20kB/sec, což je asi 10 x rychlejší než u čipů s frekvencí 125 kHz. Mají kratší reakční dobu a vysokou bezpečnost přenosu. Většina technologií funguje antikolizně, to znamená, že pokud se dostane více čteček do čtecího dosahu, vzájemně se neruší. [9,10]

2.2.4.1 Technologie NFC

Near Field Communication (NFC) je nejnovější technologie, která zaručuje komunikaci mezi dvěma zařízeními na velmi krátkou vzdálenost. Jde v podstatě o rozšíření a kombinaci několika již existujících standardů pro bezdrátovou komunikaci. Společnosti Philips a Sony byly původními tvůrci technologie NFC, později však byly přijaty organizacemi ISO/IEC jako standardy. V současné době jsou NFC technologie standardizovány sdružením NFC Forum, které mimo jiné specifikuje komunikační protokoly, formáty dat a typy tagů. Fyzické charakteristiky komunikace jsou specifikovány ve standardech ISO/IEC 18092 (NFCIP-1) a ISO/IEC 21481 / ECMA-352 (NFCIP-2). Ke komunikaci se využívá elektromagnetické vlny na frekvenci 13.56 MHz, tedy na jedné z frekvencí vy-

užívaných technologií RFID. Data jsou přenášena na maximální vzdálenost přibližně 10 cm, při maximální rychlosti přenosu 424 kb/s. [11]

Základní charakteristikou a výhodou technologie NFC je implicitní párování, kdy díky nízké vzdálenosti přenosu, a tedy nutnosti komunikující zařízení přiblížit fyzicky k sobě, odpadá nutnost ručního nastavování a potvrzování spojení. Z toho vyplývá, že je zajištěna implicitní bezpečnost komunikace, protože odposlouchávání přenosu je vzhledem k nízkému dosahu velmi obtížné. [11]

NFC zařízení se dělí na dva druhy: aktivní a pasivní. Aktivní zařízení obsahují anténu a vlastní zdroj energie a generují elektromagnetické pole. Mezi aktivní zařízení můžeme zařadit NFC čtečky a mobilní NFC zařízení. Pasivní zařízení také obsahuje anténu, neobsahují však vlastní zdroj energie, tu získává pomocí elektromagnetické indukce v poli generovaném aktivním zařízením. Pasivní NFC zařízení se nazývají NFC tagy. [11]

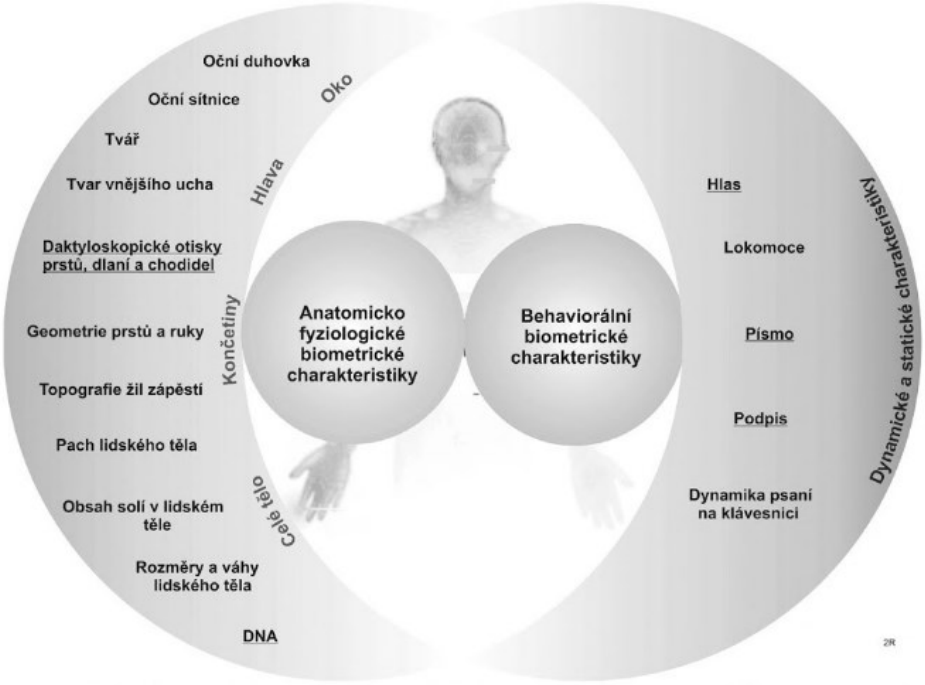
NFC definuje tři režimy komunikace: režim čtení a zápisu pro komunikaci mezi aktivní čtečkou a pasivním tagem, režim peer-to-peer pro komunikaci mezi dvěma aktivními zařízeními a režim emulace karet pro emulaci pasivního tagu aktivním zařízením.[11]

2.3 Identifikace biometrií

V minulosti byla vždy biometrická identifikace spojována a policejně-soudními a bezpečnostními aplikacemi. Teprve v současné době nachází své uplatnění i v civilní a komerční sféře. Až současný technologický rozvoj umožnuje úplné uplatnění biometrické identifikace ve všech směrech lidské činnosti. Mezi hlavní výhody bezesporu patří to, že ji nelze zapomenout nebo ztratit. Je těžké ji odcizit, napodobit nebo jakkoliv přenést, tedy nemůže být sdílena jinou osobou. Dále je to vysoká přesnost a rychlost identifikace a velmi snadná a rychlá použitelnost. Identifikace osoby založená na vlastnictví nebo znalostech je z mnoha důvodů již téměř vyčerpaná, a proto také zranitelná. Oproti tomu se stane biometrická identifikace v nejbližších letech jedním z nejdynamičtěji se rozvíjejících oborů informačních technologií. [12]

Biometrická identifikace/verifikace je definována jako využití jedinečných, měřitelných, fyzikálních a fyziologických znaků nebo projevů člověka k jednoznačnému zjištění (identifikaci) nebo ověření (verifikaci) jeho identity. Pro účely identifikace se používají anatomické nebo fyziologické charakteristiky, které jsou pro každého člověka unikátní

a časově neměnné. V bezpečnostně-komerčních aplikacích spíše převládá verifikace nad identifikací. To znamená, že uživateli je buď povolen anebo odmítnut přístup do chráněných objektů. Veškeré biologické znaky, které jsou v oblasti bezpečnostních technologii měřeny, jsou zobrazeny na obrázku níže. [12]



Obr. 2. *Základní rozdělení biometrické identifikace* [12]

2.3.1 Otisky prstů

Snímání otisků prstů patří historicky k nejstarší biometrické metodě. Pro urychlení a zkvalitnění identifikace osob byla využita výpočetní technika takřka v celosvětovém měřítku. Princip spočívá v tom, že osoba požadující vstup do určitého objektu položí prst na snímací senzor, ten sejme otisk a vzápětí následuje verifikace. Snímací senzory lze rozdělit podle kontaktu snímaného povrchu tkáně na kontaktní a bezkontaktní. Kontaktní senzory zahrnují mnoho fyzikálních způsobů snímaní otisků prstů. Patří sem senzory optické, elektrické, opto-elektrické, kapacitní, tlakové a teplotní. [12]

Optické senzory pracují na technologii FTIR – Frustrated Total Internal Reflection. Laserový paprsek zespodu osvětluje povrch prstu, který se dotýká průhledné desky senzo-

ru. Odražený světelný tok je snímán CCD prvkem. Množství odraženého světla záleží na papilárních liniích a brázdách. Linie odrážejí světlo více, brázdy méně. [12]

Elektrické senzory pracují na principu vzniku elektrického pole mezi dvěma paralelními vodivými a elektricky nabitými deskami. Horní desku elektronického senzoru tvoří povrch kůže, do kterého je pouštěn řídící elektrický signál. [12]

Kapacitní senzory byly navrženy pro snímaní otisku prstu za pomoci měření elektrické kapacity. Senzor je tvořen z velkého počtu vodivých ploch, které jsou mezi sebou odizolovány. Dotykem kůže papilární linie přemostí jednotlivé vodivé plošky v závislosti na jejich tvaru, zatímco brázdy se chovají jako izolant. Měří se napětí a kapacitní úbytek mezi jednotlivými vodivými ploškami. [12]

Tlakové senzory reagují na tlak papilárních linii na povrch snímacího senzoru. Povrch je tvořen elastickým, piezoelektrickým materiálem, který tlak papilárních linií transformuje do elektrického signálu, a tak vytvoří obraz daktyloskopického obrazu. [12]

Mezi nejznámější bezkontaktní senzory patří bezesporu optické a ultrazvukové. Optické senzory fungují na stejném principu jako kontaktní senzory. Rozdíl je ale v tom, že dokáží snímat na vzdálenost 30 až 50 mm. Tím je eliminováno znečištění snímacího senzoru. [12]

Senzory ultrazvukové jsou také založeny na podobném principu jako optické senzory. Na povrch kůže dopadá krátkovlnný svazek, který se odráží od povrchu. Papilární linie a brázdy ovlivňují odražený paprsek, který je vyhodnocován. Tento princip lze přirovnat k velmi citlivému sonaru. Ultrazvukové senzory jsou výhodné v tom, že odstraňují některé nedostatky ostatních metod snímání, zejména optických. [12]

2.3.2 Geometrie ruky

Metoda verifikace geometrie ruky je založena na principu, že i lidská ruka je do určité míry jedinečná. Kombinací délky, šířky a tloušťky měřené na všech pěti prstech jedné ruky zjistíme, že jejich tvar a rozměry jsou jedinečné, a proto lze na jejich základě založit velmi přesnou verifikaci osob. [12]

Třírozměrné moderní skenery snímají geometrické charakteristiky v desítkách bodů během několika sekund. Ruka se klade na horizontální plochu skeneru, opatřenou speciálními fixačními kolíčky, a to z toho důvodu, aby byla poloha ruky pokud možno vždy stejná. Pro osvit se používá infračervené LED diody. Pomocí soustavy zrcadel pak umožnuje-

me odraz obrazu do snímací kamery. Aby byl odražený obraz jasný a konstantní, základová deska je tvořena z leštěného materiálu, který má velkou optickou odrazivost. Vlastní snímaní je obvykle realizováno CCD digitální kamerou a přibližně 32 000 body. Skener snímá pouze siluetu dlaně s prsty, ne však otisky jednotlivých prstů jizvy nebo barvu ruky. Snímaní se provádí černobíle a připomíná promítání ruky položené na desku zpětného projektoru. [12]

Biometrická metoda geometrie ruky je používaná výhradně v komerčně-bezpečnostní sféře v režimu verifikace. Jelikož metoda neposkytuje mnoho informací, nelze ji použít k identifikaci. Používá se jako prostředek pro rychlou verifikaci v prostorech s omezeným a známým počtem lidí uvnitř určitého areálu. Mezi typické oblasti, ve kterých se skener používá, patří všechna režimová pracoviště (průmyslová, vojenská, bezpečnostní), výrobní závody, obchodní domy, sklady, hraniční kontroly, věznice, zdravotnictví atd. [12]

Nespornou výhodou geometrie ruky je, že tato metoda je uživatelsky i technologicky velice jednoduchá a rychlá. Dalším příznivým faktorem je velice malá velikost referenční šablony, která má hodnotu pouhých 9 bytů. To je s porovnáním s metodou otisků prstů, která má šablonu o velikosti 250 až 1000 bytů, nesporná výhoda. [12]

Nevýhoda této metody spočívá v tom, že přesnost je poměrně nízká. Dále může být náchylná na vytvoření třírozměrného padělku tvaru dlaně a prstů. Skener je též citlivý na jakékoliv poranění nebo fyzické změny snímané charakteristiky (amputace prstů). Určitou nevýhodou je také práce v externích venkovních podmínkách (venkovní teplota, vlhkost, přímé sluneční světlo. [12]

2.3.3 Tvář

Biometrická identifikace osoby na rozpoznání její tváře má ve srovnání s metodou otisků prstů nebo oční duhovky nižší identifikační jednoznačnost. Metoda je založena na bezkontaktním snímání i na poměrně velkou vzdálenost. V bezpečnostní praxi si pozorované objekty vůbec neuvědomují, že se staly předmětem zájmu o svou osobu. Skrytost a utajená činnost je v tomto případě jeden ze zákonných požadavků bezpečnostních služeb pro jejich efektivní a bezpečnou práci. [12]

Počítačová identifikace osoby podle její tváře má dvě základní etapy. V první etapě probíhá na scéně detekce a lokalizace tváře. Scénou může být fotografie s několika osoba-

mi nebo reálná situace zaznamenaná pomocí kamery. V druhé etapě probíhá automatické nalezení základních identifikačních charakteristik a samotná identifikace (rozpoznání již známé tváře z minulosti). [12]

Na počítačové rozpoznání tváře existuje velké množství metod a algoritmů. Rozdělení těchto metod do určitých kategorií závisí na odlišných klasifikačních kritériích. Z pohledu formy zpracovaného obrazu můžeme rozlišovat 2D a 3D obrazy. Z hlediska spektra na černobílé, barevné nebo infračervené obrazy a jejich kombinace. V závislosti na způsobu snímání obrazu rozlišujeme čelní pohledy, pohled z boku, obecné pohledy a jejich kombinace. Z časového hlediska můžeme rozpoznávat statické obrazy nebo dynamické obrazy. Z hlediska použitých výpočetních nástrojů při zpracování rozlišujeme počítačové technologie založené na znalostních pravidlech, pravidlech statického rozpoznání, neuronových sítích, genetických algoritmech apod. [12]

Jednou za staticky orientovaných metod je metoda podprostoru. Cílem je nalézt v obrazu tváře obecné a přitom markantní charakteristiky typické pro lidskou tvář. Jestliže je nalezneme v obraze, můžeme konstatovat, že vyhodnocovaný obraz je obraz tváře. [12]

Mezi znalostní metody pak můžeme zařadit metodu na rozpoznání obličejových obrysů. Obrysy neboli kontura je další důležitou charakteristikou tváře. Pokud definujeme přesné a konkrétní obrysy tváře, další detekce je podstatně jednodušší. Často si však nemůžeme být zcela jistí, jelikož současné algoritmy na detekci hran mají své omezení. Detekce kontur se používá k nalezení jednotlivých objektů tváře jako oči, nos, ústa. Obrysy kontury hrany objektů lze obecně nalézt pomocí tzv. párování, detekce hran, segmentace narůstáním oblastí, segmentace srovnáním se vzorem apod. [12]

Metody neuronových sítí lze rozdělit do dvou základních kategorií. V první kategorii jsou identifikační charakteristiky rozpoznány nejrůznějšími metodami a metoda neuronových sítí je použita pouze pro rozpoznání tváří. Ve druhé kategorii metody neuronových sítí slouží jak pro určování jednotlivých identifikačních charakteristik, tak i pro závěrečné rozpoznání. Základní princip této metody spočívá v tom, že je charakterizováno 50 základních komponent tváře, které jsou zobrazeny do pětirozměrného prostoru s autokorelační neuronovou sítí. Ve druhém rozhodovacím procesu se používají vícevrstvé rozhodovací mechanismy. [12]

Budoucnost technologického zpracování obrazu lidské tváře není jen v dokonalé identifikaci osoby. Tvář poskytuje daleko více informací než jen fyzická identita. Lidská

tvář také odráží emoce. Identifikace osoby se tak v obecné rovině rozlišuje na vnější projevy a pocity. Odtud je jen krůček k identifikaci vnitřního, emocionálního, duševního stavu lidí. Lze předpokládat, že tímto směrem se bude rozvíjet i vědecké poznání a jejich důsledky lze nyní jen těžko odhadnout nebo domyslet. [12]

2.3.4 Oční duhovka

Identifikace oční duhovky se provádí tam, kde potřebujeme bezchybně prohledávat rozsáhlé databáze, zde je jinak pravděpodobnost chybných srovnání velká. I přes malou velikost (11 mm) a někdy problematické snímání má obrovskou výhodu, neboť variabilita očních duhovek mezi jednotlivými osobami je nesmírná. Jako interní orgán oka je dobře chráněna před vnějším prostředím a je stabilní v čase. Jelikož se jedná o dvourozměrný objekt, je její snímaní relativně nezávislé na úhlu osvětlení a změny v úhlu pohledu znamenají pouze afinní transformace. Složitý vzor duhovky může obsahovat mnoho charakteristických znaků, jako například klenuté vazy, rýhy, hřebeny, krypty, prstence, korány, pihy a klikaté čáry. Barva duhovky je dána především hustotou melaninového pigmentu.[12]

Aby byly zachyceny bohaté detaily vzoru duhovky, obrazový systém by měl poskytovat snímek alespoň o minimálním rozměru 70 pixelů. Využívají se monochromatické CCD kamery, jelikož se využívá blízké infračervené pásmo o vlnových délkách 700 nm až 900 nm, které je neinvazivní pro uživatele. Zaostřování obrazu se provádí v reálném čase měřením spektrálního výkonu ve středních a horních frekvenčních pásmech 2D Fourierova spektra. Snímky, které splňují minimální ostrost, jsou následně analyzovány na přítomnost duhovky. Provádí se hrubý odhad na přesný, končící u odhadu na jeden pixel a nacházející souřadnice středů a poloměry duhovky a zornice. [12]

Mnohé aplikace rozpoznávání duhovky jsou nasazeny pro zajištění vysoké úrovně bezpečnosti, jako např.: jaderné elektrárny, věznice, bankovní trezory a ostatní aplikace zaměřené na ochranu hodnotných a zranitelných aktiv. Jiné aplikace jsou však více domácího charakteru, včetně fyzického přístupu do domu a obytných budov a také logického přístupu do budov. [12]

2.3.5 Oční sítnice

Rozpoznávání osob pomocí oční sítnice se provádí identifikace osob na základě snímání a srovnání obrazu vzoru sítnice. Používá se speciální optická kamera k získání

obrazu cév. Danou osobu je možné verifikovat nebo identifikovat v rámci určité databáze osob. Pro osvětlení sítnice se používá infračervené světlo. Po použití tohoto světla je sítnice víceméně průhledná. Až na odraz sítě cév v choroidu, který se nachází za sítnicí, vytváří snímek sítnici, která se používá k rozpoznání osob. Proto označení „snímek sítnice“ je poněkud nepřesný, jelikož se nejedná o oční sítnici jako takovou, ale o *vzor cév za oční sítnicí*. Jelikož je toto označení všeobecně zaužívané používá se nadále. [12]

Biometrická identifikace na základě oční sítnice je velice přesnou metodou rozpoznání osob. Speciální kamera pro snímání vzorku sítnice je však relativně drahá a samotný snímač není příliš moc uživatelsky příjemný. Proto tato metoda nachází uplatnění především v oblastech využívající vysokou úroveň bezpečnosti bez ohledu na uživatelskou přívětivost. [12]

2.4 Kombinace metod

Nespornou výhodou použití kombinací identifikačních metod je, že umožňuje využít jednotlivé identifikace s cílem získat maximální bezpečnost chráněného objektu a maximální komfort pro uživatele. Je nutné také přihlédnout na prostředí, kde jsou metody užívány v kontextu s použitým fyzikálním principem snímání (vnitřní, venkovní, prašné, výbušné apod.). Nejpoužívanější a nejčastější je možnost setkat se s identifikací za pomocí kombinace předmětu a hesla, nebo předmětu a biometriky. Při kombinaci metod je důležité rozlišovat, zda hodláme mít přístup svázaný s vlastnictvím předmětu nebo s oprávněnou osobou.

2.5 Dílčí závěr

V oblasti docházkových a přístupových systémů se v současné době klade největší důraz na biometrickou identifikaci. Tato identifikace je u mnoha lidí považována za velmi bezpečnou, proto je v současnosti hodně využívána v kombinaci se stávajícími systémy, jako jsou například optické nebo bezkontaktní. Dá se tedy předpokládat, že se bude tato identifikace dále rozvíjet a budou se více využívat další biometrické metody oproti těm stávajícím. Momentálně se nejčastěji využívají biometrické metody, jako otisky prstů, oční sítnice a duhovky nebo geometrie ruky atd. V budoucnu se ale objeví i méně časté metody, jako identifikace podle hlasu, písma, podpisu, a dynamiky psaní na klávesnici atd. Tato oblast je nyní málo využívána, ale do budoucna by se měla více prosazovat, a to z důvodu, že je pro uživatele lépe přívětivá.

