Přístupové systémy pro subdodavatele v leteckém a vojenském průmyslu

Jan Štípek

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

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

Jméno a příjmení:	**Jan Štípek**
Osobní číslo:	**A15157**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Přístupové systémy pro subdodavatele v leteckém a vojenském průmyslu**
Téma anglicky:	**Access Systems for Subcontractors in the Aviation and Military Industries**

Zásady pro vypracování:

1. **Vysvětlete normy, požadavky a certifikace pro letecký a vojenský průmysl.**
2. **Proveďte analýzu současných řešení přístupových systémů.**
3. **Proveďte návrh systému s ohledem na požadavky pro letecký a vojenský průmysl.**
4. **Vytvořte kritéria pro hodnocení dodavatelů systému.**
5. **Odhadněte další vývoj přístupových systémů.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-05-7.**
2. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management III. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-35-4.**
3. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-57-6.**
4. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. 3. vydání. Blatná: Cricetus, 2006. ISBN 978-80-902938-2-3.**
5. **ČSN EN 60839-11-1. Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty. Praha: Český normalizační institut, 2014.**
6. **ČSN EN 60839-11-2. Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace. Praha: Český normalizační institut, 2016.**

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

Datum zadání bakalářské práce: **8. prosince 2017**

Termín odevzdání bakalářské práce: **24. května 2018**

Ve Zlíně dne 12. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

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

Ing. Jan Valouch, Ph.D.
ředitel ústavu

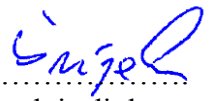
Prohlašuji, že

- beru na vědomí, že odevzdáním 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 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 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 23.5.2018



.....

podpis diplomanta

ABSTRAKT

Práce řeší požadavky na přístupové systémy v oblasti leteckého a vojenského průmyslu. Protože jsou zde vysoké požadavky na kvalitu, je třeba zpracovat požadavky standardů, norem a certifikace. Bude zpracován konkrétní návrh přístupového systému a vytvořeny kritéria hodnocení dodavatelů těchto systémů.

Klíčová slova: Systémy kontroly vstupu, přístupový systém

ABSTRACT

The thesis addresses requirements for access systems in the field of aviation and military industry. Because there are high quality requirements, standards, standards, and certifications need to be developed. Specific proposals for the access system will be developed and evaluation criteria for contractor will be developed for these systems.

Keywords: ACS, access control system

Poděkování:

Rád bych poděkoval především své rodině a svým přátelům za podporu a pomoc při mém studiu a také vedoucímu mé bakalářské práce Ing. Rudolfu Drgovi, Ph.D. za jeho cenné připomínky, ochotu pomoci a vstřícný přístup.

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 OBECNÝ POPIS SYSTÉMŮ PRO KONTROLU VSTUPU **11**
1.1 PŘÍSTUPOVÝ BOD 12
1.2 ZPŮSOBY IDENTIFIKACE 13
1.2.1 Identifikace heslem 13
1.2.2 Identifikace předmětem 14
1.2.3 Biometrická identifikace 14
1.2.4 Kombinace metod 15
1.3 IDENTIFIKAČNÍ PRVKY A JEJICH SNÍMÁNÍ 15
1.3.1 Optický identifikační systém 15
1.3.2 Magnetický identifikační systém 16
1.3.3 Čipy a čipové karty (Smart Cards) 17
1.3.4 Bezkontaktní identifikační systém RFID 17
1.3.5 Biometrické identifikační prvky 18
1.3.5.1 Otisk prstu 19
1.3.5.2 Geometrie ruky 20
1.3.5.3 Oční sítnice 20
1.3.5.4 Oční duhovka 21
1.3.5.5 Rozpoznání obličeje 21
1.3.5.6 Dynamika podpisu 21
1.3.5.7 Dynamika stisku kláves 21
2 ANALÝZA LEGISLATIVNÍCH POŽADAVKŮ A NOREM **22**
2.1 LEGISLATIVA ČR 22
2.1.1 Norma ČSN EN 60839-11-1 23
2.1.2 Norma ČSN EN 60839-11-2 24
2.2 NORMY A CERTIFIKÁTY PRO LETECKÝ A VOJENSKÝ PRŮMYSL 24
2.2.1 Management kvality 24
2.2.2 České obranné standardy: 24
2.2.3 Německé vojenské standardy 25
2.2.4 Normy IPC 25
2.2.5 Americké standardy a normy MIL 26
2.2.6 Akreditace NADCAP 27
3 SOUČASNÁ ŘEŠENÍ PŘÍSTUPOVÝCH SYSTÉMŮ **28**
3.1 ROZDĚLENÍ SNÍMACÍCH ZAŘÍZENÍ – ČTEČEK 28
3.1.1 Základní čtečky 28
3.1.2 Polointeligentní čtečky 28
3.1.3 Inteligentní čtečky 28
3.2 TOPOLOGIE A ARCHITEKTURA PŘÍSTUPOVÝCH SYSTÉMŮ 28
3.2.1 Autonomní systémy 28
3.2.2 Modulární systémy 29
3.2.2.1 Sběrnicově propojené řídicí jednotky prostupů 29
3.2.2.2 Sběrnicově propojené inteligentní čtečky 30
3.2.2.3 Sběrnicově propojené systémy s převodníky LAN 31