3 ANALYTICKÉ A PROGNOSTICKÉ METODY

Analytické a prognostické metody bývají nejčastěji využívány u bezpečnostního posouzení objektu. V této části si detailněji rozebereme používané metody jak analýz, tak prognóz. Jakákoliv použitá metoda není univerzální. Každá z metod je trochu odlišná, proto záleží na dané situaci, jakou metodu pro konkrétní situaci zvolit. [13,14]

Analýzu lze definovat jako proces, jejímž účelem je získávání, zkoumání a uspořádání informací pro určitý systém potřebný pro rozhodování o něm a o stanovených cílech. Analytické metody rozlišujeme na kvalitativní a kvantitativní. Vždy je třeba zvážit kvalitu vstupních údajů a posléze zvolit kategorii, z níž je pak nutné vybrat adekvátní metodu. [13,14]

Prognózu je možno chápat jako systematicky vydedukovaná a spolehlivě ohodnocená výpověď o budoucím stavu skutečnosti, která nastane za určitých podmínek a většinou i v určitém čase. Rozlišujeme dva druhy metod, a to metodu kvalitativní (naivní extrapolace, předpověď na základě konsensu, Delfský panel, historická analogie) a metodu kvantitativní (metoda extrapolace, regresivní analýza). Tyto metody nám přinášejí dílčí prognózy představující určitou strukturovanou výpověď o budoucnosti k vymezenému objektu a k určitému časovému horizontu. Kvalitativní prognostické metody vycházejí z vývoje společenských věd. Mnoha kvantitativních metod je založeno na tom, že budoucí vývoj je předvídatelným, a je přímým pokračováním již existujících trendů. [13,14]

3.1 Kvalitativní analytické metody

Hlavním účelem kvalitativních metod je určit priority mezi riziky, mírou ohrožení a zranitelností. Její výhodou je bezesporu jednoduchost a rychlost, ale to sebou nese také negativum, a to je subjektivita. Kvalitativní metody se převážně používají jako úvodní přehled, který pak vede k podrobnějšímu zkoumání. Dále v případech, kdy číselné údaje nebo zdroje nejsou dostatečné k provedení kvantitativní analýzy. Přístupy a metody jsou založeny na hodnocení využívající multioborové skupiny respondentů, hodnocení specialistů a expertů nebo strukturovaném interview a dotaznících. [13,14]

3.1.1 Metoda DELPHI

Jedná se o jednu z nejpoužívanějších metod analýzy rizik a můžeme ji řadit do metod expertního odhadování. Určuje, co se může stát a za jakých podmínek. Nevýhodou

může být její časová náročnost a nároky, které jsou kladené na organizaci. Výhoda je dána v menší náročnosti na spotřebu zdrojů a zohledňují se specifika posuzovaného informačního systému. Princip spočívá v řízeném kontaktu mezi experty hodnotící skupiny a představiteli hodnoceného subjektu. Skupina se skládá asi z deseti expertů. Pro rizikovou analýzu používá metoda soubor otázek, prodiskutovaných na účelových pohovorech, kdy tyto otázky jsou tvořeny pevnou částí a variabilní. Dále záleží na zachování anonymity mezi respondenty, a také na vhodném výběru respondentů, což je základem úspěšnosti metody. [14,15]

Princip metody spočívá v tom, že se ustanoví komise v počtu 3 – 5 členů, která řeší co nejpřesnější problém, který převede do formy dotazníku. Dále dochází k vyjádření expertů, což se několikrát zopakuje. Odpovědi jsou následně vyhodnoceny na shodné a odlišné názory. Výsledkem je zpracování konečné zprávy. [13,15]

3.1.2 Check List Analysis – Analýza pomocí kontrolního seznamu

Metoda je založena na systematické kontrole plnění předem stanovených podmínek a opatření. Seznamy kontrolních otázek (chcecklists) jsou tvořeny na základě charakteristik sledovaného systému nebo činností, které souvisejí s daným systémem a potenciálními dopady a vznikem škod. Struktura seznamu se může měnit od jednoduchého až po složitý, který umožňuje zahrnout různou důležitost parametru v daném souboru. Principem je ověřování stavu systému a posouzení shody s požadavky norem, úplnost vedené dokumentace pro provoz, její údržba atd. Identifikuje různé druhy ohrožení, odchylek od návrhů a možné nevhodné situace spojené s vybavením a řízením procesu. [13,14,15]

3.1.3 Whaf If – Co se stane, když?

Metoda využívá možnosti brainstormingu, tj. spontánní diskuse při poradách a hledání nápadů skupiny zkušených odborníků, kteří jsou dobře obeznámeni s procesem. Jde o postup, který podrobně rozebírá jednotlivé provozní situace za účelem nalézání potenciálních negativních dopadů. Metoda analyzuje ohrožující situace nebo havarijní události. Na základě daných informací lze stanovit předpokládané následky a posoudit již existující preventivní opatření a následně navrhnout varianty pro snížení rizika. Předpokladem pro úspěšnost metody je odpovídající znalost procesu a aktivní účast všech zúčastněných. Metoda je časově nenáročná, avšak předpokládá profesionalitu diskutérů. [13,14,15]

3.1.4 Preliminary Hazard Analysis (PHA) – Předběžná analýza ohrožení

Tato metoda má za cíl určit identifikaci a kategorizaci stavu ohrožení nebezpečných situací a událostí, jejich příčin a dopadů na jejich zařazení do kategorií předem stanovených kritérií. Zabývá se celou škálou technik pro posuzování rizik, a také kvantifikací zdrojů rizik. Metoda PHA specifikuje zaměřené postupy analýz rizik na daný systém, a to v případě, že rizika jsou natolik závažná, že je třeba hledat další způsoby minimalizace nebezpečí. Nesmíme podcenit žádné riziko ani v případě, že se nám osobně zdá být bezvýznamné či nedůležité. Proto je zde vhodné použít seznamy rizik. [13,14,15]

3.1.5 Event Tree Analysis (ETA) – Analýza stromu událostí

Jde o postup, sledující průběh procesu od iniciační události přes konstruování událostí, vždy na základě dvou možností příznivé nebo nepříznivé. Jedná se o graficko – statistickou metodu analýzy. Někdy je označována za metodu kvantitativní. Bývá tvořena grafem s dohodnutou symbolikou a popisem nebo názorně zobrazeným systémovým stromem událostí, který znázorňuje všechny potenciální události daného systému. Pokud počet událostí narůstá, výsledný graf se rozvětvuje jako větve stromu. Tato analýza je vhodná pro stávající systémy, které mají zavedený bezpečnostní systém či nouzový havarijní postup. Za její pomoci je možné sestavení modelových situací v časové závislosti mezi selháním a událostmi v posloupnosti nehod. [13,14,15]

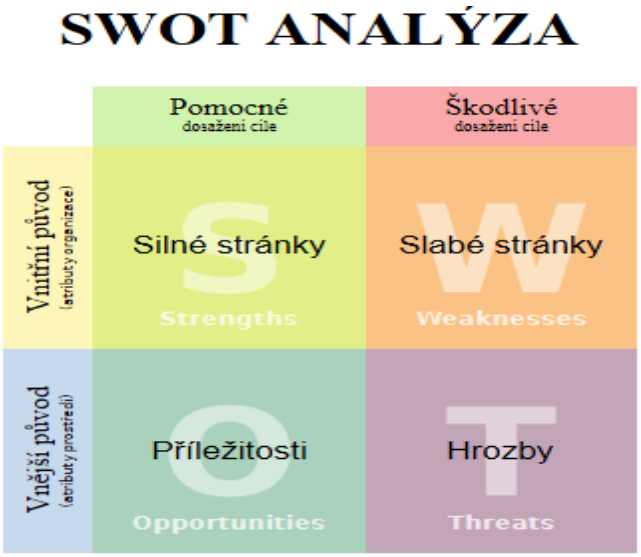
3.1.6 Safety Audit – Bezpečnostní kontrola

Jde o nejstarší metodu analýzy rizik, která hledá rizikové situace a navrhuje opatření pro zvýšení bezpečnosti. Metoda představuje postup hledání potenciálně možné nehody nebo provozního problému, který se může nastat. Využití je pro existující provozy zahrnující posouzení vybraných aspektů závodu, provozu a zařízení. [13,14,15]

3.1.7 SWOT analýza

Tato metoda je založena na identifikaci faktorů objektů, kterými jsou slabé stránky (Weaknesses), které mohou být překážkou při realizaci projektu a silné stránky (Strengths) lidské, věcné, finanční faktory. Dále jsou to příležitosti (Opportunities), kterých se využívá při optimálním řešení projektu a hrozby (Threats) jsou vnější faktory, které ohrožují cíle projektu. SWOT metoda je jednou z metod strategické analýzy výchozího stavu organizace. Základ metody je dán ohodnocením a klasifikací jednotlivých faktorů, které jsou rozděleny do čtyř základních skupin. Před zahájením sestavování SWOT analýzy je nutné určit

výchozí stav a provést jeho podrobnou analýzu a zařadit do jedné za čtyř základních skupin. K naplnění jednotlivých polí pro daný konkrétní subjekt je využíváno expertizních metod, jako je brainstorming, delphi, brainwriting nebo metoda psaní scénářů. SWOT analýza je užívaná především v marketingu, ale je také využitelná při tvorbě politiky, hlavně v bezpečnosti. [13,14,15]



Obr. 3. *SWOT analýza* [15]

3.2 Kvantitativní analytické metody

Kvantitativní metody bezpečnostní analýzy jsou exaktní metody, které jsou založeny na systematickém postupu numerického vyčíslení očekávané frekvence a následků potencionálních havárií spojených se zařízením na odhadu, vyhodnocení a matematických metodách. Nevýhodou je náročnost na čas a obsah vstupních dat. Tvořeny jsou ze dvou kroků, a to pravděpodobnost výskytu jevu a pravděpodobnost ztráty. Kvantitativní analýza se provádí pomocí speciálních vypracovaných programů, jednoduché lze provádět „ručně“. [13,14,15]

3.2.1 FTA – Analýza stromem poruch

Je nejčastěji používanou metodou při kvantitativním hodnocení rizik, která byla zavedena v roce 1960. FTA je deduktivní technika analýzy a soustřeďuje se na jednotlivé havárie či poruchy systému, a tak poskytuje metodu pro určení příčin této události. Vý-

sledkem je strom poruch zobrazující vztahy mezi základními událostmi a zvolenou vrcholovou událostí. [13,14,15]

3.2.2 QRA – Analýza kvantitativních rizik procesu

Umožňuje identifikovat a určit prioritu jednotlivých nebezpečí. Jedná se o systematický a komplexní přístup pro predikci odhadu četnosti a dopadů nehod pro zařízení nebo provoz systému. Nejčastější využití nachází především v oblasti bezpečnostních organizací, projektů a jejich informačních systémů a v jaderném průmyslu. Umožňuje identifikovat a určovat prioritu jednotlivých nebezpečí. Přínosem této metody je, že jednoznačně odhaluje zdroje rizika a na objektivním základě navrhuje potřebná opatření i s ohledem na efektivitu investic. [13,14,15]

3.2.3 HRA – Analýza spolehlivosti lidského činitele

Metoda se specializuje na posouzení vlivu lidského činitele na výskyt pohrom, nehod, havárií, útoků a některých jejich dopadů. Analyzuje systematické posouzení lidského faktoru a lidské chyby. HRA má úzkou vazbu s aktuálními pracovními předpisy a s požadavky na bezpečnost práce. Úkolem HRA je zcela identifikovat nežádoucí stavy a lidské selhání. Má základní čtyři procedury, a to vytyčení kritických míst systému, náročnost ovládání technologií z hlediska obtížnosti obsluhy, vypracování úkolové analýzy, hodnocení faktorů ovlivňujících lidskou spolehlivost. [13,14,15]

3.2.4 FMEA (Analýza selhání a jejich dopadů)

Je založena na principu modelování souvislostí popisující vztah „příčina – důsledek“ nebo „selhání – důsledek“. Používá se pro vážná rizika. Pro její použití se vyžaduje speciální výpočetní program. Doba a náklady analýzy jsou úměrné velikosti procesu a počtu analyzovaných komponent. Jedná se o tzv. týmovou metodu, protože se zde spolupracuje s odborníky výrobního procesu z různých úrovní řízení. Výsledkem hodnocení jsou číselné hodnoty, odrážející nebezpečnost dané události. [13,14,15]

3.3 Dílčí závěr analytických metod

Tato část se zabývá vybranými metodami bezpečnostní analýzy. Základem je rozdělení analýz na kvalitativní a kvantitativní metody. Kvalitativní metody stanovují priority mezi riziky, mírou ohrožení a zranitelností. Kvantitativní metody jsou časově náročné. Jsou zde popsány druhy metod a jejich princip fungování. Každá metoda je vhodná

pro jiný proces. V následující tabulce je vyhodnocení vybraných metod. Kde znaménko plus znamená kladné hodnocení a znaménko mínus záporné. [13,14]

Tab. 3. *Vyhodnocení vybraných analytických metod* [13]

Analytické metody	Kvantitativní	Kvalitativní		
		CHECK list	What if	SWAT
Výsledek	+	+	+	+
Náročnost výpočtu	-	+	-	+
Náročnost na programové vybavení	-	-	-	+
Časová náročnost	-	+	-	+
Finanční náročnost	-	+	-	+
Přesnost	+	+	+	+

3.4 Kvalitativní prognostické metody

Tyto metody bývají založeny na úvahách, názorech či zkušenostech expertů, proto je jejich výsledek subjektivní. To však nemusíme považovat za negativní faktor, jelikož ne vždy je k dispozici dostatečné množství faktů a údajů k tvorbě kvantitativních prognóz. Výstupem těchto prognóz je takzvaná předběžná prognóza. [13,14]

Zásadní výhoda těchto metod je především v možnosti využití velkého množství informací. Nevýhodami může být jejich nesystematičnost v měření a vyhodnocování přesnosti prognózy, a také jistá předpojatost (subjektivita) expertů prognózu provádějících. Obecně jsou však vhodné tyto metody pro dlouhodobější předpovědi. [13]

Dále lze dělit kvalitativní prognostické metody podle jejich účelu, a to na výzkumné a normativní. První uvedené vychází z informací o minulosti a současnosti. Na tomto základě daných informací jsou aplikovány heuristické přístupy jako odhad, intuice či zkušenost, za účelem dosažení vize stavu budoucího. To zároveň napomáhá k tvorbě scénářů, co a kdy by mělo nastat za určitých podmínek. U druhých normativních metod si naopak vytyčíme budoucí cíl či stav, kterého je třeba dosáhnout, a vracíme se do přítomnosti, kde identifikujeme zdroje a potřebné technologie k dosažení dílčího cíle. Zároveň jsou monitorovány prvky, které by dosažení cíle mohly zabránit a řeší způsoby jejich eliminace. [13,14]

3.4.1 Brainstorming (burza nápadů)

Metoda se používá na generování co nejvíce nápadů na dané téma. Nejčastější použití je v managementu, podnikání, při hledání optimálních postupů. Probíhá ve skupině do dvaceti členů představující rychlou diskuzi, řízenou podle stanovených pravidel. Mezi tyto pravidla můžeme zařadit např. podobné postavení a společenská úroveň expertů, přátelské a klidné prostředí při diskuzi, anonymně zaznamenávat nápady, jiné skupiny odborníků dle písemného záznamu provádí konečné formulace atd. Výhodou této metody je rychlost a operativnost, která slouží k překlenutí oblastí. [13,14,16]

3.4.2 Naivní extrapolace

Vychází se z jednoduchého předpokladu, že vývoj budoucnosti (výsledky) nejsou ničím jiným než rozšířením výsledků aktuálních událostí. Z toho vyplývá předpoklad, že budoucí stav bude totožný se stavem aktuálním.

3.4.3 Předpověď na základě konsensu

Jde o expertizní metodu vycházející z názorů či zkušeností expertů. Tito experti pracují v typických činnostech jako je marketing, výroba, odbyt, finance, bezpečnost a využívají například brainstormingu či brainwritingu. [13,14,16]

3.4.4 Delfský panel

Jedná se taktéž o expertizní metodu, která má původ v oblasti vojenství při prognózování složitých problémů. Patří mezi nejužívanější kvalitativní metody. Metoda je založena na anonymním více kolovém expertním odhadu odborníků. Princip spočívá v dotazování expertů prostřednictvím dialogu nebo písemné ankety v několika kolech s více týdenními intervaly, za účelem vyjádření předpovědi hodnot podle zvolených kritérií. Důležitým faktorem je formulace dílčích otázek. Odpovědi musí být doprovázeny podrobnou argumentací. Její nevýhodou je časová náročnost. [13,14,16]

3.4.5 Analogie

Metoda analogie využívá k prognózování systém na základě hledání analogie vývoje prognózovaného procesu s dalším procesem, jehož završení již proběhlo v minulosti, a které jsou podobné současným – analogie historická. Snaha o nalezení co nejvíce shodných podstatných vlastností a znaků. Výběr je náhodný a neměl by se nechat ovlivnit předčasným názorem. Je také vhodná v případech určení trendu, pro který nemáme vhodnou

metodu na základě vývoje známého trendu. Metoda analogie je vhodná v určitých případech, a to v hledání analogie vývoje prognózovaného procesu s dalším procesem, v analogii hledající ve vývoji technicko - ekonomického systému s vývojem biologického systému, určení vývoje trendu. [13,14,16]

3.4.6 Historická analogie

Tato metoda vychází z myšlenky obecné analogie, ale vztahuje se k událostem z minulosti, které se již udály a jsou podobné těm současným. Je používána k zobecňování historických zkušeností, důsledků a v souvislosti sociálních, ekonomických a technických jevů. Jsou používány dva přístupy. Kvalitativní, který je využíván pro získání názorného podobenství vývoje a kvantitativní, který srovnává hodnoty charakteristik trendů historického a prognózovaného trendu. [13,14,16]

3.5 Kvantitativní prognostické metody

Na rozdíl od metod kvalitativních jsou kvantitativní metody založeny na objektivních informacích, získaných ze statistických analýz dat z minulosti. Jedná se o praktickou aplikaci matematických modelů a rovnic nebo tvorbu bodových prognóz vázaných k určitému okamžiku v budoucnu. Metody lze rozdělit na dvě kategorie. První je metoda časových řad, tvořena z analýzy chronologických sekvencí určených proměnných ve stanovených časových intervalech pozorování, to ale za předpokladu, že studiem hodnot z minulosti a jejich vývoje v čase, lze předpovídat hodnoty v budoucnosti. Druhou kategorií jsou metody ekonomické či příčinné. Jde o deterministické metody, tudíž jsou realizovatelné jen za předpokladu, že vše je předurčeno. Princip je založen na predikci budoucích proměnných hodnot na základě chování jiných nezávislých proměnných. Cílem výše zmiňovaných metod je nalézt matematický vzorec například mezi objemem prodejů a příjmů zákazníků či riziky loupeže a technologiemi zabezpečení. [13,14]

3.5.1 Metoda extrapolace – Analýza trendových funkcí

Analýza trendových funkcí se odvíjí od skutečnosti, že sledovaný proces se bude v budoucnu vyvíjet stejným směrem nebo i se stejnou intenzitou. Vývoj daného jevu lze uskutečnit sestrojením křivky vývoje, např. vývoj dle přímky, cyklické křivky (periodicky se opakující jev), parabola, exponenciála (intenzita neustále narůstá nebo klesá), logistické

křivky, které jsou typické pro společenské jevy a odráží se v nich fakt, že exponenciální růst nebo pokles probíhá pouze po určité meze. Metoda má stanovený postup, který je rozdělen do čtyř etap. První etapou je určení parametrů trendu, dále pak výběr dat charakterizující minulý vývoj, posléze volba délky extrapolovaného období a nakonec určení funkce vyjadřující budoucí trend (křivka). [13,14,17]

3.5.2 Regresní analýza

Jedná se o statistickou metodu popisující závislost proměnných, která slouží k podpoře metody extrapolace. Za její pomoci odhaluje hodnotu jisté náhodné veličiny (závislé) na základě znalosti jiných veličin (nezávislé). Korelací je nazýván vzájemný vztah mezi dvěma procesy nebo veličinami. V případě, že se mění jedna z nich, mění se i druhá a naopak. Korelace se vyjadřuje pomocí korelačního koeficientu, který nabývá hodnot -1 až +1. [13,14,17]

3.5.3 Strom významnosti a morfologická analýza

Její použití spočívá v tom, že na začátku jsou zadány budoucí potřeby nebo cíle a na jejich základě jsou identifikovány okolnosti, opatření, technologie potřebné k jejich dosažení. Jde o analytickou metodu, která člení široké téma do stále užších dílčích podtémat formou stromového diagramu. Morfologická analýza pak zahrnuje mapování určité disciplíny s cílem dosažení širšího náhledu nad existujícími řešeními. Morfologie popisuje určité tvary daných objektů. [14,17]

3.5.4 Kolo budoucnosti

Tato metoda pomáhá organizovat myšlení a pokládat otázky o budoucnosti. Postupem této metody je napsat název události nebo trendu uprostřed plochy papíru a k němu se připisují malé paprsky, které jsou umístěny do kruhu kolem středu. Na konci každého paprsku jsou napsány primární dopady a důsledky. Jde o velmi levnou techniku a je využitelná ve složitých situacích. Metoda nevyžaduje žádné vybavení ani software, a tak je uživatelsky příjemná. [14,17]

3.6 Dílčí závěr prognostických metod

V této části byly přiblíženy prognostické metody, které se dělí na kvalitativní (subjektivní) a kvantitativní (objektivní). Kvalitativní metody pracují s pravděpodobností a mnohoznačností budoucího vývoje. Kvantitativní metody zase s vlastností časových řad, které popisují často se vyskytující situaci v reálném životě. Prognostické metody jsou svou podstatou určeny k jiným činnostem než analytické, hlavní podstatou je řešení otázek dosti odlišných, a to konkrétně k tvorbě scénářů, předpokladů a prognóz. Jednoduše to lze vysvětlit příklad tak, že naivní extrapolace se používá pro tvorbu scénářů potenciálního ohrožení objektu, naopak je dosti nevhodná pro tvorbu postupů zajišťujících preventivní opatření. V následující tabulce je vyhodnocení vybraných metod. Kde znaménko plus znamená kladné hodnocení a znaménko mínus záporné. [13,14]

Tab. 4. *Vyhodnocení prognostických metod* [18]

Prognostické metody / Činnosti bezp. Prognózy	Tvorba scénářů potenciálního ohrožení objektu	Tvorba předpokladů vývoje kriminality	Tvorba postupů zajišťujících preventivní opatření	Prognózování krizových stavů ve společnosti
Naivní extrapolace	+	+	-	-
Předpověď na základě konsensu	+	+	+	+
Delfský panel	+	-	-	+
Analogie	+	-	+	-
Historická analogie	+	+	+	+
Analýza trendu funkcí	+	+	-	-
Regresivní analýza	-	-	+	-
Strom významnosti a morfologická analýza	-	+	-	+
Kolo budoucnosti	+	-	-	+

II. PRAKTICKÁ ČÁST

4 ANALÝZA SOUČASNÉHO PŘÍSTUPOVÉHO A DOCHÁZKOVÉHO SYSTÉMU

Tato teoretická část se bude zabývat analýzou soudobého přístupového a docházkového systému námi vybrané rozsáhlé výrobní společnosti XY. Bude zde zahrnut popis dané společnosti, seznam stávajících prvků a metodika přístupu do areálu. Dále popis všech přístupových bodů do areálu. V dané části se budeme zabývat pouze přístupovým systémem ke vstupu do areálu společnosti. Přístupový a docházkový systém je tvořen prvky a přístupovým systémem Aktion, který je určený pro fyzické zabezpečení objektů. Umožnuje také nastavení přístupových oprávnění do jednotlivých částí objektu a evidenci pohybu osob.