3.2.2.4 IP řídicí jednotky (kontroléry) 31
3.2.2.5 IP čtečky 32
3.2.3 IP technologie a cloud 33
3.2.4 Architektura sítě 34
II PRAKTICKÁ ČÁST 36
4 NÁVRH PŘÍSTUPOVÉHO SYSTÉMU 37
4.1 CHARAKTERISTIKA OBJEKTU 37
4.2 PŘÍZEMÍ 38
4.3 SUTERÉN 38
4.4 PRVNÍ PATRO 39
5 PŘEDSTAVENÍ ŘEŠENÍ AKTION 41
5.1 ESMARTREADER 42
5.2 EREADER 44
5.3 EXPANDER 45
5.4 EBOX 46
5.5 AXR-110 46
5.6 SOFTWARE AKTION.NEXT 47
6 KRITÉRIA PRO HODNOCENÍ DODAVATELŮ ACS 49
6.1 POŽADAVKY NA DODAVATELE 49
6.2 POŽADAVKY NA SYSTÉM, FUNKCE A VAZBY 49
6.3 POŽADAVKY NA SPECIÁLNÍ FUNKCE 50
6.3.1 Antipassback 50
6.3.2 Interlock 50
6.4 MOŽNOSTI INTEGRACE 51
6.5 VÝHODY A NADSTANDARDNÍ PŘÍNOSY 51
7 ODHAD BUDOUCÍHO VÝVOJE 52
ZÁVĚR 54
SEZNAM POUŽITÉ LITERATURY 56
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 59
SEZNAM OBRÁZKŮ 60
SEZNAM TABULEK 61
SEZNAM PŘÍLOH 62

ÚVOD

Potřeba mít absolutní kontrolu nad stavem věcí za účelem ochrany majetku a bezpečí provází lidstvo odnepaměti. Přístupové systémy neboli systémy kontroly vstupu sice primárně neslouží k ochraně majetku, ale jak ze samotného názvu vyplývá, ke kontrole a řízení přístupu osob. Na základě jednoznačné identifikace osoby a jejích přístupových práv je této osobě povolen nebo zamítnut přístup do daných prostor. Tato schopnost kontroly a omezení volného pohybu osob pak s sebou přináší i zvýšenou ochranu majetku v daných prostorách, zvýšení bezpečnosti zaměstnanců v objektu a lepší ochranu ostatních hodnot. Dalším hlavním cílem je možnost evidence přístupů a monitoringu aktuálního pohybu osob v objektu.

V současné době už SKV nevystupuje jako samostatný systém, ale je s výhodou integrován i s jinými systémy, což zvyšuje jejich flexibilitu, snižuje celkové náklady na jejich pořízení a provoz a zároveň zvyšuje celkový komfort ovládání těchto systémů.

Přehled o kvalitě a spolehlivosti přístupových systémů, jak na úrovni jednotlivých zařízení, tak na úrovni systémové, poskytují příslušné normy a certifikace. Pro odvětví vojenského a leteckého průmyslu, kde jsou obecně kladeny vyšší nároky, jsou normy a certifikace méně známé a pro nezasvěcené i hůře dostupné. To bylo podnětem ke vzniku této práce, ve které analyzuji normy a certifikace ve vztahu k přístupovému systému ve firmě výrobce plošných spojů pro vojenský a letecký průmysl.

Cílem této práce je tedy seznámení se nejen s normami a certifikáty relevantními k danému problému, ale také s aktuálními nabízenými řešeními přístupových systémů na českém trhu, které splňují požadavky vyplývající z příslušných norem a certifikací a nakonec navržení přístupového systému pro nově vznikající budovu zadavatelské firmy se zohledněním jejích požadavků.