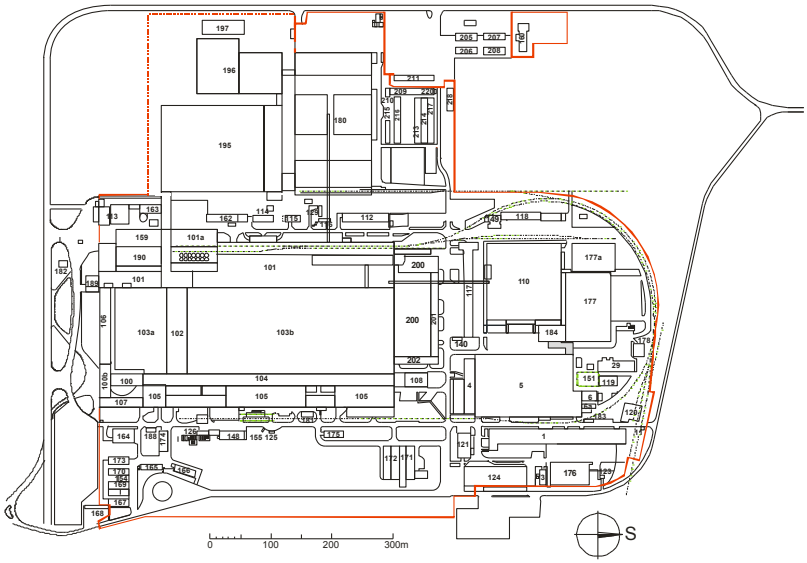
Výhodou tohoto systému je:

- modulární řešení,
- neurčuje limit počtu – dveří, uživatelů, držitelů karet,
- umožňuje integraci se systémy PZTS,
- umožňuje grafické vizualizace,
- funkce antipassback - eliminace průchodu více osob na jednu kartu,
- řídící jednotky s připojením na internet.

Jeho součástí mohou být snímače identifikačních karet, otisky prstů i klávesnice pro zadání PIN kódu. Systém Aktion umožnuje ovládání dveřních zámků, závor, turniketů, automatických dveří.

4.1 Současné informace o vybrané společnosti

Námi vybraná rozsáhlá výrobní společnost XY je mezinárodní výrobce, zabývající se výrobou důležitých částí automobilů. Společnost se nachází na okraji malého moravského města. Nachází se zde dobře rozvinutá infrastruktura. Samotný areál je umístěn v blízkosti železniční tratě, u silnice 1. třídy a malého letiště. V současné době zaměstnává okolo 4500 zaměstnanců. Areál se rozkládá na ploše 738 m^2, jak je zobrazeno na obrázku č. 4. nachází se zde mnoho budov a výrobních hal. Objekt přímo sousedí s dalším průmyslovým objektem. V areálu se nachází také několik společností a firem, které nespadají pod námi vybranou společnost. V objektu v současné době dochází k velkému pohybu osob a nákladních vozidel, jelikož právě probíhá rekonstrukce a rozšiřování výrobních kapacit.



Obr. 4. *Areál vybrané společnosti*

4.2 Výčet stávajících přístupových prvků

Společnost má pro vstup do areálu osm přístupových bodů, na kterých využívá veškerou níže vyjmenovanou techniku.

4.2.1 Terminál TPC/E

Obr. 5. *Docházkový terminál TPC/E* [19]

Docházkový terminál TPC/E je možno použít jako samostatnou řídicí jednotku. Je přizpůsoben pro snadnou montáž na zeď, dřevo či kovový podklad. V terminálu je zabudován bezkontaktní snímač typu APR-P20/USB s dosahem 5 – 10 cm. Dotyková LCD obrazovka má velikosti 7“. Využívá operační systém Windows XP Embedded. Jeho stávající rozměry jsou 195 x 180 x 105 mm (š x v x h) a je opatřen ochranou IP 64. [19]

4.2.2 Multifunkční terminál AXT-300/310

Obr. 6. *Multifunkční terminál AXT-300/310* [20]

Jedná se o multifunkční terminál řady Aktion NEXT pro systémy evidence docházky, kontroly přístupu, evidence výroby a stravování s možností identifikace kartou Mifare. Je vybaven rozhraním Ethernet. Lze využívat funkce on-line/off-line provozní režim a globální antipassback. Je vybaven integrovanou 1.3 MegaPixeovou kamerou. Terminál lze použít jako samostatnou řídící jednotku. Do terminálu je integrován bezkontaktní snímač dle typu a to Unique/HS (AXT-300) nebo Mifare (AXT-310). Dotyková LCD obrazovka o velikosti 8“. Rozměry terminálu jsou dány velikostí 262 x 230 x 96 mm (š x v x h) a je opatřen ochranou IP 30. [20]

4.2.3 Kontrolér MultiCon – KMC/E/2M

Obr. 7. *Kontrolér MultiCon – KMC/E/2M* [21]

Jedná se o samostatnou řídící jednotku s rozšířenou pamětí, která je určená pro rozsáhlé instalace. V kombinaci s připojenými moduly MMC ji lze využít i pro nejnáročnější aplikace. Na sekundární linku RS485 lze připojit až patnáct modulů nebo terminálů MultiCon. K vlastnímu kontroléru lze pak navíc připojit dva bezkontaktní snímače nebo dva terminály s dotykovým displejem. KMC/E/2M s plným počtem připojených modulů MMC umožňuje ovládání až 30 dveří na sekundární lince RS485 + 2 dveře na KMC/E/2M a nastavení Antipassbacku a Messengeru (vazby mezi vstupy a výstupy). Kapacita paměti pro události závisí na počtu připojených podřízených modulů, počtu nahraných osob se jménem, nebo beze jména a počtu podmíněných karet. Rozměry kontroléru jsou dány velikostí 235 x 175 x 42 mm (š x v x h) a je opatřen ochranou IP 30. [21]

4.2.4 Modul MultiCon – MMC

Obr. 8. *Modul MultiCon – MMC* [22]

Jedná se o rozšiřující I/O modul pro kontrolér KMC/E. Modul MMC nelze použít jako samostatnou řídící jednotku, ale výhradně v kombinaci s řídícím kontrolérem KMC. Zařízení je vybaveno dvojitě vyváženými vstupy pro dveřní kontakty, tlačítka a tamper. Díky funkci Messenger je možné definovat vazby mezi vstupy a výstupy modulů a informovat tak o různých situacích, jež mohou nastat (pokus o průchod, průnik, sabotáž, plná paměť atd.). Další z nabízených funkcí je Antipassback. V jeho rámci je možné automaticky zablokovat přístupová oprávnění osobě, která porušila pravidla pro pohyb ve chráněných prostorech. Rozměry modulu jsou dány velikostí 155 x 120 x 33 mm (š x v x h) a je opatřen ochranou IP 30. [22]

4.3 Metodika vstupu do areálu společnosti

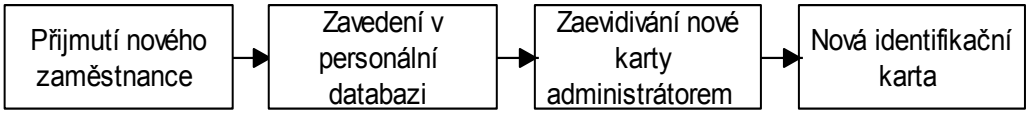
Společnost má pro vstup do svého areálu stanoveny určité podmínky, které se odvíjejí od použitého přístupového systému a jsou upraveny interní směrnicí. Aby byl umožněn přístup do areálu, musí být nejprve vydána identifikační karta, kterou vydá příslušník bezpečnostní divize. Tyto karty má společnost rozdělena podle druhu použití na:

- osobní karta zaměstnance,
- karta Kontraktor,
- krátkodobá (Temporary) osobní karta pro zaměstnance externích společností,
- návštěvní (Visitor) osobní karta,
- karta návštěvy s vozidlem,
- karta osobního vozidla,
- karta nákladního vozidla.

Každá karta má posléze nastaveno příslušná přístupová oprávnění, která zajišťuje administrátor bezpečnostní divize. Těchto oprávnění je hned několik a odvíjejí se podle účelu vstupu do areálu nebo místem vykonávání práce. Zaměstnanec je povinen určeným způsobem zaznamenat příchod a odchod do/z areálu vlastní identifikační čipovou kartou. Tato karta je nepřenosná, a je zakázáno jakékoliv zapůjčování této karty jiným osobám. Při přerušení pracovní doby a opuštění areálu je každý zaměstnanec povinen zaznamenat na dotykovém terminálu důvod přerušení pracovní doby (lékař, dovolená, služební cesta, apod.). Důvod přerušení pracovní doby je do systému zaznamenán až po stisku tlačítka a přiložení karty. Příchod a odchod je zaznamenán automaticky po přiložení identifikační karty ke čtecímu zařízení (čtečka, terminál). Tato pravidla platí také pro zaměstnance externích firem, které mají sídlo v areálu vybrané společnosti.

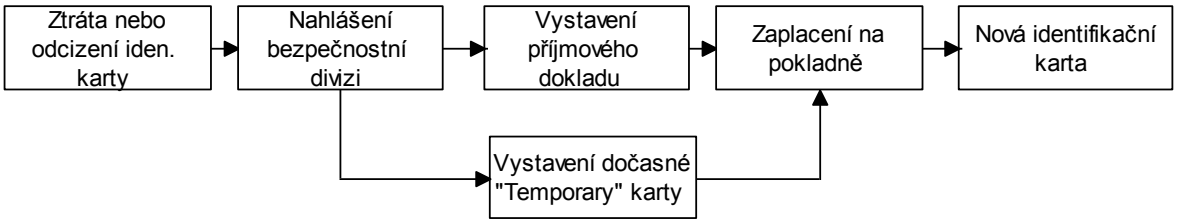
4.3.1 Osobní karta zaměstnance

Tato karta musí obsahovat na svém obalu tři základní informace, a to osobní číslo zaměstnance, jméno a příjmení, název společnosti. Karta je vydána na základě zavedení osoby v personální databázi, resp. požadavku personální divize. Zaměstnancům je posléze vydávána identifikační karta administrátorem bezpečnostní divize.



Obr. 9. *Postup vydání nové karty zaměstnanci*

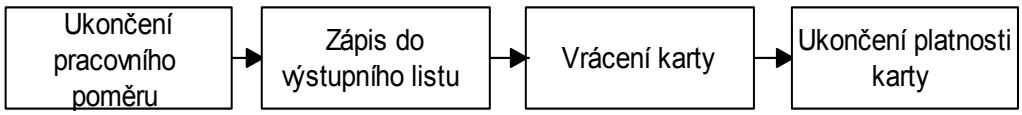
Pokud dojde ke změně pracovního zařazení zaměstnance, vydává se nová čipová karta pouze v případě, že dojde také ke změně osobního čísla. Při ztrátě nebo odcizení čipové karty je držitel karty povinen nahlásit tuto ztrátu bezpečnostní divizi. Pokud dojde ke ztrátě, poškození, nebo odcizení čipové karty ve lhůtě kratší než 2 roky, administrátor docházkového systému zajistí u příslušného účetního střediska, ve kterém je zaměstnanec kmenově zařazen, vyhotovení příjmového pokladního dokladu. Po zaplacení v pokladně bude zaměstnanci vydán duplikát karty na základě předložení potvrzeného příjmového dokladu. Do doby vydání nové karty použije zaměstnanec kartu „Temporary“ Na tuto kartu jsou nastavena stejná přístupová práva jako na kartě zaměstnance.



Obr. 10. *Postup při ztrátě nebo odcizení*

Při zapomenutí karty bude podobným způsobem vydána náhradní „Temporary“ karta. Karta se vystavuje pouze držiteli platné (neblokované) čipové karty, který ji z objektivních důvodů nemůže použít, např. z důvodu zapomenutí, či předpokládané ztráty. Platnost dané náhradní karty je stanovena na dobu maximálně tří dnů. Osoba vystavující náhradní čipovou kartu je povinna ověřit totožnost žadatele – firmu, osobní číslo, středisko, popř. požádat o jiný doklad totožnosti (občanský průkaz, pas). Náhradní karta kopíruje přístupová oprávnění původní karty.

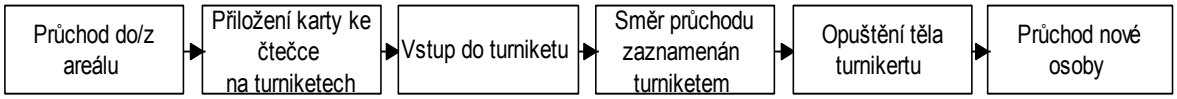
Při ukončení pracovního poměru jsou všechny karty, určené k průchodům a průjezdům přes vrátnice, vráceny do bezpečnostní divize, kde administrátor provede ukončení platnosti. Vrácení karty zapíše příslušný personalista do výstupního listu. O způsobu vrácení čipové karty rozhodne personalista. Vrátit kartu lze několika způsoby, a to personalistovi, do pohlcovače karet, na vrátnici nebo administrátorovi docházkového systému.



Obr. 11. *Postup vrácení karty po ukončení pracovního poměru*

4.3.2 Průchod osob do/z areálu

Pro příchod a odchod osob do areálu se využívají čtyři přístupová místa, vrátnice O1,O2,O3,O4. U všech přístupových míst platí stejný postup příchodu a odchodu odvíjející se od přístupového a docházkového systému. Pro vstup do areálu nejprve předloží osoba čipovou kartu ke čtečce na turniketech. Obdobný způsob je i při odchodu, kdy osoby přiloží čipovou kartu ke čtečce nebo terminálu. Směr průchodu je vždy zaznamenán automaticky průchodem turniketu. Příchod či odchod je pak zaznamenán až po fyzickém průchodu tělem turniketu. Pro průchod další osoby je potřeba nejprve vyčkat až osoba opustí tělo turniketu. Také není umožněno předkládat čipovou kartu, dokud nedojde k průchodu předcházející osoby.



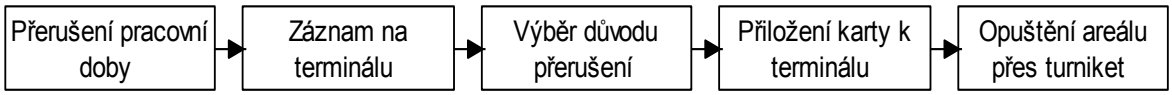
Obr. 12. *Postup průchodu turniketem*

Pokud dojde k přerušení pracovní doby, toto přerušení se musí nejprve zaznamenat na terminálu při odchodu přes vrátnici. Osoba nejprve vybere symbol přerušení pracovní doby. Tento záznam potvrdí přiložením karty k terminálu. Posléze může projít turniketem a opustit areál firmy. Způsobů přerušení pracovní doby je hned několik a jsou graficky zobrazeny na displeji terminálu. Nacházejí se tam tyto možnosti:

- práce mimo areál – veškerá práce mimo areál, ke které nebude dokládán cestovní příkaz,
- služebně – služební cesta, která je dokládána cestovním příkazem,
- bankomat - návštěva bankomatu KB,
- dovolená – při nástupu na dovolenou,
- návštěva pracovní – vyzvednutí pracovní návštěvy, předání dokumentů před areálem atd.,
- návštěva soukromá - nepracovní jednání na vrátnici,
- lékař – návštěva lékaře,
- nemoc – nástup na nemocenskou,

- náhradní volno - čerpání náhradního volna,
- kouření – přerušení pracovní doby z důvodu kouření,
- ošetřování – ošetřování člena rodiny,
- osobní překážky – osobní překážky na straně zaměstnance jako dárcovství krve, svatba atd.,
- docházkové informace – informace o odpracovaných hodinách, započtených mzdových složkách atd.,
- školení – školení zaměstnanců společnosti,
- studium – započitatelné vzdělání zaměstnancem vykazované průměrem,
- osobní údaje – osobní údaje zaměstnance typu jméno, příjmení, osobní číslo.

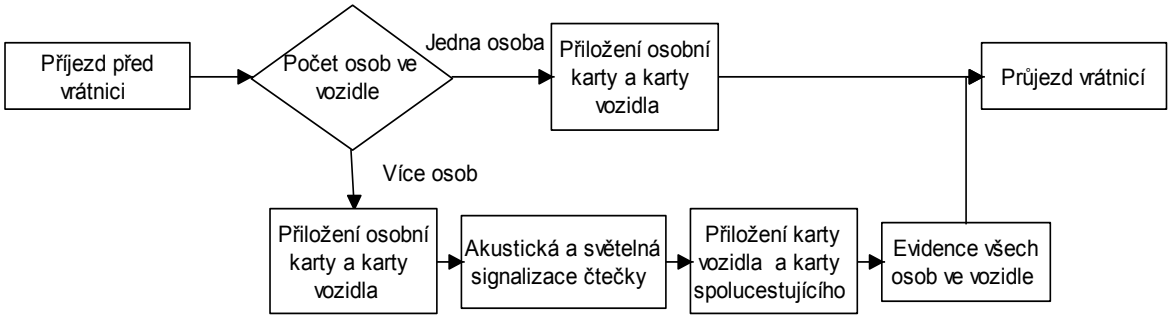
Na terminálu se mohou objevit dvě hlášení „Jméno“ a „Způsob průchodu“, pokud jsou přidělena příslušná práva na průchod. Dále hlášení „Vstup odmítnut“, pokud nejsou přidělena příslušná práva na průchod.



Obr. 13. *Postup pří přerušení pracovní doby*

4.3.3 Průjezd dopravních prostředků do/z areálu

Pro vjezd a výjezd dopravních prostředků do areálu se využívají čtyři přístupová místa, a to vrátnice D1, D2, D3, D4. U všech přístupových míst platí stejný postup příjezdu a odjezdu, odvíjející se od přístupového a docházkového systému. Vjezd a výjezd je zaznamenán po přiložení karty vozidla a osoby ke čtecímu zařízení. V případě, že je ve vozidle více cestujících, jsou rovněž povinni se stejným způsobem zaznamenat. Pokud má osobní karta nastavena pro současný vjezd i určité vozidlo, je přiložena pouze jedna karta. V případě průjezdu více osob v jednom vozidle se postupuje tak, že řidič přiloží kartu vozidla a poté osobní kartu. Po akustické a světelné signalizaci čtečky přiloží kartu vozidla a osobní kartu spolujezdce. Takto jsou postupně zaevidovány všechny osoby ve vozidle. Řidič odpovídá za evidenci spolucestujících osob ve vozidle při vjezdu a odjezdu z areálu společnosti.



Obr. 14. *Postup průjezdu vozidla*

Oprávnění pro trvalý vjezd do areálu společnosti je povolen vozidlům vrcholového managementu a vozidlům zaměstnanců na základě vydaného povolení a přidělené čipové karty („Karta osobního vozidla“, „Karta nákladního vozidla“). Dále také vozidlům externích společností, které mají uzavřeny smlouvy o pronájmu objektů, po vystavení čipové karty. Také servisním vozidlům, která zabezpečují nepřetržitý provoz a pravidelné služby pro výrobní společnost a externí firmy se sídlem v areálu. O schválení trvalého vjezdu a následném vystavení čipové karty rozhoduje ředitel bezpečnostní divize.

Oprávnění pro dočasný vjezd do areálu společnosti je povolen vozidlům, která nemají trvale (Temporary a návštěvní karty) přidělenou čipovou kartu. Jedná se především o dovoz a vývoz zboží, dokládaným platným dodacím listem. Dovozem kusových zásilek a vývozem zboží na doklady z pokladny (za hotové). Dále také vozidlům, která zabezpečují neodkladné úkoly pro výrobní společnost a externí firmy v areálu společnosti. Rovněž schváleným návštěvám při dovozu zboží, materiálu či nářadí.

Kontrolovanému vjezdu nepodléhají vozidla hasičského záchranného sboru, pracovníků HZSp, v případě jejich svolání k likvidaci požáru či jiné havárie, pracovníků odboru energetiky, odboru údržeb a odboru výstavby, policie ČR, sanitní vozy zdravotnické záchranné služby, krajské hygienické stanice, kontrolních orgánů státní správy a samosprávy doprovázená zástupci společnosti.

Pokud dojde k porušení dopravních předpisů v areálu společnosti například špatné parkování zaměstnancem společnosti, bude daný přestupek předán k řešení přímému nadřízenému. V opakovaném případě bude vozidlu zakázán vjezd do areálu. V případě porušení dopravních předpisů externí firmou bude vůči ní uplatněna smluvní pokuta. Při opakovaném porušování pravidel může být provedena trvalá blokace čipové karty k vjezdu do areálu.

4.3.4 Návštěvy

Návštěvy, které jsou předem očekávány, nahlásí pověřený zástupce oddělení zaměstnanci bezpečnostní divize v administrativní budově v časovém předstihu nejpozději však v den příjezdu. Musí být nahlášeny tyto základní údaje:

- jméno a příjmení osob,
- společnost,
- předpokládaná délka pobytu,
- jméno a kontaktní telefon pověřeného zástupce,
- zda bude vyzvednut na vrátnici.

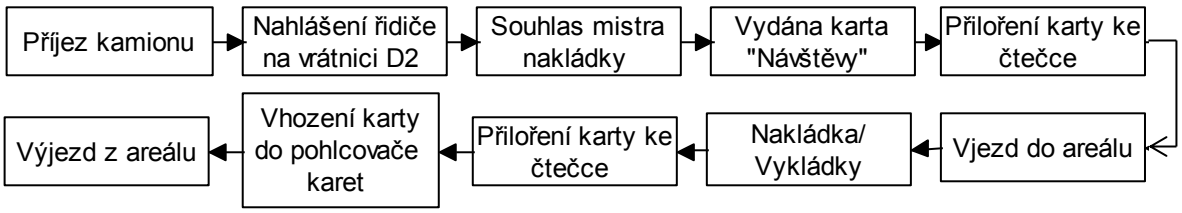
Pracovník bezpečnostní divize zaregistruje takto nahlášenou návštěvu do návštěvnického systému a připraví kartu „Návštěva“ pro vstup do areálu. Poté bude telefonicky vyrozuměno pracoviště, které má být navštíveno, a následně bude povolen vstup pouze s doprovodem pověřeného zástupce. Pro dlouhodobé návštěvy může administrátor docházkového systému bezpečnostní divize vydat na základě požadavku navštívené osoby kartu „Temporary“.

Vstup do objektů pro tuzemské a zahraniční návštěvy je umožněn vrátnicí v administrativní budově O1 (informace), nebo D2 (vozová vrátnice). K zápisu do evidence dochází na základě předloženého dokladu (cestovní pas, OP, ŘP). V evidenci návštěv docházkového systému musí být uvedena osoba, která návštěvu přijímá. Zaměstnanec bezpečnostní divize přivolá navštívenou osobu a vydá kartu „Návštěva“ Pracovní návštěvy servisního typu, které zahrnují dovoz a odvoz zboží, popřípadě servis ke vstupu resp. vjezdu do areálu využije vrátnici D2. Zaměstnanec bezpečnostní divize vydá kartu „Návštěva“ U tohoto typu návštěv se nevyžaduje přímý doprovod.

Za návštěvu se považují i osoby ve vozidlech mimo řidiče (spolucestující), které se neprokáží identifikační kartou pro vstup do areálu. Tyto spolucestující zaeviduje zaměstnanec bezpečnostní divize na vrátnici D2 a vydá návštěvní identifikační karty. Při odchodu z areálu je návštěva povinna kartu vhodit do pohlcovače karet, kdy se po vhození karty uvolní turniket k průchodu.

Vjezd a výjezd vozidel řidičů kamionové dopravy na vrátnici D2 odpovídá případu “Návštěvy“. Řidič se ohlásí na vrátnici zaměstnanci bezpečnostní divize a po souhlasu

mistra nakládky a následném vydání karty vjede do areálu. Při výjezdu z areálu odevzdá kartu vhozením do pohlcovače.



Obr. 15. *Postup vjezdu a výjezdu kamionu*

Externí firmy, které v areálu společnosti vykonávají servisní či stavební práce na sjednanou dobu, která je delší než jeden týden, jsou povinny si s dostatečným předstihem zažádat o vystavení „Temporary“ karty pro vícedenní vstup.

4.3.5 Vstup zaměstnanců externích společností do areálu

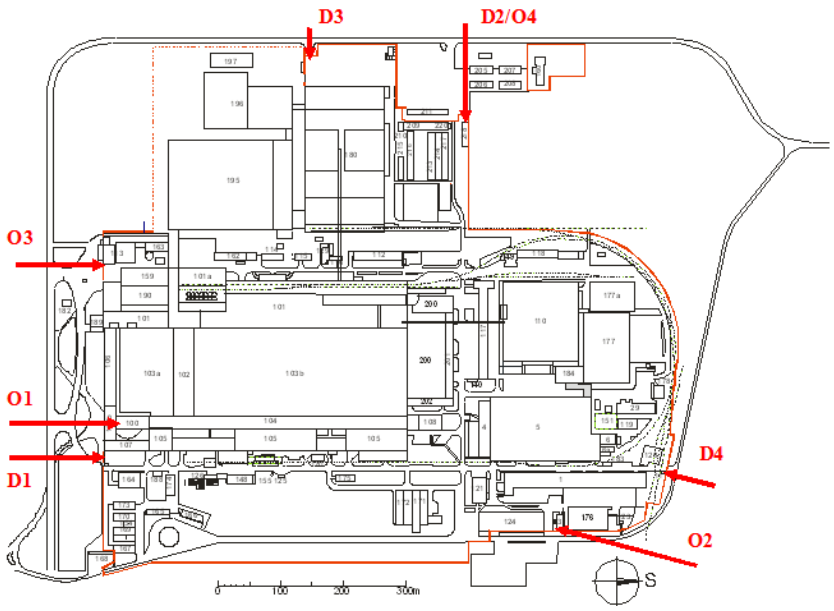
Zaměstnanci externích společností se sídlem mimo společnost, dočasně pracující v areálu, jsou oprávněni ke vstupu na základě identifikační karty. Administrátor docházkového systému bezpečnostní divize vydá „Temporary“ kartu. Externím společnostem se sídlem v areálu je karta pro vstup či vjezd vydána na základě vyplněné žádosti jednatelem externí firmy, nebo jím pověřeném zástupcem. Platnost karty zaniká oznámením společnosti o ukončení smlouvy nebo personální změnou. U společností se sídlem v areálu tuto skutečnost oznámí jednatel, nebo pověřený zástupce společnosti. U společností se sídlem mimo areál oznamuje skutečnost osoba odpovědná za smlouvu. Zaměstnanci externích firem jsou povinni používat pouze vrátnice vybrané výrobní společnosti. Evidence doby příchodu a odchodu zaměstnanců externích společností je vedena identicky jako pro zaměstnance dané společnosti. Identifikační karta může být odebrána rozhodnutím ředitele bezpečnostní divize nebo ředitele personální divize na základě závažného či opakovaného porušení závazných pravidel.

4.3.6 Vstup Policie ČR

Pokud je přivolána Policie ČR externí společností se sídlem v areálu nebo zaměstnancem společnosti, musí být neprodleně vyrozuměni zaměstnanci bezpečnostní divize. Zaměstnanec bezpečnostní divize vydá na základě předložení služebního průkazu „Návštěva“. V případě mimořádné události vstupují příslušníci Policie ČR bez evidence na základě služebního průkazu při doprovodu zaměstnanců bezpečnostní divize.

4.4 Přístupové body

Do areálu námi vybrané společnosti lze získat přístup několika místy, které má společnost přímo určené a můžeme je rozdělit na vstup pro osoby a vjezd pro dopravní prostředky. Na obrázku níže jsou graficky zobrazeny všechny přístupové body do areálu společnosti. Vstupy označené červenou O1 až O4 jsou určené pro osoby. Vstupy označené červenou D1 až D4 jsou určené pro dopravní prostředky.



Obr. 16. *Zobrazení přístupových bodů*

Vrátnice určené pro vstup pro osoby

- O1 – Vrátnice v administrativní budově
- O2 – Bezobslužná vrátnice s 2 turnikety
- O3 – Bezobslužná vrátnice s 1 turnikety
- O4 – Bezobslužná vrátnice u D2

Vrátnice určené pro vstup pro dopravní prostředky:

- D1 – Bezobslužná vrátnice pro osobní vozidla
- D2 – Nákladní vrátnice
- D3 – Pomocná nákladová výjezdní vrátnice
- D4 – Náhradní vjezd

4.4.1 Vrátnice O1

Obr. 17. *Pohled na vrátnici O1*

Vrátnice je umístěna v hlavní administrativní budově. Slouží jako hlavní vchod pro zaměstnance a návštěvníky společnosti. Díky umístění vně budovy je chráněna proti veškerým venkovním podmínkám. Jedná se o velký prostorný vstup, jak je zobrazeno na obrázku výše, nacházející se v přední části auly. Pro vstup do areálu slouží čtyři turnikety od společnosti Gunnebo model Speedgate FP, které jsou pro vstup dovnitř i ven. Je zde také jedna pomocná branka. Na všech turniketech je využit modul MultiCon – MMC. Pro výstup z areálu na krajním turniketu je používán ještě multifunkční terminál AXT-300/310, který slouží k zadání přerušení pracovní doby. Nachází se zde i pohlcovač karet od firmy Aktion REC/L/P/SL. Ten slouží pro odběr návštěvních karet. Jak lze vidět na obrázku výše turnikety nejsou příliš vysoké, a proto by byly snadno překonatelné. Před nimi se nachází informační pult s příslušníky bezpečnostní divize. Ti se zde pracují 24 hodin denně. Jejich povinnostmi jsou např. výdej klíčů, kontrola osob, registrace návštěv, příjem balíků apod. Za určitých podmínek umožnují také průchod brankou osobám:

- pokud se jedná o management společnosti (jednatelé, ředitelé),
- významné návštěvy,
- uchazeči o zaměstnání v doprovodu personalisty,
- exkurze v doprovodu odpovědné osoby,
- zaměstnanci provádějící strojové čištění podlahy,

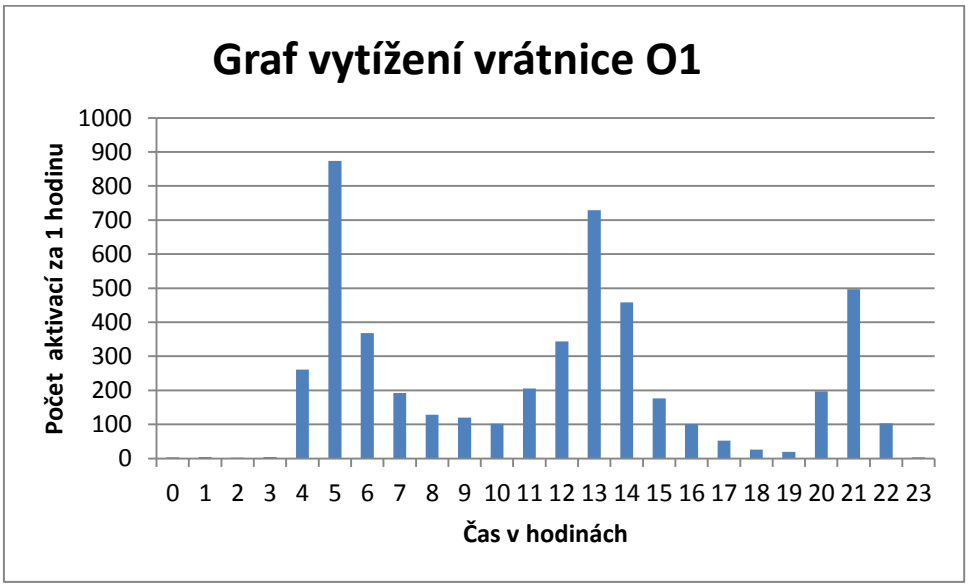
- krátkodobé opuštění areálu, kdy je zaměstnanec bezpečnostní divize schopen zajistit kontrolu opuštění areálu a bezprostřední návrat (např. převzetí balíků na vrátnici apod.).

Na vrátnici O1 bylo s poskytnutých dat zjištěno, že za normálního 24 hodinového dne je zaznamenáno okolo 5000 průchodů. Nejvytíženější v zaznamenaný den byl terminál T3, s celkovými 1834 průchody. Veškerá ostatní zjištěná data jdou zobrazena v tabulce níže, kde dané číslo znamená počet průchodů za 24 hodin.

Tab. 5. *Tabulka počtu příchodů a odchodů na O1*

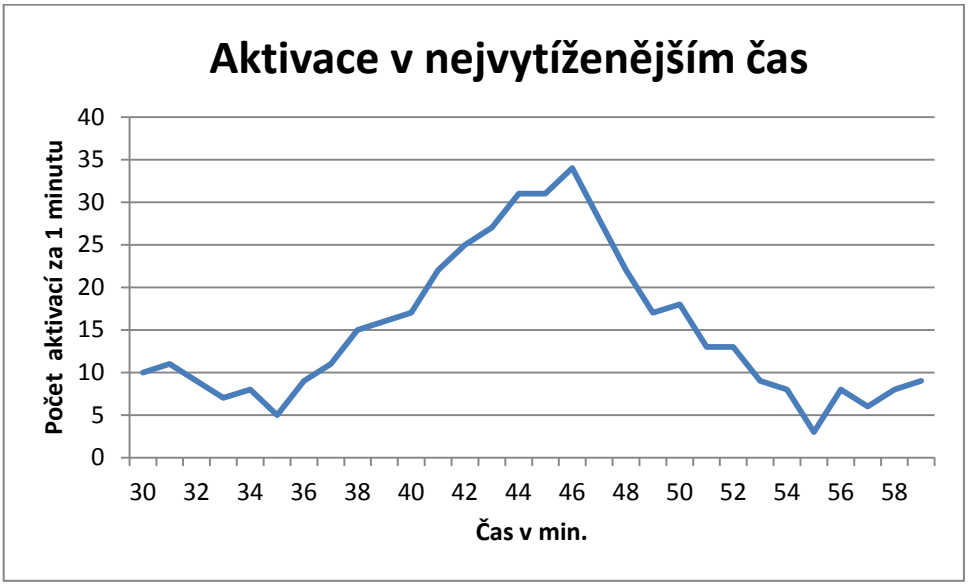
	Terminál T1	Terminál T2	Terminál T3	Terminál T4	Celkem
Příchody	494	822	820	360	2496
Odchody	298	669	1014	497	2478
Celkem na jednotlivých terminálech	792	1491	1834	857	4968

Z poskytnutých dat bylo zjištěno, že největší počet aktivací z hlediska času se odehraje mezi 5. a 6. hodinou, kdy je něco málo pod 900 aktivací. Následně pak mezi 13. a 14. hodinou a nakonec mezi 21. až 22. hodinou, což odpovídá nástupu zaměstnanců do směny.



Obr. 18. *Graf vytížení vrátnice O1*

Další graf zobrazuje, kolik proběhlo aktivací v nejvytíženější čas na vrátnici O1. Pro graf bylo zvoleno časové rozmezí mezi 5:30 až 6:00 hodin, kde podle předchozího grafu je největší počet aktivací. Na grafu níže lze vidět, že největší počet aktivací se odehraje mezi 44. až 46. minutou, kde dochází k nejvíce průchodům na vrátnici O1.



Obr. 19. *Graf aktivace v nejvytíženějším čas na O1*

4.4.2 Vrátnice O2

Obr. 20. *Pohled na vrátnici O2*

Vrátnice se nalézá na severovýchodní straně areálu. Slouží pro příchod a odchod zaměstnanců společnosti a zaměstnanců externích firem. Jedná se o jeden z pomocných vstupů, jelikož z této strany areálu se nachází parkoviště pro osobní vozidla a kolárna. Z této strany areálu je i přímý přístup na vlakové a autobusové nádraží. Jde o bezobslužnou

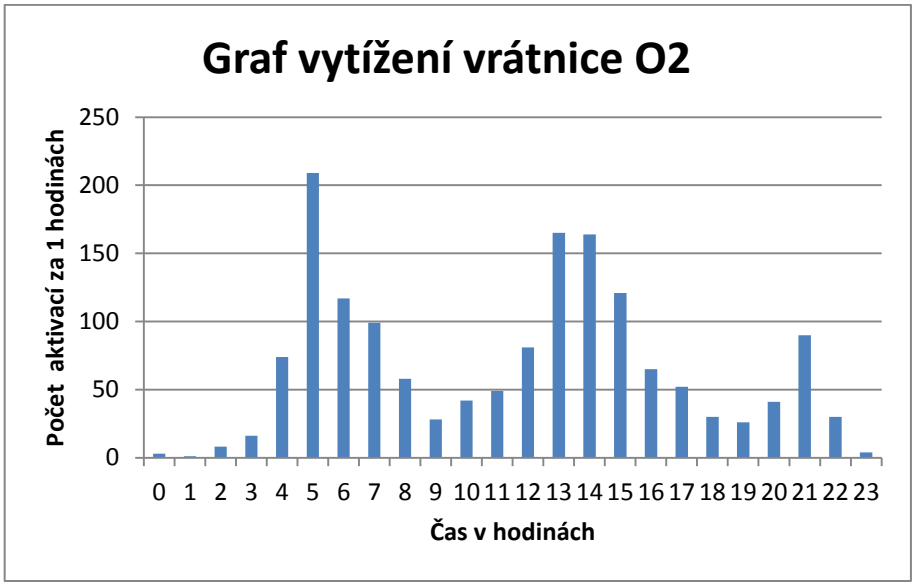
vrátnici, která je v provozu 24 hodin denně a nemá fyzickou ostrahu. Je tvořena kontejnerovou obytnou buňkou. Na jejím boku se nacházejí dva plno-vysoké turnikety Gunnebo Rotasec, vhodné pro venkovní použití, jelikož dobře odolávají povětrnostním vlivům. Tyto plno-vysoké turnikety umožňují ruční průchod v obou směrech. Pro vstup do areálu je využit modul MultiCon – MMC a pro výstup multifunkční terminál AXT-300/310. Nad těmito turnikety se nalézá zastřešení. Vrátnice je přímo spojena s oplocením areálu. Díky plno-vysokým turniketům a navazujícímu oplocení je dobře chráněna před fyzickým překonáním.