I. TEORETICKÁ ČÁST

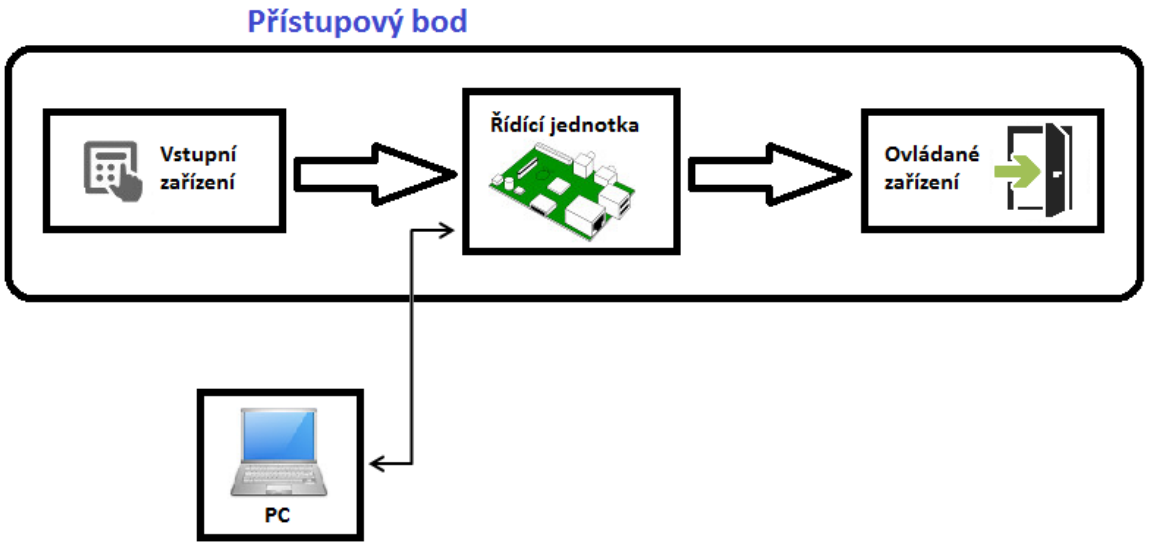
1 OBECNÝ POPIS SYSTÉMŮ PRO KONTROLU VSTUPU

Cílem systému kontroly vstupu je za pomoci elektronických, mechanických a systémových opatření zajistit kontrolu a řízení přístupů osob do prostor v chráněném objektu. To se děje na základě jednoznačné identifikace příslušné osoby a v souladu s předem definovanými přístupovými právy pro tuto osobu. Přístupová práva lze přiřazovat každému uživateli v systému libovolně na základě personální politiky, postavení ve firmě, časového harmonogramu atp. Chování systému a přístupová práva lze předdefinovat a vztáhnout nejen na jednotlivé uživatele v systému, ale také na skupiny uživatelů, což usnadňuje celkovou přehlednost administrace systému a jeho správu. Sofistikovanější systémy pak umožňují i trasování pohybu osob po chráněném objektu, monitorovat počty osob v objektu a v jednotlivých prostorách, definovat návaznosti průchodů, měnit přístupová práva uživatelům v reálném čase a další pokročilé funkce jako je anti-passback apod. Efektní je možnost nastavení akcí a reakcí na průchod uživatele přístupovým bodem, jako například ovládání osvětlení nebo spouštění a vypínání zařízení v jednotlivých prostorech. Sekundárním cílem SKV je omezit nebo zcela vyloučit přítomnost fyzické ochrany, nejčastěji vykonávané v podobě strážní služby nebo ostrahy, která je v systému nejnákladnější a nejrizikovější. Omezením lidského faktoru v systému se zvýší spolehlivost systému.

Možnost zaznamenávání historie veškerého dění v systému pak nabízí možnost jejího zpracování dalšími systémy nebo podklady pro vyšetřování nestandardních situací v chráněném objektu. Kompletní evidence pohybu osoby po objektu může být například využita i pro zaměstnavatele k naplnění jeho zákonné povinnosti evidovat pracovní bodu a přestávky zaměstnanců.

1.1 Přístupový bod

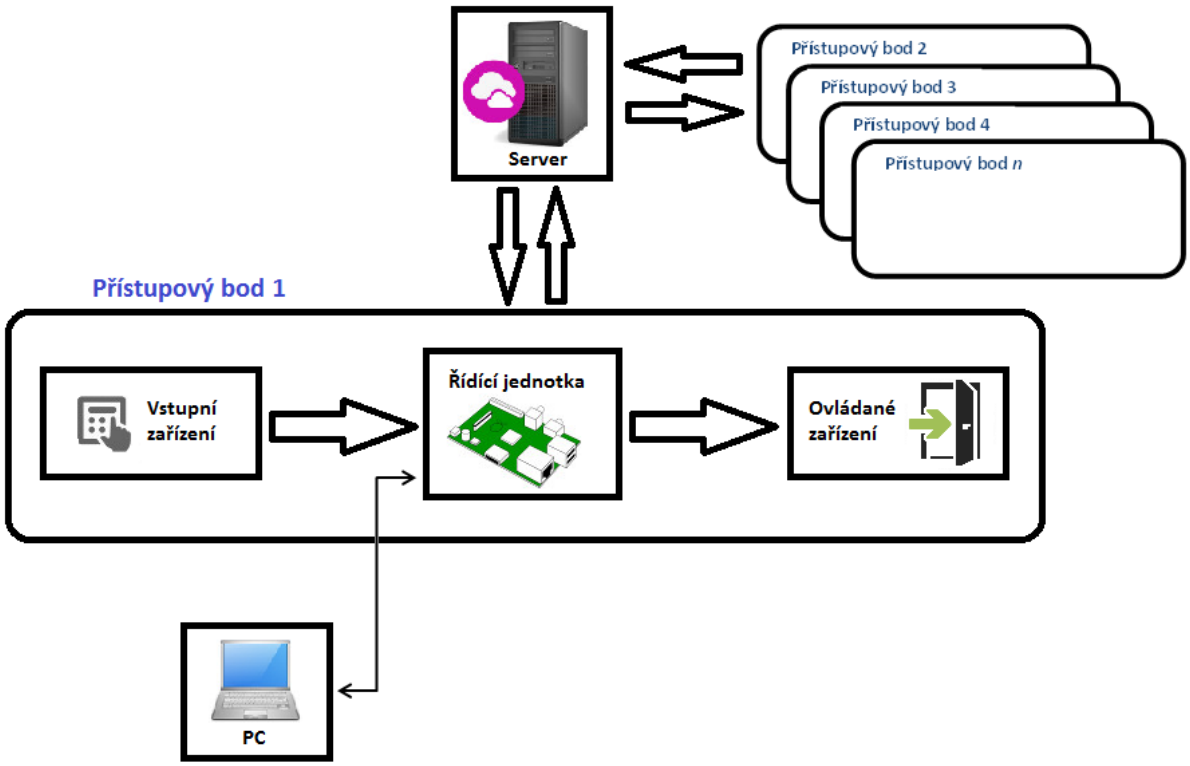
Nejjednodušší přístupový systém je tzv. přístupový bod tvořený vstupním zařízením, řídicí jednotkou a ovládaným zařízením (viz obr. 1).



Obr. 1 Blokové schéma přístupového bodu

Přístupový bod je nejmenší samostatně funkční jednotkou. Před zařazením tohoto bodu do provozu je potřeba nakonfigurovat řídicí jednotku. To lze provést například pomocí softwaru na PC připojeném k řídicí jednotce nebo manuálně přes vstupní zařízení, které je již součástí přístupového bodu. Konfigurace spočívá především v nadefinování přístupových práv pro jednotlivé osoby jednoznačně identifikovatelné například kódem, přístupovou kartou, biometrickým údajem, atp. Řídicí jednotka většinou disponuje i RTC (hodiny reálného času), které po správném nastavení umožňují další funkce řídicí jednotce - logování historie, omezení přístupu v časových intervalech, atd. Obecně to lze vyjádřit třemi body – KDO, KDY, KAM. Standardní princip fungování je pak následující: přes vstupní zařízení se provede autentizace osoby, řídicí jednotka rozhodne, zda má osoba oprávnění k průchodu a nakonec také rozhodne, zda mu průchod umožní. O celé akci nakonec provede záznam do historie.

Tyto přístupové body je možné skládat a řetězit do velmi rozsáhlých systémů. Správa a konfigurace jednotlivých přístupových bodů se pak s výhodou provádí přes centrální prvek – server (obr. 2). V případě výpadku komunikace se serverem mohou přístupové body pracovat po nějakou dobu i samostatně na základě posledních konfiguračních údajů uložených v řídicí jednotce.



Obr. 2 Blokové schéma přístupového systému

1.2 Způsoby identifikace

1.2.1 Identifikace heslem

Jde o nejstarší a nejrizikovější metodu založenou na sdíleném tajemství mezi uživatelem a systémem, jako je například PIN kód, uživatelské jméno a heslo, osobní identifikační číslo atd. V systému by měla být dodržena korelace mezi počtem uživatelů a počtem kombinací kódu - minimálně 1:1000.

Autentifikace probíhá tak, že systém po zadání sdíleného tajemství uživatelem porovná získaná data s údaji, které má uložené ve své databázi.