Na vrátnici O2 bylo s poskytnutých dat zjištěno, že za normálního 24 hodinového dne je zaznamenáno okolo 1600 průchodů. Ze zjištěných dat lze pozorovat, že oba turnikety jsou využívány rovnoměrně. Veškerá ostatní zjištěná data jdou zobrazena v tabulce níže, kde dané číslo znamená počet průchodů za 24 hodin.

Tab. 6. *Tabulka počtu příchodů a odchodů na O2*

	Turniket T1	Turniket T2	Celkem
Příchod	581	211	792
Odchod	176	605	781
Celkem na jednotlivých turniketech	757	816	1573

S poskytnutých dat bylo také zjištěno, že největší počet aktivací z hlediska času se odehraje mezi 5. a 6. hodinou, kde je něco málo nad 200 aktivací. Následně pak mezi 13. a 14. hodinou a 14. až 15. hodinou. Z grafu lze vysledovat, že vrátnice je používána častěji v odpoledních hodinách.



Obr. 21. *Graf vytížení vrátnice O2*

Další graf zobrazuje, kolik proběhlo aktivací v nejvytíženější čas na vrátnici O2. Pro graf bylo zvoleno časové rozmezí mezi 5:30 až 6:00 hodin, kde podle předchozího grafu bylo nejvíce aktivací. V tomto časovém rozmezí dochází k největšímu počtu aktivací mezi 33. až 51. minutou. Lze zde vidět, že v průběhu jedné minuty dojde v průměru 8 až 10 aktivacím.

Obr. 22. *Graf aktivace v nejvytíženějším čas na O2*

4.4.3 Vrátnice O3

Obr. 23. *Pohled na vrátnici O3*

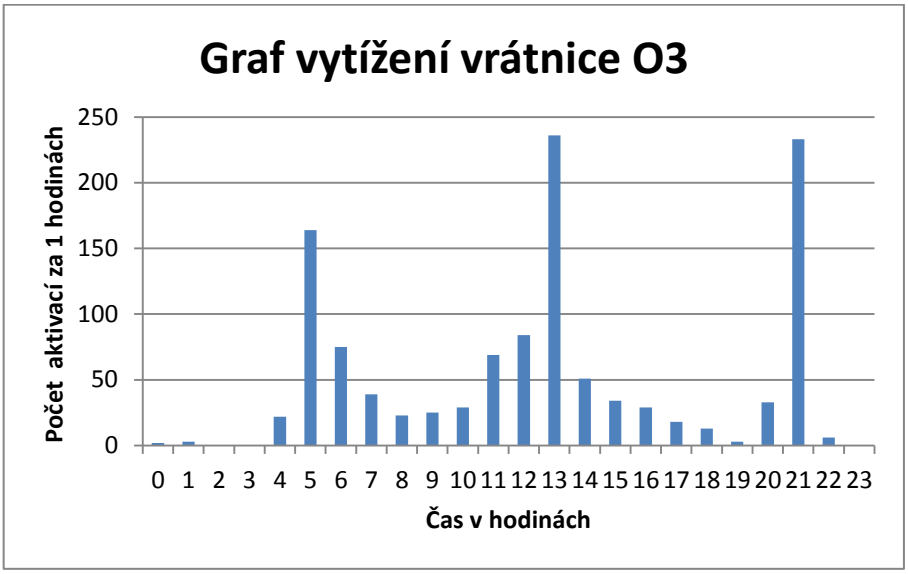
Vrátnice se nalézá na jihozápadní straně areálu společnosti. Je umístěna v prostoru mezi podnikovou prodejnou a výrobní halou, která v současnosti prochází rekonstrukcí. Vrátnice slouží pro příchod a odchod zaměstnanců společnosti a zaměstnanců externích firem. Jedná se o jeden z pomocných vstupů, jelikož poblíž se nachází parkoviště pro osobní vozidla. Jde o bezobslužnou vrátnici tvořenou jedním plno-vysokým turniketem Gunnebo Rotasec, který je umístěn vedle stěny podnikové prodejny. Vrátnice je v provozu 24 hodin denně a nemá fyzickou ostrahu. Pro vstup do areálu je využit kontrolér MultiCon – KMC/E/2M a pro výstup terminál TPC/E. Díky umístění mezi dvěma objekty a zastřešení, je vrátnice chráněna proti povětrnostním podmínkám a aktuálnímu počasí.

Na vrátnici O3 bylo s poskytnutých dat zjištěno, že za normálního 24 hodinového dne je zaznamenáno okolo 1200 průchodů. Veškerá ostatní zjištěná data jdou zobrazena v tabulce níže, kde dané číslo znamená počet průchodů za 24 hodin.

Tab. 7. *Tabulka počtu příchodů a odchodů na O3*

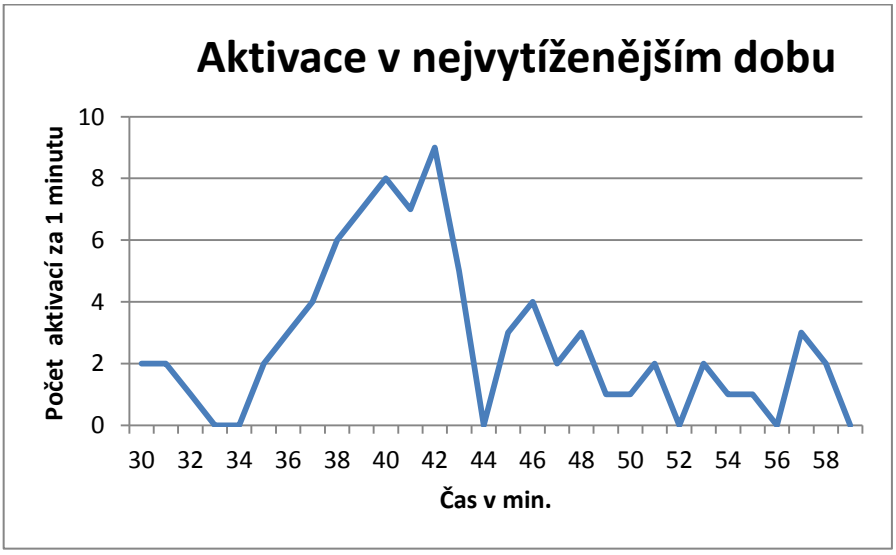
	Příchod	Odchod	Celkem
Vrátnice O3	598	594	1192

Z poskytnutých dat bylo také zjištěno, že největší počet aktivací z hlediska času se odehraje mezi 13. a 14. hodinou, kde je něco okolo 240 aktivací. Následně pak mezi 21. a 22. hodinou a posléze mezi 5. až 6. hodinou. Z grafu lze vysledovat, že vrátnice je nejčastěji používána v časech, kdy dochází k výměně pracovních směn.



Obr. 24. *Graf vytížení vrátnice O3*

Další graf zobrazuje, kolik proběhlo aktivací v nejvytíženější čas na vrátnici O3. Pro graf bylo zvoleno časové rozmezí mezi 13:30 až 14:00 hodin, kde podle předchozího grafu bylo nejvíce aktivací. V tomto časovém rozmezí dochází k největšímu počtu aktivací mezi 33. až 43. minutou. Lze zde vidět, že největší nápor během jedné minuty je 7 až 8 aktivacím v kratším časovém úseku.



Obr. 25. *Graf aktivace v nejvytíženějším čas na O3*

4.4.4 Vrátnice O4

Obr. 26. *Pohled na vrátnici O4*

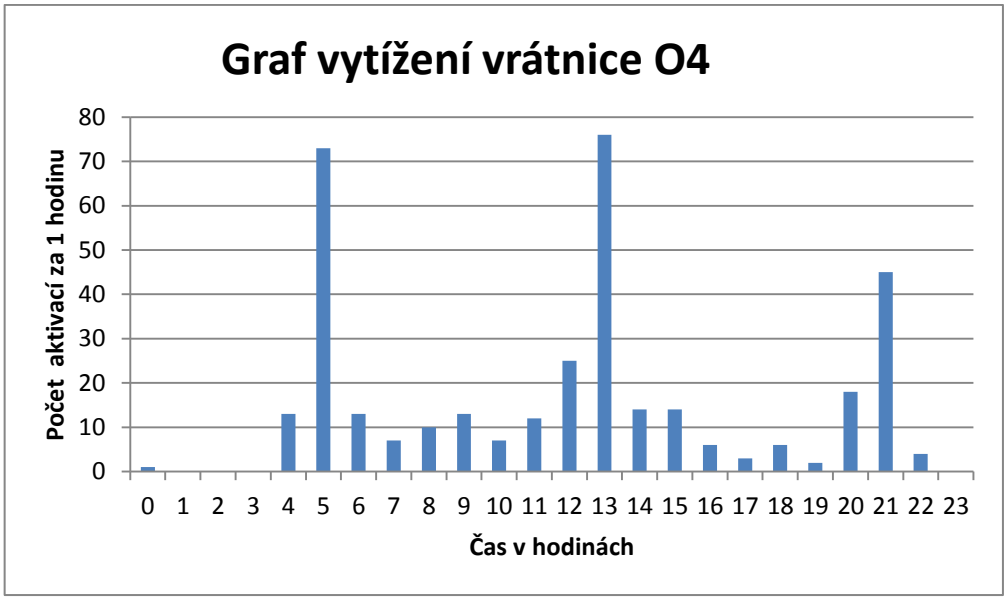
Vrátnice se nalézá na západní straně areálu společnosti. Jedná se o nově postavenou bezobslužnou vrátnici, která je umístěna vedle nové nákladové vrátnici D2. Slouží k příchodu a odchodu zaměstnanců společnosti a zaměstnanců externích firem do areálu. Stejně jako vrátnice O3 je tvořena jedním plno-vysokým turniketem Gunnebo Rotasec. Pro vstup do areálu je využit kontrolér MultiCon – KMC/E/2M a pro výstup multifunkční terminál AXT-300/310. Na straně výstupu z areálu se také nalézá pohlcovač karet od firmy Aktion REC/L/P/SL. Ten slouží pro odběr návštěvních karet. Jedná se o bezobslužnou vrátnici, která je v provozu 24 hodin denně. Vrátnice je zastřešena pomocí přiléhající vrátnice D2, ale je plně vystavena povětrnostním podmínkám a aktuálnímu počasí. Hlavní nevýhoda této vrátnice spočívá v přímém umístění příjezdové cesty. Tím dochází k nedostatečnému zabezpečení a lze vrátnici jednoduše obejít.

Na vrátnici O4 bylo s poskytnutých dat zjištěno, že za normálního 24 hodinového dne je zaznamenáno okolo 340 průchodů. Veškerá ostatní zjištěná data jdou zobrazena v tabulce níže, kde dané číslo znamená počet průchodů za 24 hodin.

Tab. 8. *Tabulka počtu příchodů a odchodů na O4*

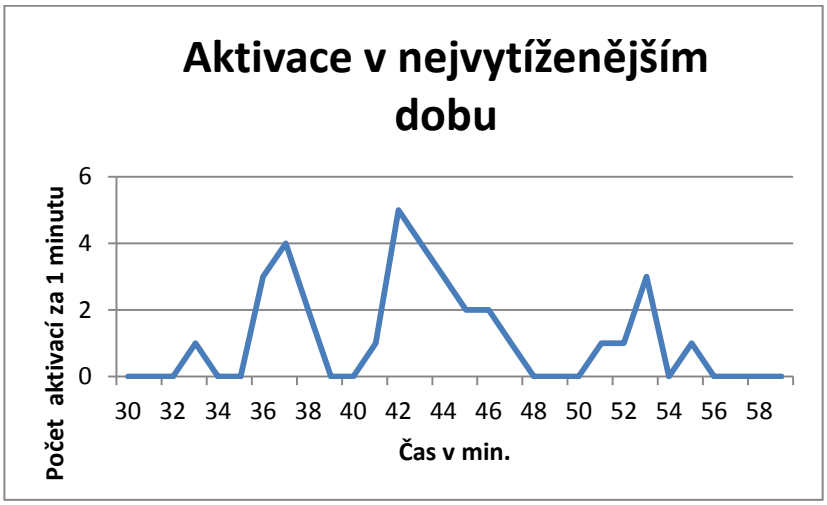
	Příchod	Odchod	Celkem
Vrátnice O4	181	185	336

Z poskytnutých dat bylo také zjištěno, že největší počet aktivací z hlediska času se odehraje mezi 13. a 14. hodinou, kde je něco okolo 75 aktivací. Následně pak mezi 5. a 6. hodinou a posléze mezi 21. až 22. hodinou. Z grafu lze vysledovat, že vrátnice je nejčastěji používána v časech, kdy dochází k výměně pracovních směn.



Obr. 27. *Graf vytížení vrátnice O4*

Graf na obrázku č. 28 zobrazuje, kolik proběhlo aktivací v nejvytíženější čas na vrátnici O4. Pro graf bylo zvoleno časové rozmezí mezi 13:30 až 14:00 hodin, kde podle předchozího grafu bylo nejvíce aktivací. V tomto časovém rozmezí dochází k největšímu počtu aktivací mezi 41. až 47. minutou. Lze zde vidět, že během největšího náporu proběhne 4 až 5 aktivací v kratším časovém úseku.



Obr. 28 *Graf aktivace v nejvytíženějším čas na O4*

4.4.5 Vrátnice D1

Obr. 29. *Pohled na vrátnici D1*

Vrátnice se nalézá vedle administrativní budovy společnosti. Slouží pro vjezd automobilových vozidel, která mají povolený vstup do areálu společnosti. K výjezdu jsou oprávněna pouze vozidla managementu. Jedná se o nově postavenou bezobslužnou vrátnici, která je tvořena malou kontejnerovou buňkou s automatickou závorou. Pro vjezd je využit kontrolér MultiCon – KMC/E/2M a k výjezdu terminál TPC/E. Ke vstupu se využívá identifikační karta vozidla, kde při přiložení ke čtečce se otevře přístupová brána. Přesný postup je popsán v kapitolách výše. Vrátnice je plně vystavena povětrnostním podmínkám a aktuálnímu počasí. Hlavní nevýhoda této vrátnice spočívá v přímé návaznosti na parkoviště vedle administrativní budovy. Díky této skutečnosti může jakákoliv osoba snadno překonat automatickou závoru a neoprávněně získat přístup do areálu společnosti.

4.4.6 Vrátnice D2

Obr. 30. *Pohled na vrátnici D2*

Vrátnice se nalézá na západní straně areálu společnosti. Jedná se o nově postavenou vrátnici, která slouží pro vjezd a výjezd osobních automobilů a nákladních vozidel, které provádějí nakládku nebo vykládku zboží, servis apod. Objekt nové vrátnice je tvořen ze dvou částí, a to zastřešením a velkým obytným kontejnerem. Ten je postavený na betonové ploše. Budova slouží pro bezpečnostní personál, který vydává návštěvní karty a kontroluje vjezd a výjezd vozidel do areálu. Vrátnice je v provozu 24 hodin denně. Provádí se zde také evidence nově přijetých kamionů a registrace do přístupového a docházkového systému. Objekt má dva přístupové body. Jeden slouží pro vjezd a druhý pro výjezd. Na obou stranách se nalézá automatická závora modul MultiCon – MMC a Multifunkční terminál AXT-300/310. U výjezdové brány je postaven také pohlcovač karet, který uvolňuje závoru umožňující výjezd. Přesný postup je popsán v kapitolách výše. I díky zastřešení je vrátnice plně vystavena povětrnostním podmínkám a aktuálnímu počasí.

4.4.7 Vrátnice D3

Vrátnice se nalézá na západní straně areálu společnosti v blízkosti budovy pro nakládání hotových výrobků. Slouží pouze jako pomocný výjezd pro nákladní automobily. Vrátnice je v provozu pouze po omezenou časovou dobu a to od 7 do 15 hodin. Na vrátnici je také fyzická ostraha, která kontroluje správný výjezd nákladních kamionů. Vrátnice je tvořena jednou obytnou kontejnerovou buňkou, která slouží pro příslušníky bezpečnostní divize. Pro výjezd je použit kontrolér MultiCon – KMC/E/2M a terminál TPC/E. Ty jsou umístěny ve venkovním stojanu od firmy Aktion model ST 220. Ve stojanu se nalézá také pohlcovač karet REC/ST. Vše je zobrazeno na obrázku níže. Dále je zde použita automatická závora. Hlavní nevýhoda této vrátnice spočívá v tom, že pohlcovač karet je příliš nízko, díky čemuž nemůže řidič kamionu snadno vhodit kartu dovnitř. Proto je zde zapotřebí pomoc příslušníka bezpečnostní divize, který od řidiče převezme kartu a vhodí do pohlcovače.

Obr. 31. *Pohlcovač karet na vrátnici D3*

4.4.8 Pomocný vjezd D4

Obr. 32. *Pohled na pomocný vjezd*

Jedná se o pomocný vjezd, který se nalézá v severní části areálu společnosti. Je určený pouze pro vjezd vozidel, pokud není umožněn vjezd na vrátnici D2. Jeho využití je velmi malé. Jak lze vidět na obrázku je tvořen dvoukřídlou železnou branou, která je přímo napojena na oplocení areálu. Pro kontrolu vjezdu do areálu je použit kontrolér MultiCon – KMC/E/2M.

4.5 Dílčí závěr

Námi vybraná výrobní společnost je světový výrobce komponentů pro automobily. Společnost zaměstnává několik tisíc osob. Areál společnosti je velmi rozsáhlý. V samotném areálu nesídlí jenom uvedená společnost, ale také několik externích firem. Přístupový a docházkový systém vybrané rozsáhlé výrobní společnosti je založen na technologii RFID. Pro získání přístupu do areálu společnosti je potřeba nejprve získat identifikační kartu. Těchto karet má firma hned několik a jsou rozděleny podle způsobu vstupu do společnosti (zaměstnanecká, dočasná, návštěvní atd.). Tyto karty lze získat buď v kanceláři bezpečnostní divize umístěné v administrativní budově, nebo na vrátnici D2. Do areálu společnosti lze získat přístup několika místy, které můžeme rozdělit na vstup pro osoby a vjezd pro dopravní prostředky. Těchto přístupových míst je celkem osm a nacházejí se na všech stranách areálu.

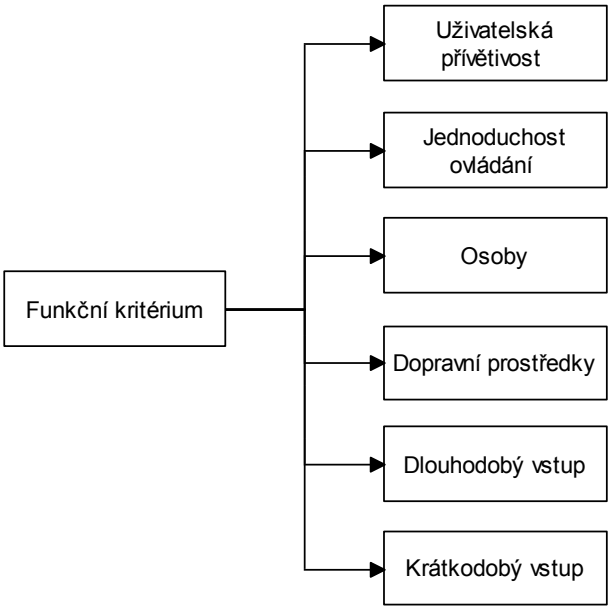
Při analýze přístupového a docházkového systému byly zjištěny následující skutečnosti, které nás nadále budou ovlivňovat. Do areálu společnosti každý den vstupuje několik tisíc osob. Jedná se především o zaměstnance společnosti a externích firem. Ale také vstupuje mnoho osob, které areál pouze navštěvují. Přístupový systém díky tomu musí být rychlý na identifikaci osob a uživatelský přívětivý. Do areálu lze vstoupit několika vrátnicemi, které umožnují jak vstup osob, tak motorových vozidel. Převážná část vrátnic se nalézá ve venkovních prostorech, a proto pří výběru nových metod přístupového a docházkového systému musí být tyto metody schopny procovat i ve venkovních prostorách, kde budou ovlivňovány přírodními podmínkami.

5 STUDIE NOVÝCH METOD PŘÍSTUPOVÝCH A DOCHÁZKOVÝCH SYSTÉMŮ PRO PODMÍNKY ROZSÁHLÉ VÝROBNÍ SPOLEČNOSTI

V následující kapitole se zaměříme na několik metod přístupových a docházkových systému, které by byly možné uplatnit pro vybranou výrobní společnost. Při této studii je potřeba zohlednit některé skutečnosti, které nás budou nadále ovlivňovat. Aby bylo možné tyto metody využít ve vybrané výrobní společnosti, musí být splněny některé podmínky. Použitá metoda musí být dostatečně jednoduchá a uživatelsky přívětivá. To znamená, že použitá metoda by neměla osoby nijak zásadně ovlivňovat a zpomalovat v průchodu turniketem nebo branou. Z technického hlediska by použitá metoda měla mít co možná nejrychlejší čas verifikace, aby nedocházelo k tvoření řad u turniketů v nejvytíženějších časech. Dále je důležité, aby mohla spolehlivě pracovat ve venkovních podmínkách. Ovlivňovat návrh bude i to, na kterou z vrátnic bude možné danou metodu použít. Zda je schopna verifikovat pouze osoby nebo je také díky ní umožněn vstup i dopravním prostředkům.

5.1 Evaluační metodika pro rozsáhlou výrobní společnost

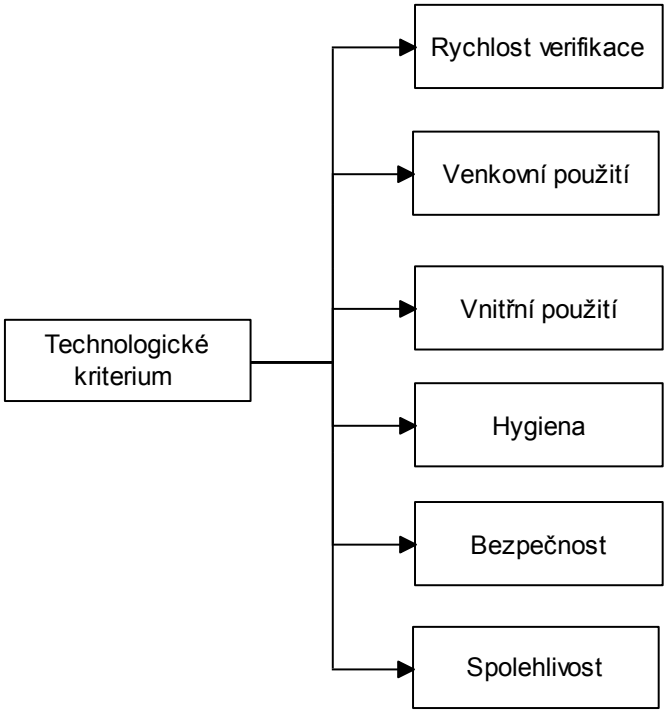
Abychom mohly co nejvhodněji zhodnotit jednotlivé metody, které by bylo možno uplatnit v dané rozsáhlé výrobní společnosti, musí být stanovena základní kritéria pro jejich zhodnocení. Tato kritéria jsou odvozena od základního charakteru společnosti a od vlastností jednotlivých metod. Díky těmto kritériím pak můžeme snadněji rozhodnout, na kterou z jednotlivých vrátnic je bude nejvhodnější uplatnit. Na základě těchto skutečností jsou děleny na tři základní kritéria, a to funkční kritérium, technologické kritérium a ekonomické kritérium. Tato základní kritéria se dále větví na jednotlivé vlastnosti, které by měly jednotlivé metody splňovat, aby bylo možné jejich uplatnění v podmínkách pro rozsáhlou výrobní společnost.



Obr. 33. *Funkční kritérium*

Jako první je zvoleno funkční kritérium, u kterého nás bude zajímat těchto šest jednotlivých vlastností, a to:

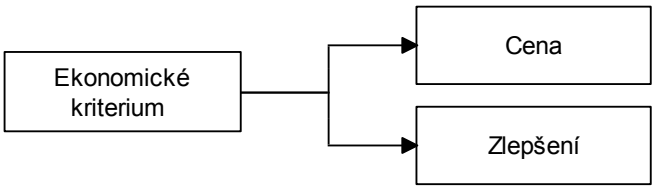
- uživatelská přívětivost – zda nová metoda bude kladně přijata jak zaměstnanci společnosti, tak osobami vstupujícími do areálu společnosti. Jestli bude akceptovatelná a její používání pro ně nebude jakkoliv nevhodné;
- jednoduchost ovládání – aby za použití dané metody neprobíhaly žádné složité operace pro průchod turniketem, které by zpomalovaly vstup do areálu;
- osoby – jestli daná metoda bude uplatnitelná pro vstup osob na vrátnicích O1,O2, U3, O4.;
- dopravní prostředky - jestli daná metoda bude uplatnitelná pro vjezd dopravních prostředků na vrátnicích D1, D2, D3, D4. A zda díky ní půjde jednoduše zaevidovat i dopravní vozidlo;
- dlouhodobý vstup - zda danou metodu bude vhodné použít pro zaměstnance vybrané společnosti, ale tak zaměstnance externích společností;
- krátkodobý vstup - zde nás bude zajímat, zda danou metodu bude vhodné použít pro osoby, které navštěvují areál společnosti krátkodobě (řidiči kamionů, servisní služby apod.);



Obr. 34. *Technologické kritérium*

Jako druhé je zvoleno technologické kritérium. U tohoto nás bude zajímat šest jednotlivých vlastností, a to:

- rychlost verifikace – zda nová metoda bude dostatečně rychlá na verifikaci, aby posléze nedocházelo ke zbytečnému zpomalení průchodu terminálem na vrátnicích,
- venkovní použití - zda daná metoda bude uplatnitelná ve venkovních podmínkách a nebude příliš ovlivněna rozmary počasí (déšť, sluneční svit apod.),
- vnitřní použití - zda daná metoda bude uplatnitelná v interiéru, a to hlavně na vrátnici O1,
- hygiena – zda použití dané metody nebude mít negativní vliv na zdraví dané osoby při jejím používání (přenos nemocí),
- bezpečnost – zda danou metodu nepůjde snadno oklamat a získat tak nepovolený přístup do areálu (např. padělání otisků prstů),
- spolehlivost - zda daná metoda dokáže spolehlivě pracovat i když dojde např. k poranění rukou.



Obr. 35. *Ekonomické kritérium*

Jako poslední je zvoleno ekonomické kritérium, u kterého nás budou zajímat dvě základní vlastnosti, a to:

- cena – zde se jedná o průměrnou cenu jednotlivých snímačů, které se nalézají na trhu,
- zlepšení - zda daná metoda přináší nějaké výhody, zjednodušení a zlepšení oproti stávajícímu přístupovému a docházkovému systému.

5.2 Zpracování osobních údajů

Před započetím výběru metod je potřeba si uvědomit, že při použití biometrické identifikace jsou zpracované osobní údaje považovaný za údaje citlivé. To znamená, že jejich ochraně je věnována zvýšená pozornost, což se projevuje v určitých zpřísněných požadavcích, které stanovuje zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Záměr zaměstnavatele na trvalé ukládání biometrických údajů, například samotných skenů či snímků, otisků prstů, je možné jen za podmínek stanovených § 9 zákona o ochraně osobních údajů, tedy buď s výslovným souhlasem subjektu údajů podle § 9 písm. a), nebo bez tohoto souhlasu, za podmínek dále tímto ustanovením stanovených. Současně musí být dodrženy všechny ostatní povinnosti správce podle zákona o ochraně osobních údajů, zejména uvedených v § 10. Je potřeba zdůraznit, že biometrika založená na zpracování citlivých údajů v centrální databázi by měla být v pracovněprávních vztazích využita jen ve výjimečných situacích. Dále si je potřeba uvědomit povinnost zaměstnavatele podle § 316 zákoníku práce, který se týká zákazu otevřeného i skrytého sledování zaměstnance. Toho by zaměstnavatel mohl dosáhnout, pokud by pro kontrolu docházky přípustný systém biometrické autentizace využíval pro kontrolu pohybu zaměstnance na pracovišti nad rámec evidence přítomnosti zaměstnance na pracovišti podle § 96 odst. 1 písm. a) zákoníku práce. [23]

Tyto podmínky pro zpracování osobních údajů dané zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých, bude brzy nahrazen obecným nařízením EU 2016/679 o ochraně osobních údajů (General Data Protection Regulation – GDPR). Toto nařízení vstoupí v platnost 25. května 2018. Nařízení upravuje práva a povinnosti fyzických osob, jejichž osobní údaje jsou zpracovávány, a subjektů, které údaje zpracovávají nebo za jejich zpracování odpovídají. Podle nařízení práva fyzických osob posilují a subjekty, které jejich osobní údaje zpracovávají, budou muset vynaložit veškerou odbornou péči na eliminaci rizik spojených se zneužitím, neoprávněným přístupem nebo neoprávněným zveřejněním osobních údajů. Fyzické osoby získávají právo být tzv. zapomenuty, a to v případě, že zpracovávané údaje už nejsou potřebné pro účely, pro které byly shromážděny, nebo pokud sám občan odvolal svůj souhlas se zpracováním svých osobních údajů. Pro správce a zpracovatele osobních údajů jsou stanoveny podmínky, kdy budou muset přijmout taková technická a organizační opatření, aby zajistili a byli schopni doložit, že zpracování je prováděno v souladu s nařízením. Bude potřeba vést detailní záznamy o zpracování údajů. Podniky, které zpracovávají ve velkém rozsahu citlivé údaje nebo provádějí rozsáhlé pravidelné a systematické monitorování subjektů údajů, budou muset najmout nového pracovníka, tzv. pověřence pro ochranu osobních údajů. [24]

5.3 Snímače otisků prstů

Technologie založená na rozpoznávání otisků prstu je vůbec nejznámější a nejpoužívanější metodou. Princip spočívá v tom, že snímač snímá obrazce papilárních linií, které obsahují tzv. markanty. Markanty jsou označovány jakékoliv změny v papilárních liniích. Unikátnost každého otisku prstu je dána různým počtem markantů, jejich umístěním a jejich vzájemnou kombinací. Aby bylo vyhodnoceno, jestli jsou otisky stejné, je potřeba nalézt několik podobných markantů. [25]

Výhody:

- široká nabídka snímačů,
- nízká cena,
- energeticky málo náročné, malé rozměry – možnost mobilního použití. [25]

Nevýhody:

- bez kontroly živosti lehce oklamatelné,
- otisk lze snadno získat bez vědomí uživatele,
- problém při snímání prstu s kožními chorobami. [25]

5.3.1 Parametry snímačů

- **Rozlišení**

Bývá označována jako počet jednotek DPI (bodů na palec). Minimální rozlišení v rozmezí 250-300 DPI. Při použití menších rozlišení se možnost extrakce informací z otisků snižuje. Obvykle skenery používají rozlišení 500 DPI. [26]

- **Oblast**

Jedná se o velikost snímané oblasti. Čím větší je tato oblast, tím více informací je možné zachytit a případný otisk je lépe zřetelný. [26]

- **Počet pixelů**

Počet pixelů lze snadno odvodit z tohoto vzorce: *R*v* × *R*š*, kde *v(výška)* × *š(šířka): počet pixelů* a *R* je rozlišení skeneru v DPI. [26]

- **Dynamický rozsah**

Dynamický rozsah určuje počet bitů, které jsou nutné pro zakódování hodnoty intenzity každého pixelu. Nejčastější dynamický rozsah je 8bitů. [26]

- **Geometrická přesnost**

Je obvykle určena maximálním geometrickým zakřivením, které způsobuje snímací zařízení. Toto zakřivení se udává v procentech s ohledem na osu x a osu y. [26]

- **Kvalita obrazu**

Tato charakteristika bere do úvahy věci jako: zda je prst vlhký či suchý, zda jsou na prstě nějaké jizvy a další faktory. [26]

5.3.2 Optoelektronické biometrické snímače

Optoelektronické biometrické snímače jsou díky svým výhodám a vlastnostem vhodné především pro algoritmy rozpoznání založené na markantech. Princip činnosti

je založený na rozdílném odrazu světla. Optický snímač zachycuje digitální zobrazení otisku pomocí viditelného světla. Obraz otisku se přenese na maticový CCD detektor, je následně digitalizován a dále předán pro zpracování. Pod vrstvou, kam se přikládá prst (dotykový povrch), je vrstva fosforu, která osvětluje celou plochu prstu. Odražené světlo od povrchu prstu prochází luminoforní vrstvou k CCD maticovému detektoru, a tam se vytvoří obraz otisku. [27]

Výhody – vysoká kvalita, odolnost proti statickým výbojům a minimální vliv okolního prostředí. [27]

Nevýhody – znečištění nebo poškození prstu může způsobit špatné vykreslení prstu. Dále pak otisk, který se aktuálně vytváří, může při snímání zachytit předchozí stopu otisku. Celkově mají optoelektronická zařízení větší rozměry, což je limitujícím faktorem pro implementaci do malých a přenosných zařízení. [27]

5.3.3 Kapacitní biometrické snímače

Založeny na principu využití rozdílu kapacity mezi deskou snímače a povrchem prstu. Snímač představuje jednu desku kapacitoru a druhou desku interpretují jednotlivá místa na prstu. Otisk se tak z pixelů získává v digitální formě. Pro načtení obrazu se prst přikládá na citlivou plochu osazenou velkým množstvím elektrod. Ty převedou kapacitně otisk prstu na digitální obraz, který se dál zpracovává. Papilární linie jsou k podložce více přilehlé než mezery mezi nimi, takže mají vyšší kapacitní odpor. [27]

Výhody – malý rozměr, jednoduchý princip funkčnosti, vysoká kvalita. [27]

Nevýhody – doba životnosti je krátká (dochází ke zničení snímače vlivem statické elektřiny), snímače je většinou nutné měnit v rozmezí 3 let. [27]

5.3.4 Teplotní biometrické snímače

Teplotní snímače obsahují malý citlivý čip (pyrodetektor). Pyrodetektor snímá rozdíl teplot mezi jednotlivými papilárními liniemi a prostoru mezi nimi. Pro získání obrazu otisku prstu je nutné přejíždět prstem přes citlivou plochu. Na výstupu je získán obraz otisku ve formě digitálních pásů. Digitální pásy se následně skládají do výsledného obrazu otisku. [24]

Nevýhody – nízká kvalita, problémy s algoritmy pro zpracování markant. Vzhledem ke snímání otisků pouze pohybem prstu může být po několika sejmutích pokaždé sejmuta

jiná část prstu. Tím pádem je obtížné vytvořit databázi otisků. Špatná kvalita obrazu otisku dále činí tento snímač nevhodným pro použití v přístupových systémech. [27]

5.3.5 Elektroluminiscenční biometrické snímače

Princip činnosti je založený na využití speciální vrstvy, která reaguje na tlak způsobený luminiscenčním efektem. Důležité z hlediska funkčnosti je světlo – eliminující vrstva, která filtruje světlo z míst, kde na ni tlačí papilární linie. Zpracování je zajištěno pomocí fotodiod, výstup je v digitální podobě. [27]

Výhody – terminály mají miniaturní rozměry a nabízejí velmi dobrý poměr poskytovaného rozlišení k prodejní ceně. Terminály dovedou číst při srovnatelné kvalitě i extrémně suché otisky. [27]

Nevýhody – jsou dány konstrukčním řešením: menší odolnost proti mechanickému poškození, náchylnost proti znečištění prachem či vodou. [27]

5.3.6 Radiofrekvenční biometrické snímače

Princip činnosti spočívá v připojení generátoru střídavého signálu na 2 rovnoběžné desky (jedna deska je plocha snímače a druhá plocha otisku prstu). Jelikož je vlnová délka mnohem větší než délka desek, vyskytuje se pouze složka elektrického pole bez pole magnetického. Pokud tedy jedna z desek bude náš otisk prstu, tvar pole se změní a bude kopírovat tvar papilárních linií. Vodivé prostředí mezi prstem a plochou je docíleno pomocí vodivé plochy kolem každého snímače, a proto i suché prsty nejsou problémem, jelikož se pracuje s živou tkání těsně pod povrchem pokožky. Zvlněním pole, které je způsobené přiloženým otiskem prstu, dopadá na senzory signál s rozdílnou velikostí signálu. Výběžky mají větší signál a tzv. údolí nižší signál. Kapacitní senzory tak měří rozdílnou permitivitu mezi výběžky a údolími. [27]

Výhody – technologie je odolná vůči nečistotám. Technologie trueprint je přizpůsobivá stavu kůže (vysušená pokožka, částečně poškozená kůže), pořizuje několik snímků, které jsou postupně optimalizovány až do doby buď přesného přijetí, nebo odmítnutí snímků. [27]

5.3.7 Multispektrální biometrické snímače

Multispektrální zobrazovací technologie je schopna snímat a zpracovat vlastnosti prstu i pod povrchem kůže. Senzor se skládá ze dvou hlavních částí, kterými jsou zdroj

světla a zobrazovací systém. Tyto systémy využívají více osvětlovacích soustav o rozdílných vlnových délkách. Světlo projde pod povrch kůže a senzor umožní shromáždit více identifikačních údajů z prstu. Multispektrální technologie může spolehlivě fungovat za extrémních podmínek okolního prostředí (stříkající a tekoucí voda, vliv okolního světla, apod.). U nevýrazných otisků nebo při slabém stisknutí je schopna tento obraz z otisku dotvořit, a tudíž zabránit odmítnutí identifikace. Multispektrální technologie založená na spektrální analýze obrazu používá více vlnových délek světla k identifikaci otisku. Ty snímají biometrické údaje i pod povrchem kůže a tím zabraňují neoprávněné osobě s falešným otiskem správné identifikaci pod jiným uživatelským účtem. [27]

5.3.8 IEVO Ultimate

Z výše uvedených technologií snímání otisků prstů se nejlépe hodí pro podmínky vybrané společnosti multispektrální biometrický snímač otisků prstů iEvo Ultimate. Jedná se o snímač s vysokou úspěšností snímání i u problematických prstů. Je také vhodný pro venkovní použití s vysokou odolností vůči vnějším vlivům. [28]

Obr. 36. *Čtečka otisků prstů iEvo Ultimate* [28]

Tab. 9. *Technické parametry IEVO Ultimate* [28]

Parametr	Popis
Technologie snímače	optická multispektrální
Způsob ověření identity	identifikace (1:N)
Kapacita paměti vzorů	8.000
Připojení k PC	Ethernet
Software pro správu	iEvo SW (v dodávce čtečky)
Napájecí napětí	12 Vss
Odběr	600 mA
Výstup	Wiegand (nastav. délka)
Rychlost identifikace	< 0.7 sec
Pracovní teplota	-20 - 70 °C
Použití v exteriéru	Ano (IP 65)
Rozměry (v x š x h)	137 x 76 x 91 mm
Další funkce	volitelný režim aktivace piezo tlačítkem; vysoká úspěšnost identifikace i u nekvalitních otisků; oddělená vyhodnocovací jednotka od snímací hlavy

5.3.9 Zhodnocení využití ve výrobní společnosti

Využití snímače otisků prstů pro přístupový a docházkový systém v podmínkách vybrané výrobní společnosti je uplatnitelný na určitých místech a pouze za určitých podmínek. Jedná se o jednu z nejčastěji využívaných biometrických identifikací. Její aplikace do výrobní společnosti by ale mohla způsobit problém. Důležitou otázkou zůstává, zda bude přijata všemi osobami, které chtějí vstoupit do areálu společnosti. Snímání otisků prstů je uživatelsky velmi přívětivé a jednoduché. Stačí pouze přiložit prst na snímač. Moderní snímače mají rychlost identifikace < 1 sekunda. Proto by plynulost průchodu přes turnikety neměla znamenat žádný problém. Využití ve výrobní společnosti z hlediska evidence osob má značný problém. Do areálu společnosti vstupují nejen samotní zaměstnanci, ale i zaměstnanci externích firem umístěných v areálu společnosti. Dále také osoby, které se v areálu zdržují jen dočasně, jako řidiči kamionů, návštěvníci společnosti, servisní firmy a dovozci zboží, apod. Pro tyto osoby musí být uděleno přístupové právo. Díky využití identifikace pomocí otisků prstů jsou všem osobám sejmuty tzv. citlivé osobní údaje. Podmínky pro uchovávání těchto údajů jsou uvedeny v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých právních předpisů. Nejdůležitější věcí je ale, že musí být dán písemný souhlas. Díky této skutečnosti je možné tuto metodu zavést pro vstup zaměstnanců, kteří vstupují do areálu dlouhodobě. Je ale značně nepraktické pro osoby, které vstupují krátkodobě. Zůstává také otázkou, zda všechny osoby dají souhlas k využití citlivých údajů pro vstup do areálu.

Pokud chceme využít vstup do areálu pomocí otisků prstů, z technologického hlediska je pro dané podmínky nejlépe použitelný multispektrální snímač. Většina vstupů se nachází mimo interiér, jsou tedy často vystaveny nepříznivým přírodním podmínkám. Jsou vhodné také z důvodu, protože se jedná o výrobní společnost, takže se dá předpokládat, že ruce osob mohou být znečištěné nebo jakkoliv poškozené. Všechny tyto neduhy dokáže multispektrální snímač překonat. Díky použití více vlnových délek světla k verifikaci otisku, které snímají i pod povrchem kůže, zabraňuje multispektrální snímač vytvoření falešného otisku a tím zabrání vstupu neoprávněné osoby do areálu. Jelikož dochází k přímému kontaktu se snímačem, může zde nastat problém s nechtěným přenosem nemocí.

Z hlediska použití na jednotlivých vrátnicích, se nejlépe tato metoda hodí na vrátnice umožňující vstup osob. Jedná se o vrátnice O1, O2, O3, O4. Nejlépe se tato metoda hodí pro vrátnici O1. Na této vrátnici je největší počet průchodů osob do a z areálu. Naštěstí technologie je dostatečně rychlá, aby zvládala rychlou verifikaci, i když v danou dobu prochází vrátnicí větší počet osob. To může nastat v době, kdy začínají a končí pracovní směny. Vrátnice se nalézá uvnitř budovy, a tak není vystavena přírodním podmínkám. Chybnou verifikaci by mohly způsobit znečištěné ruce. Na vrátnicích O2, O3, O4 je použití této metody také vhodné. Tyto vrátnice nejsou tak zatíženy průchodem osob jako vrátnice O1. Jejich hlavní nevýhodou ale je, že se nalézají ve venkovních prostorách a může tak dojít k chybné verifikaci při snímání otisků prstů, z důvodu nestálých přírodních podmínek (sluneční svit, prudký déšť, velký zima apod.). Využití na vrátnicích D1, D2, D3, D4 je dost nepraktické jelikož slouží pro vjezd a výjezd dopravních prostředků. Pro povolení vjezdu nebo výjezdu by byl zaregistrován pouze řidič a nikoliv auto nebo kamion. Dále by nastával problém při registraci více osob, které se mohou nalézat např. v automobilu. Na těchto vrátnicích by mohla tato metoda fungovat pouze jako doplněk ke stávajícímu přístupovému systému.

Výhodou využití této metody přístupu pro výrobní společnost je, že odpadá nutnost pořizování a využívání čipových karet. Tím dojde ke značnému zjednodušení pro postup přístupu do areálu. Odpadá nutnost mít několik různých čipových karet na různé varianty přístupu (návštěvní, osobní, krátkodobá). Dochází také ke značnému administrativnímu zjednodušení, jelikož odpadá potřeba řešit problémy spojené se ztrátou, odcizením nebo zapomenutím karty.

Další výhodou použití snímačů otisků prstu je cena. Ta se pohybuje v cenové relaci od 3 000 do 18 000 Kč. Díky tomu by pořizovací náklady nemusely být tak velké.

Tab. 10. *Použití otisků prstů na jednotlivých vrátnicích*

	O1	O2	O3	O4	D1	D2	D3	D4
Snímače otisků prstů	*	*	*	*				

5.4 Snímače geometrie ruky

Technologie je založená na principu kombinace délky, šířky a hloubky, měřené na všech pěti prstech jedné ruky. Jejich tvar a tedy i rozměry jsou jedinečné a je možné na nich založit relevantně přesnou verifikaci osob. Je to dáno i tím, že identifikační charakteristiky ruky se od dospělosti nemění. Případné změny jsou způsobené buď změnou hloubky prstů a dlaně jako takové, nebo některými nemocemi, popřípadě úrazy. Skenery ignorují délku nehtů, které se v čase velmi rychle mění a dynamicky ovlivňují měřené charakteristiky.

Postup je takový, že nejprve uživatel klade ruku na vodorovnou plochu skeneru, která je opatřena speciálními fixačními kolíky, které slouží k tomu, aby při každém snímání byla poloha ruky co nejvíce stejná. Pro osvícení se používají infračervené LED diody. Soustava zrcadel umožňuje odraz obrazu do snímací kamery a zároveň podstatně snižuje rozměry a hmotnost celého zařízení. Současné skenery snímají geometrické charakteristiky v desítkách, někdy i ve stovkách bodů během jediné sekundy. Aby byl odražený obraz jasný a kontrastní, snímací deska je vytvořena z leštěného materiálu, který má velkou optickou odrazivost. Snímání se provádí za pomoci CCD (Charged Coupled Devices) digitální kamery s přibližně 32 000 pixely. Skener snímá pouze siluetu dlaně. To znamená, že otisky prstů nebo dlaně, tetování, jizvy ani barva pokožky není brána v úvahu. Snímání je černobílé. [29]

Výhody:

- uživatelsky i technologicky velmi jednoduchá a rychlá,
- odolná vůči špinavým rukám,
- velmi malá velikost referenční šablony (9 bytů),
- uživatelsky mnohem přijatelnější než jiné biometrické technologie. [29]

Nevýhody:

- přesnost je poměrně nízká,
- náchylná k vytvoření umělé kopie tvaru dlaně a prstů,
- citlivý na poranění či fyzické změny ruky,
- rozměry skeneru jsou dány rozměry lidské ruky,
- použití pouze v interiéru. [29]

5.4.1 HandKey II

Jedná se o zařízení firmy IR Recognition Systems, využívající technologii rozpoznávání geometrie ruky. Toto zařízení je jedno z nejprodávanějších na trhu, a proto by bylo možné jej využít v naší výrobní společnosti. Jde o autonomní zařízení pro kontrolu vstupu a evidenci docházky, vhodné zejména do těžších podmínek a provozů. Navrženo je pro dosažení maximálního stupně spolehlivosti. Představuje kompletní systém, schopný fungování bez jakéhokoliv dalšího zařízení. Je možné ho nasadit jak v malých aplikacích, například k zabezpečení jedných dveří do výpočetního střediska, tak i ve velkých aplikacích se stovkami navzájem propojených snímačů. [30]

Obr. 37. *HandKey II* [30]

Tab. 11. *Technické parametry HandKey II* [30]

Parametr	Popis
Čas verifikace	< 1 sekunda
Délka ID čísla	1-10 číslic
Nátlakový kód	1. číslice, uživatelsky definovatelný
Komunikace	RS232 / RS422 / RS485, volitelně Ethernet nebo modem
Velikost šablony	9 bytů
Vstupy	2 vstupy, požadavek odchodu, dveřní spínač
Vstup pro čtečku karet	Standardně: 26 bitů Wiegand, volitelně: mag.karta, čárový kód, smart card
Výstupy	1 výstup na zámek
Emulace čtečky karet	Wiegand, mag.karta, čárový kód, 1 programovatelný výstup
Deska pro položení ruky	Antimikrobiální, vyznačený obrys ruky
Rozměry (v x š x h)	29,6 cm x 22,5 cm x 21,7 cm
Napájení	12-24V stř./ 12-24V ss.
Hmotnost	2,4 kg (bez držáku a záložního akumulátoru)
Provozní teplota	0°C - 45°C

5.4.2 Zhodnocení využití ve výrobní společnosti

Využití snímače geometrie ruky pro přístupový a docházkový systém v podmínkách vybrané výrobní společnosti je uplatnitelná na určitých místech a pouze za určitých podmínek. V současnosti se jedná o druhou nejpoužívanější metodu biometrické identifikace. Ukázalo se, že ho uživatelé snadněji akceptují a je pro ně přijatelnější metodou geometrie ruky než jiné biometrické metody, jako je např. otisk prstu, oční sítnice, hlas atd. Z tohoto důvodu by zavedení této metody do výrobní společnosti nepředstavovalo takový problém. Zůstává zde otázka, zda by však byl akceptován všemi zaměstnanci, jelikož se jedná jako u otisků prstů o citlivý osobní údaj. Zde nastává obdobný problém, jestli je možné použít tuto metodu i na osoby, které vstupují do areálu krátkodobě. Samotná metoda snímání za pomoci geometrie ruky je velmi jednoduchá. Stačí pouze přiložit ruku na snímač. Z tohoto důvodu by nemělo nastat jakékoliv zdržení při průchodech turniketem.

Pokud vezmeme využití pro vstup do areálu pomocí geometrie ruky z technologického hlediska, její použití je značně omezeno. Snímač má jednu nespornou výhodu, a to že dokáže verifikovat i například špinavé ruce, což je značná výhoda pro použití ve výrobní společnosti. Dále také, že čas samotné verifikace je velmi krátký a to < 1 sekunda. Díky tomu by nemusel nastat problém s plynulostí průchodu přes vrátnice. Nevýhoda této metody spočívá v tom, že snímač má větší rozměry, což je dáno tím, že musí snímat celou ruku. Další nevýhodou pro zavedení ve výrobní společnosti je, že lze použít pouze v interiéru, jelikož je značně ovlivňován venkovními přírodními podmínkami. Nastává také problém,

pokud dojde například k závažnému poranění rukou, jako je amputace prstu apod. Díky tomu se pak stává tato metoda pro vstup do areálu pro tyto osoby značně nepoužitelná. Snímače geometrie ruky mají také jednu malou nevýhodu, a tou je hygiena. Jelikož princip spočívá v přímém kontaktu se snímačem, může tak snadno docházet k přenosu nemocí. Toto riziko je tím větší, že do areálu vstupuje každý den několik tisíc lidí. Dále pak nastává největší problém a to, že snímač je náchylný k vytvoření umělé kopie tvaru dlaně a prstů.

Z hlediska využití na jednotlivých vrátnicích lze podle zjištěných údajů použít pouze na vrátnici O1, která se nachází v administrativní budově. Pro ostatní vrátnice je značně nepoužitelná, jelikož se ostatní vrátnice nalézají ve venkovních prostorách. Zde by díky venkovním podmínkám mohlo docházet k chybné verifikaci. Daná zařízení na to nejsou přizpůsobena. Použití snímačů geometrie ruky je tak vhodné pro zabezpečení přístupu pouze do určitých budov, které se nalézají v areálu společnosti.

Výhodou využití této metody přístupu pro výrobní společnost je, že odpadá nutnost pořizování a využívání čipových karet. Tím dojde ke značnému zjednodušení pro postup přístupu do areálu. Odpadá nutnost mít několik různých čipových karet na různé varianty přístupu (návštěvní, osobní, krátkodobá). Dochází i ke značnému administrativnímu zjednodušení, jelikož odpadá nutnost řešit problémy jako je ztráta, odcizení nebo zapomenutí karty.

Drobnou nevýhodou pro použití snímačů geometrie rukou je cena. Ta se pohybuje v cenové relaci od 30 000 Kč do 40 000 Kč. Při použití na více místech by pořizovací náklady mohly být dosti značné.

Tab. 12. *Použití geometrie ruky na jednotlivých vrátnicích*

	O1	O2	O3	O4	D1	D2	D3	D4
Snímače Geometrie ruky	*							

5.5 Snímače krevního řečiště

Jedná se o poměrně novou metodu, která se ale rychle rozvíjí. Využívá pouhýma očima neviditelných vlastností větvení cévního řečiště ukrytého pod kůží. Pro snímání se používají cévy v prstech, dlani nebo hřbetu ruky. Struktura krevního řečiště se vyvíjí již

před narozením člověka a jeho rozpoložení je neměnné, v důsledku dospívání se mění pouze velikost a odstup jednotlivých žil. [31]

Krevní řečiště není možné snímat ve viditelném světle z důvodu vysokého rozptylu světla ve tkáni. Využívá se proto optických vlastností v erytrocytech obsaženého hemoglobinu, který částečně pohlcuje blízké infračervené záření. Tím je získána změna jasu a je možné odlišit žíly od okolní tkáně. Snímání obrazu je řešeno kamerou, která musí být schopna zaznamenat NIR záření s vlnovou délkou kolem 850 nm. [31]

Díky umístění zdroje infračerveného záření rozlišujeme tři metody:

- **Transmisní**

  Prst pokládáme mezi obrazový senzor a zdroj IR osvětlení. Prosvícením prstu se v cévách absorbuje část infračerveného záření, tím se objeví tmavá místy na pořízeném snímku. Tato metoda poskytuje relativně vysoký kontrast zobrazení žilních struktur, ale přístroj je z důvodu umístění osvětlení naproti snímači prostorově rozměrnější. [31]

- **Reflexní**

  Prst se umístí nad snímač, vedle kterého jsou rozmístěny IR LED. Osvětlením je snímáno odražené záření, které má nižší intenzitu v místech přítomnosti cév. Nevýhodou je, že záření z větší části bývá odraženo od kůže a neprostoupí hlouběji do tkáně, proto kontrast snímku pořízeného touto metodou bývá nízký. Oproti transmisní metodě však umístění osvětlovacích LED v rovině se snímačem umožňuje vyrobit přístroj menších rozměrů. [31]

- **S bočním osvětlením**

  Poslední metoda, představená firmou Hitachi, je kompromisem mezi oběma předcházejícími metodami. Zde jsou IR LED umístěny vedle prstu. Při nasvícení je záření uvnitř prstu rozptýleno a následně zachyceno obrazovým senzorem. Podle autorů je výstupem této metody kontrastní snímek a zároveň je zachována kompaktnost zařízení. [31]

Výhody:

- rychlé vyhodnocení identifikace i verifikace,
- možnost multimodálního provedení,
- žilní řečiště je jedinečné a po celý život neměnné,

- žíly jsou skryty pod pokožkou, tím pádem je jejich padělání obtížnější,
- velká akceptace u uživatelů biometrických systémů, udává se takřka 100%,
- možnost provedení v kontaktní i bezkontaktní podobě,
- rychlost snímání a vyhodnocení je zhruba 1-1,5s, [31]

Nevýhody:

- poměrně vysoká cena,
- některé skenery jsou náchylné na okolní světlo, které ovlivňuje kvalitu snímku,
- nízká nabídka skenerů na našem trhu, [31]

5.5.1 PV-WTC-Mifare

Jednou z dostupných zařízení, které by bylo možno použít ve vybrané společnosti je biometrický terminál PV-WTC. Ten je určen pro identifikaci osoby na základě jejího krevního řečiště. Doplňkově obsahuje také čtečku pro karty Mifare classic / DESFire. Lze jej nastavit buď v režimu "karta + dlaň", případně režimem "Karta nebo dlaň". Do terminálu PV-WTC je možné uložit až 300.000 dlaní a rozpoznání osoby se odehrává v časovém rámci pod 2 vteřiny. Terminál je vybaven relé i Wiegand výstupem pro pohodlné napojení přímo na dveřní zámek, nebo na přístupový systém. Biometrické předlohy dlaní a veškerá nastavení uživatelů (vč. ID čísel jejich karet) se spravují v softwaru BioSmart Studio v5. [32]

Obr. 38. *Čtečka krevního řečiště dlaně PV-WTC* [32]

Tab. 13. *Technické parametry PV-WTC* [32]

Parametr	Popis
Čas verifikace	< 2 sekunda
Napájecí napětí	10-14V DC
Proudový odběr	1000 mA
Typ čtečky	Mifare, Mifare DESfire
Vstupy	Dveřní senzor
Výstupy	Relé, Wiegand, RS-485, Ethernet
Teplota provozní	0 až +50 °C
Max. počet uživatelů	1000000
Počet záznamů v deníku	10000000
Stupeň krytí	IP54
Software	BioSmart studio v5
Další vlastnosti	skener krevního řečiště dlaně, klávesnice, 3.5" TFT display 320x240 pixelů
Rozměry (v x š x h)	215 x 150 x 117 mm
Hmotnost	0,82 kg

5.5.2 Zhodnocení využití ve výrobní společnosti

Využití snímače krevního řečiště pro přístupový a docházkový systém v podmínkách vybrané výrobní společnosti je uplatnitelná na určitých místech a pouze za určitých podmínek. Tato metoda je v oblasti přístupových systémů poměrně nová, ale její přijetí mezi uživatele je docela kladné. Z tohoto důvodu by nemuselo její zavedení ve výrobní společnosti znamenat žádný problém. Jako u otisků prstů a geometrie ruky zde nastává problém, zda bude akceptován všemi zaměstnanci nebo osobami vstupujícími do areálu společnosti. Proto, jako u předešlých metod, je vhodnější její využití pro dlouhodobý přístup než pro krátkodobý. Samotná metoda snímání krevního řečiště je velmi jednoduchá. Stačí pouze přiložit ruku ke snímači, jelikož se jedná o bezkontaktní metodu. Z tohoto důvodu by nemělo nastat jakékoliv zdržení při průchodech turnikety.

Pokud vezmeme využití pro vstup do areálu pomocí krevního řečiště z technologického hlediska, pro dané podmínky je nejlépe použitelný bezkontaktní snímač dlaně ruky. Snímač má jednu nespornou výhodu, a to že dokáže verifikovat i například špinavé ruce, což je značná výhoda pro použití ve výrobní společnosti. Jelikož se jedná o bezkontaktní způsob, nemusíme zde zohledňovat žádné hygienické podmínky. Čas samotné verifikace je velmi rychlý, a to 1 – 2 sekundy. To by nemělo jakkoliv ovlivnit plynulost průchodu přes vrátnice, a to ani v časech, kdy je maximálně vytížena. Další výhoda spočívá v tom, že žíly jsou skryty pod pokožkou, tím pádem je jejich padělání obtížnější. Menší nevýhodou

této metody jsou obdobně jako u geometrie ruky její rozměry. Tyto rozměry se ale odvíjejí od toho, kterou část budeme snímat, jestli prst, hřbet nebo dlaň. U prstu je velikost poměrně malá, ale u hřbetu nebo dlaně jsou její rozměry poněkud větší. Jednou z nevýhod pro zavedení ve výrobní společnosti je, že některé skenery jsou náchylné na okolní světlo, které ovlivňuje kvalitu snímku. Proto je výhodnější umístění tam, kde nedochází k přímému slunečnímu svitu. Dalšími přírodními podmínkami (déšť, zima) nejsou nijak ovlivněny, proto je možná jejich instalace i ve venkovním prostředí.

Z hlediska použití na jednotlivých vrátnicích, se nejlépe tato metoda hodí na vrátnice umožňující vstup osob. Jedná se o vrátnice O1, O2, O3, O4. Tak jako u ostatních metod se nejlépe hodí pro vrátnici O1. Na této vrátnici je největší počet průchodů osob do a z areálu. Vrátnice se nalézá uvnitř budovy, a tak není vystavena přírodním podmínkám. Problém co by mohly způsobit rozměry snímačů. Na vrátnicích O2, O3, O4 je použití této metody taky možné. Tyto vrátnice nejsou tak zatíženy průchodem osob jako vrátnice O1. Jejich hlavní nevýhodou je, že se nalézají ve venkovních prostorách a může tak dojít k chybné verifikaci při snímání krevního řečiště vlivem přírodních podmínek (sluneční svit). Využití na vrátnicích D1, D2, D3, D4 je sice možné, ale nepraktické. A to z důvodu, že tyto vrátnice slouží pro vjezd a výjezd dopravních prostředků. Pro povolení vjezdu nebo výjezdu by byl zaregistrován pouze řidič a nikoliv auto nebo kamion. Dále by nastával problém při registraci více osob, které se mohou nalézat např. v automobilu. Na těchto vrátnicích by mohla tato metoda fungovat pouze jako doplněk ke stávajícímu přístupovému systému.

Výhodou využití této metody přístupu pro výrobní společnost je, že odpadá nutnost pořizování a využívání čipových karet. Tím dojde ke značnému zjednodušení pro postup přístupu do areálu. Odpadá nutnost mít několik různých čipových karet na různé varianty přístupu (návštěvní, osobní, krátkodobá). Dochází i ke značnému administrativnímu zjednodušení, protože odpadá nutnost řešit problémy jako je ztráta, odcizení nebo zapomenutí karty.

Drobnou nevýhodou pro použití snímačů krevního řečiště je cena. Jelikož se jedná o novou technologii, je výběr dostupných výrobců dosti omezen. Cenová relace se pohybuje okolo 20 000 Kč až 30 000 Kč. Při použití na více místech by pořizovací náklady mohly být dost značné.

Tab. 14. *Použití krevního řečiště na jednotlivých vrátnicích*

	O1	O2	O3	O4	D1	D2	D3	D4
Snímače krevního řečiště	*	*	*	*				

5.6 NFC

NFC principiálně vychází přímo z RFID, přičemž umožňuje složitější operace mezi zařízeními. Stále umožnuje číst pasivní RFID čipy s čtečkou NFC nebo také zapisovat data do jejich omezené paměti. Umožňuje zápis dat do určitých druhů RFID čipů pomocí standardního formátu nezávisle na typu značky a výrobce. Dále je možná komunikace s ostatními zařízeními v duplexním nebo polo-duplexním módu. NFC zařízení si mohou mezi sebou vyměňovat informace o svých schopnostech, uložené záznamy nebo zahájit dlouhodobou vzájemnou komunikaci. Nejčastější použití pro identifikaci je buď pomocí mobilním telefonem nebo NFC tagů. Mobilní telefony s podporou NFC jsou nejvýznamnějšími zařízeními. Integrace NFC do mobilních telefonů je velkou příležitostí pro snadné použití, rozšíření a přijetí této technologie. NFC tag je čip, který nemá integrovaný zdroj napájení. Běžně použití je v platebních kartách, chytrých vizitkách, přístupových systémech apod. [33]

Jedná se o bezdrátovou technologii, které má krátký dosah přibližně na vzdálenost do 4 cm. NFC je definováno skupinou standardů bezkontaktních karet. Jsou to standardy bezkontaktních čipových karet ISO/IEC 14443, FeliCa a ISO/IEC 15693. První dva standardy pracují na frekvenci 13,56 MHz. Jejich obvyklé přenosové rychlosti jsou od 106 kbit/s do 424 kbit/s. Vzdálenost třetího standardu je 1,5 m. Díky této vzdálenosti je přenosová rychlost výrazně nižší. Pohybuje se okolo 26 kbit/s. Rozšíření standardu je specifikováno pomocí standardu NFCIP, rozšiřuje standard ISO/IEC 14443 o další specifikace, což definuje komunikaci mezi dvěma zařízeními, nazývá se ISO/IEC 18092. [33]

Výhody:

- poměrně krátký čas pro navázání spojení mezi zařízeními,
- jednoduché ovládání,
- poměrně vysoká bezpečnost komunikace,
- univerzálnost (možnost provádět více úkonů),

- kompatibilita s ostatními zařízeními,
- podpora ostatních technologií (Wi-Fi Bluetooth),
- kompatibilita s RFID. [33]

Nevýhody:

- v současnosti jen u novějších mobilních telefonů,
- vyšší pořizovací náklady,
- krátký dosah. [33]

5.6.1 Zhodnocení využití ve výrobní společnosti

Využití bezkontaktní identifikace pomocí technologie NFC pro přístupový a docházkový systém v podmínkách vybrané výrobní společnosti je možné na všech přístupových místech. Jelikož je technologie principiálně podobná jako současně používaná metoda přístupu pomocí RFID, bylo by její zavedení osobami vstupujícími do areálu společnosti velmi dobře akceptovatelné a pro některé i nepostřehnutelné. Díky možnosti kompatibility s RFID by se v podstatě nijak neměnily metody přístupu a bylo by možné nadále využívat stávajících identifikačních karet. Největší výhodou zavedení NFC spočívá v tom, že by pro vstup do areálu mohla být využita alternativa, a to za pomoci mobilních telefonů. To by odstranilo nutnost použití identifikačních karet pro některé osoby. Výhodou použití mobilních telefonů pro přístup je jejích komfortní řešení. Pro vstup by osoba mohla použít svůj vlastní mobilní telefon, do kterého by jenom bylo nutno nainstalovat příslušnou aplikaci. Díky této aplikaci by bylo možné zadávat také např. důvody přerušení pracovní doby apod. Použití mobilního telefonu pro přístup lze jak pro dlouhodobý přístup, tak především pro krátkodobý přístup do areálu. Nevýhodou ovšem zůstává, že jenom malé množství mobilních telefonů zatím podporuje NFC. A ne všechny osoby by zvládly používat tuto novou technologii.

Z technologického hlediska je použití pro vstup do areálu pomocí technologie NFC značně výhodné. Největší výhoda spočívá především v rychlém navázání spojení mezi zařízeními a poměrně vysoké bezpečnosti komunikace. Díky této skutečnosti by neměl nastat žádný problém v plynulosti průchodu přes turnikety. Dále by bylo obtížnější padělání přístupových karet a získání neoprávněného přístupu do areálu. Jak již vyplívá z dané metody, zde nás netrápí žádné hygienické problémy které nás trápily u předchozích metod.

Z hlediska použití na jednotlivých vrátnicích se tato technologie hodí pro všechny vrátnice. Jak pro vrátnice pro vstup osob O1, O2, O3, O4, tak na vrátnice pro vjezd D1, D2, D3, D4. Jelikož se jedná o podobný princip jako u současného přístupového systému, nejsou zde žádné nevýhody, které by omezovaly použití na jednotlivých vrátnicích. Zde nás také netrápí důvody, které by nás omezovaly pro použití ve venkovních prostorách. Působení přírodních podmínek nemá na NFC žádný negativní účinek.

Výhodou využití této technologie přístupu pro výrobní společnost především spočívá v rychlosti a bezpečnosti identifikace. Díky využití mobilních telefonů jako identifikátoru také odpadá nutnost pořizování většího množství identifikačních karet a ponechání si těch původních. Dalším kladem je, že přístupový systém se stane uživatelsky přívětivějším a do značné míry jednoduší. Odstraní se tím i zátěž spojená s administrativní činností vystavováním nových identifikačních karet.

Další výhodou použití NFC je cena. Ta se pohybuje v cenové relaci od 1 000 Kč do 6 000 Kč. Díky tomu by pořizovací náklady nebyly tak vysoké.

Tab. 15. *Použití NFC na jednotlivých vrátnicích*

	O1	O2	O3	O4	D1	D2	D3	D4
NFC	*	*	*	*	*	*	*	*

5.7 Dílčí závěr

Tato kapitola popisuje nejnovější metody přístupu, které jsou v současnosti nejpoužívanější u přístupových a docházkových systémů. Mezi vybrané byly zvoleny metody přístupu za pomoci otisků prstů, geometrie ruky, krevního řečiště a bezdrátové identifikace za pomoci NFC. Ty byly posléze zhodnoceny pro podmínky námi vybrané rozsáhlé výrobní společnosti. Jedním z důležitých parametrů bylo vyhodnocení, na které z přístupových vrátnic by bylo vhodné dané metody přístupu uplatnit. V tabulce níže jsou vypsány jednotlivé metody přístupu a vrátnice pro vstup do areálu. Červená hvězdička zobrazuje, na kterých vrátnicích by bylo dobré uplatnit jednotlivé metody přístupu.

Tab. 16. *Použití přístupových metod na jednotlivých vrátnicích*

	O1	O2	O3	O4	D1	D2	D3	D4
Snímač otisků prstů	*	*	*	*				
Snímač geometrie ruky	*							
Snímač krevního řečiště	*	*	*	*				
NFC	*	*	*	*	*	*	*	*

Aby bylo možné přístupové metody uplatnit na jednotlivých vrátnicích, musí splňovat určité podmínky, které vycházejí z analýzy vybrané rozsáhlé výrobní společnosti. Tyto základní podmínky jsou zobrazeny v tabulce níže. Zde je pak znázorněno, jestli dané podmínky splní nebo nesplní, a to vyjádřením buď slovem „Ano“ nebo „Ne“.

Tab. 17. *Podmínky pro jednotlivé metody*

	Otisky Prstů	Geometrie ruky	Krevní řečiště	NFC
Uživatelská přívětivost	Ano	Ano	Ano	Ano
Jednoduchost ovládání	Ano	Ano	Ano	Ano
Venkovní použití	Ano	Ne	Ano	Ano
Dlouhodobý vstup	Ano	Ano	Ano	Ano
Krátkodobý vstup	Ne	Ne	Ne	Ano
Rychlá verifikace	Ano	Ano	Ano	Ano
Cena (v tis.)	3 - 18	30 - 40	20 - 30	1 - 6
Osoby	Ano	Ano	Ano	Ano
Dopravní prostředky	Ne	Ne	Ne	Ano
Hygiena	Ne	Ne	Ano	Ano
Bezpečnost	Ano	Ne	Ano	Ano
Spolehlivost	Ano	Ano	Ano	Ano

Každá z vybraných metod přístupu má své klady a zápory. Proto je velmi problematické jejich umístění na všech přístupových místech. Jedná se totiž o velmi komplexní výrobní společnost. Do společnosti každý den vstupuje několik tisíc osob a probíhá zde vjezd a výjezd mnoha dopravních prostředků. Převážná část osob zde vstupuje dlouhodobě, ale je zde několik osob, které navštíví areál společnosti krátkodobě. Dále je zde několik vstupů, které se nalézají na všech stranách areálu. Většina těchto vstupů se nalézá ve venkovních podmínkách. Díky těmto skutečnostem je velmi obtížné zvolit novou metodu přístupu. Jako nejlepší varianta připadá bezdrátová identifikace pomocí NFC. Ta se jeví jako vhodné řešení pro všechna přístupová místa a splňuje veškeré podmínky.

Další variantou by mohlo být použití více metod najednou. Jako nejlepší řešení se zde jeví použití otisků prstů s NFC. Pro zaměstnance vlastní i zaměstnance externích firem by byl použit přístupový systém založený na otiscích prstů. Pro ostatní osoby vstupující do areálu a pro vjezdy a výjezdy dopravních prostředků by byl použit přístupový systém založený na bezdrátové identifikaci pomocí NFC.

ZÁVĚR

V této diplomové práci se zabýváme provedením studie modernizace přístupových a docházkových systémů pro podmínky rozsáhlé výrobní společnosti. Zvolená rozsáhlá výrobní společnost je mezinárodní výrobce důležitých částí automobilů. Zaměstnává několik tisíc osob a v samotném areálu se nachází několik externích firem. Každý den tedy vstoupí do areálu společnosti několik tisíc osob. Díky dlouhodobému používání a opotřebení současného přístupového a docházkového systému je kladen požadavek na modernizaci, a to především pomocí biometrických metod.

V teoretické části diplomové práce jsou popsány systémy kontroly vstupu. Jsou zde uvedeny základní funkce, které má systém splňovat a jeho struktura. První kapitola se zabývala veškerými normami, které se vztahují k systému kontroly vstupu. Tyto normy v současnosti prošly aktualizací a jsou v nich stanoveny nové podmínky pro aplikaci systému kontroly vstupu.

Druhá kapitola teoretické části uváděla současné technologické trendy v oblasti přístupových a docházkových systémů. Zde jsou popsány různé metody přístupu a identifikace. Od těch nejzákladnějších jako je použití PINu, až po ty nejmodernější a v současnosti nejpoužívanější metody.

Třetí kapitola teoretické části se zabývala analytickými a prognostickými metodami. Uvádí se zde jednotlivé analytické i prognostické metody, které jsou rozčleněny na kvantitativní a kvalitativní. Následně jsou u každé z metod popsány ty nejznámější a nejpoužívanější z nich. V závěru pak dochází ke srovnání analytických a prognostických metod.

Praktická část diplomové práce ve čtvrté kapitole analyzuje současný přístupový a docházkového systému vybrané rozsáhlé výrobní společnosti. Je zde popsána základní charakteristika firmy. Dále jsou uváděny jednotlivé prvky, které přístupový a docházkový systém využívá, různé způsoby, jakými lze získat přístup do areálu firmy. Co vše je vyžadováno a co musí být splněno. V závěru jsou popsány jednotlivé vrátnice, které jsou určeny pro vstup do areálu společnosti. V práci jsou graficky znázorněny. Je analyzováno jejich vytížení v nejpoužívanější dobu.

V poslední kapitole praktické části je provedena studie nových metod přístupových a docházkových systémů pro podmínky dané rozsáhlé výrobní společnosti. Zde je zmíněn

zákon č. 101/2000 Sb., o ochraně osobních údajů, včetně nařízením EU 2016/679, o ochraně osobních údajů. Tyto právní předpisy nás ovlivňují převážně u biometrických metod. Dále práce uvádí v současnosti nejpoužívanější metody přístupu, které by byly možné aplikovat pro podmínky dané výrobní společnosti. Následně dochází ke zhodnocení jednotlivých metod a doporučení, na které z vrátnic mají být aplikovány.

Cílem a hlavním přínosem diplomové práce je uvedení přehledu o současných nejnovějších dostupných metodách přístupu a doporučení bezpečnostním manažerům uvedené společnosti, jak zvolit to nejefektivnější řešení pro modernizaci přístupových a docházkových systémů vybrané rozsáhlé výrobní společnosti.

SEZNAM POUŽITÉ LITERATURY

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

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

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

[4] ČSN EN 50130-4 ed. 2. *Poplachové systémy – Část 4: Elektromagnetická kompatibility- norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012. 28 s. Třídící znak 334590

[5] ČSN EN 50130-5 ed. 2. *Poplachové systémy – Část 5. Metody zkoušek vlivu prostředí.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012. 28 s. Třídící znak 334590

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

[7] *Autentizace a identifikace uživatelů*. ÚVT MU zpravodaj [online]. Brno [cit. 2017-03-02]. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/560.html

[8] UHLÁŘ, Jan. *Technická ochrana objektů* [online]. Vyd. 1. Praha: Vydavatelství Policejní akademie České Republiky, 2006, 246 s. [cit. 2017-03-02]. ISBN 80-725-1235-8.

[9] SUCHÁČEK, Lukáš. *Systémy elektronické kontroly vstupu a návrh rozšíření jejich funkčnosti*. Zlín, 2012. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

[10] NORMAN, Thomas L. *Electronic access control*. Waltham: Elsevier, c2012, 1 online zdroj (xx, 423 s.). ISBN 978-0-12-382029-7. Dostupné také z: http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=407848

[11] ŠMIGALA, Andrej. *Možnosti využití technologie NFC na mobilních platformách založených na OS Android*. Brno, 2013. Bakalářská práce. Masarykova univerzita.

[12] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. Profesionál. ISBN 978-80-247-2365-5.

[13] MEDKOVÁ, Hana. *Metody realizace bezpečnostního posouzení objektu*. FAI UTB, 2014. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Jan Valouch Ph.D.

[14] KUČÍK, Kamil. *Metody bezpečnostního posouzení administrativních objektů*. FAI UTB, 2015. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Jan Valouch Ph.D.

[15] VALOUCH, Jan. *Projektování integrovaných systémů* [online]. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2011.

[16] ŠTĚDROŇ, Bohumír, POTŮČEK, Martin, KNÁPEK, Jaroslav, MAZOUCH, Petr a kol. *Prognostické metody a jejich aplikace 1*. vydání. Praha: C. H. Beck, 2012. ISBN 978-80-7179-174-4. 198 s.

[17] VALOUCH, Jan a Martin HROMADA. *Bezpečnostní futurologie*. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2016. ISBN 978-80-7454-621-1.

[18] ŠEVČÍK, Jiří. *Bezpečnostní posouzení objektu*. Zlín, 2010. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Jan Valouch, Ph.D.

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

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

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

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

[23] STANOVISKO č. 3/2009 *Biometrická identifikace nebo autentizace zaměstnanců* [online]. In: . s. 4 [cit. 2017-05-08]. Dostupné z: https://www.uoou.cz/files/stanovisko_2009_3.pdf

[24] Reforma ochrany osobních údajů, firmy čekají nové povinnosti. *Podnikatel.cz* [online]. [cit. 2017-05-08]. Dostupné z: http://www.podnikatel.cz/clanky/reforma-ochrany-osobnich-udaju-firmy-se-musi-pripravit-na-radu-novinek/

[25] KONČICKÝ, Martin. *Biometrický snímač otisků prstu*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 70 s. (78 233 znaků). Dostupné také z: http://hdl.handle.net/10563/24672. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav bezpečnostního inženýrství. Vedoucí práce Drga, Rudolf.

[26] BOUŠKA, Petr. *Biometrické systémy: zpracování otisku prstu včetně možnosti rekonstrukce otisku z biometrické šablony* [online]. Brno: Fakulta Informatiky, 2007. 66 s. Diplomová práce. Masarykova univerzita, Fakulta Informatiky. Dostupné z WWW:<http://is.muni.cz/th/50818/fi_m/diplomova_prace.pdf?lang=en>.

[27] Biometrie otisku prstu. Biometricke-ctecky.cz [online]. [cit. 2017-05-07]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/

[28] Biometrická čtečka otisků prstů iEvo Ultimate. *Adiglobal* [online]. 2017 [cit. 2017-05-08]. Dostupné z: http://www.adiglobal.cz/cz/produkty130:10209849/biometricka ctecka-otisku-prstu-ievo-ultimate-cerna-barva

[29] HRNČIŘÍK, Matej. *Otestování možností biometrického systému - technologie geometrie ruky* [online]. Vysoké učení technické v Brně. Fakulta informačních technologií, 2010 [cit. 2017-05-10]. Dostupné z: http://hdl.handle.net/11012/56106. Bakalářská práce. Vysoké učení technické v Brně. Fakulta informačních technologií. Ústav inteligentních systémů. Vedoucí práce Dana Lodrová.

[30] HandKey 2 | MOVIBIO s.r.o. *MOVIBIO s.r.o. - vítejte v našem internetovém obchodě | MOVIBIO s.r.o.* [online]. [cit. 2017-05-10]. c2009-2017 Dostupné z: http://www.movibio.cz/kontrola-vstupu-a-dochazky/handkey-2.htm

[31] BĚLEHRÁBEK, Stanislav. *Biometrie krevního řečiště prstu*. Brno, 2015. Bakalářská práce. Vysoké Učení Technické v Brně. Vedoucí práce Ing. Martin Mézl.

[32] PV-WTC-Mifare|Katalog ABBAS. *ABBAS, a.s.* [online]. c2010-2017 [cit. 2017-05-11]. Dostupné z: http://katalog.abbas.cz/pv-wtc-mifare-s30374/

[33] GRIGAR, Jiří. *Identifikace firemních objektů s využitím technologie NFC v mobilních zařízeních.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2015, 67 s. (91 382 znaků). Dostupné také z: http://hdl.handle.net/10563/34116. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav informatiky a umělé inteligence. Vedoucí práce Vala, Radek.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

%	Procenta
§	Paragraf
1D	Jednorozměrná
2D	Dvourozměrná
3D	Třírozměrná
apod.	A podobně
atd.	A tak dále
CCD	(Colony Collapse Disorder) Syndrom zhroucení včelstev
CCTV	Uzavřený televizní okruh
CE	Označení shody
cm	Centimetry
č.	Číslo
ČR	Česká republika
ČSN	České technické normy.
D1	Bezobslužná vrátnice pro osobní vozidla
D2	Nákladní vrátnice
D3	Pomocná nákladová výjezdní vrátnice
D4	Náhradní vjezd
DNA	Deoxyribonukleová kyselina (deoxyribonucleic acid).
EACS	Elektronický systém kontroly vstupu
EAN	Mezinárodní číslo obchodní položky (European Article Number).
ed.	Edice
EEPROM	Elektricky vymazatelná PROM, paměť
EMC	Elektromagnetická kompatibilita

EN	Evropské normy.
ES	Evropská společenství
FAR	Četnost falešných přijetí
FTIR	Experimentální spektroskopická technika
GDPR	(General Data Protection Regulation) Obecné nařízení o ochraně údajů
GSM	Globální systém pro mobilní komunikace
h	Hloubka
HZS	Hasičský záchranný sbor
IEC	Mezinárodní úřad pro elektrotechniku
IP	Protokol internetu
IR	Infračervené záření
ISO	Mezinárodní normy
IT	Informační technologie
Kb (kbit)	Kilobit
kg	Kilogram
kHz	Kilohertz
LAN	Místní síť
LCD	Displej z tekutých krystalů
LED	Dioda emitující světlo (Light-Emitting Diode)
m^2	Metry krychlové
mA	Miliampér
MHz	Megahertz
mm	Milimetry
např.	Například
NFC	Komunikace v blízkém poli
NIR	Blízká infračervená oblast

nm	Nanometry
NV	Nařízení vlády
º C	Stupeň Celsia
O1	Vrátnice v administrativní budově
O2	Bezobslužná vrátnice s 2 turnikety
O3	Bezobslužná vrátnice s 1 turnikety
O4	Bezobslužná vrátnice u D2
OP	Občanský průkaz
PC	Osobní počítač
PDI	Palec na bod
PIN	Osobní identifikační číslo
PUK	(Personal Unblocking Key) Osobní odemykací klíč
PZTS	Poplachové zabezpečovací a tísňové systémy
R	Rozlišení skeneru
R/O	(read/only) Nepřepisovatelné
R/W	(read/write) Přepisovatelné
REX	(request to exit divice) zařízení pro uvolnění východu
RFID	Identifikace pomocí rádiové frekvence
ŘP	Řidičský průkaz
s	Sekunda
Sb.	Sbírky
SIM	Účastnická identifikační karta
SKV	Systém kontroly vstupu
š	Šířka
T1	Terminál 1
T2	Terminál 2

T3	Terminál 3
T4	Terminál 4
TV	Televize
Tzv.	Tak zvané.
USB	Univerzální sériová sběrnice
V	Volty
v	Výška
Vss	Volt stejnosměrného napětí

SEZNAM OBRÁZKŮ

SEZNAM TABULEK