Výhody:

- nejlacinější řešení
- jednoduchá a rychlá možnost výměny sdíleného tajemství (například telefonicky)
- jednoduchá změna sdíleného tajemství
- možnost signalizace výjimečných stavů (např. nátlakové situace) použitím jiného kódu

Nevýhody:

- nutnost zapamatování sdíleného tajemství
- nutnost ručního zadávání
- nelze použít jako jednoznačný identifikátor nositele, tuto informaci lze vynutit z uživatele pod nátlakem
- možnost odpozorování

1.2.2 Identifikace předmětem

Tato metoda je založena na vlastnictví nějakého předmětu - tokenu. Token je identifikační předmět potvrzující identitu svého vlastníka. Tyto autentizační předměty by měly být především jedinečné, složitě padělatelné a nemělo by být možné je duplikovat. Jako token se používají nejčastěji kontaktní či bezkontaktní karty a přívěšky.

Výhody:

- jednoduché používání, dotykové i bezdotykové verze tokenů
- vysoká průchodnost systémem
- token může nést doplňkové informace
- token lze použít i v jiných systémech a kombinovat s jinými technologiemi

Nevýhody:

- možnost ztráty či odcizení tokenu
- možnost poškození tokenu
- bez doplňkových informací jednoznačně neidentifikuje svého majitele

1.2.3 Biometrická identifikace

Metoda biometrické autentizace využívá fyziologických nebo behaviorálních charakteristik člověka. Autentizace na základě behaviorálních charakteristik, jako je například dynamika podpisu nebo rozpoznávání hlasu zaručuje sice větší jistotu, že identifikaci provádí opravdu daná osoba, přesto zde existují způsoby napodobování nebo možnost neoprávněné manipulace s přístroji za účelem jejich zmatení. Proto je dobré doplnit tuto metodu o přítomnost ostrahy, která by měla kontrolovat, co a jak je ke snímačům přikládáno a zda nedochází k nežádoucí manipulaci se zařízeními. Není-li možné využít fyzickou ostrahu, nabízí se zde také možnost využít kamerový systém.

Výhody:

- z principu vyplývající nemožnost ztráty či zapomenutí identifikačního prvku
- univerzálnost a zároveň jedinečnost – neexistují dvě osoby se stejnými biometrickými charakteristikami
- permanence – biometrické údaje jsou časově invariantní
- jednoduché používání, kontaktní i nekontaktní provedení

- vysoká bezpečnost

Nevýhody:

- vysoká cena
- systém je náročný na správu a technické prostředky
- delší doba identifikace snižuje průchodnost systému
- menší odolnost systému vůči vandalizmu
- existují osoby, které nemohou takovéto systémy používat

1.2.4 Kombinace metod

Kombinací výše popisovaných metod lze využít výhod jednotlivých způsobů autentizace a získat tak maximální zabezpečení s ohledem na komfort při užívání systému pro kontrolu vstupu. Nejčastější kombinace jsou identifikace pomocí hesla a předmětu nebo předmětu a biometrického údaje. Při volbě vhodné kombinace je nutné si stanovit, zda má být povolení přístupu svázáno s oprávněnou osobou (použití biometriky) nebo s vlastnictvím předmětu (vylučuje použití biometrických údajů).

1.3 Identifikační prvky a jejich snímání

1.3.1 Optický identifikační systém

Nejtypičtější pro optickou identifikaci je použití čárových kódů (obr. 3). Cena karet s čárovými kódy je v podstatě zanedbatelná a jejich výroba je velmi snadná. Snadné je také vytvoření duplikátu, na který postačí obyčejné kopírovací zařízení. Z tohoto důvodu zde nelze hovořit o jakémkoliv zabezpečení a tento systém identifikace nelze použít v bezpečnostních systémech.

Čárový kód - nosičem informace jsou skupiny černých proužků na bílém podkladě. První a poslední proužek je použit pro synchronizaci, ostatní pak představují logické hodnoty pro čtečku. Čtečkou je optoelektronický snímač vyzařující paprsek a vyhodnocující, zda došlo k odrazu paprsku od bílého pozadí nebo naopak k pohlcení paprsku černým proužkem.

Obr. 3 Čtení čárového kódu.

Převzato z [1]

1.3.2 Magnetický identifikační systém

Základem je magnetický pásek, na kterém se zmagnetizováním vytvoří linie malých permanentních magnetů a jejich polarizace pak definuje logickou hodnotu. Karty mají omezenou kapacitu záznamu, která je dána délkou magnetického proužku a hustotou záznamu. Standard ISO 7811 definuje tři stopy záznamu (obr. 4):

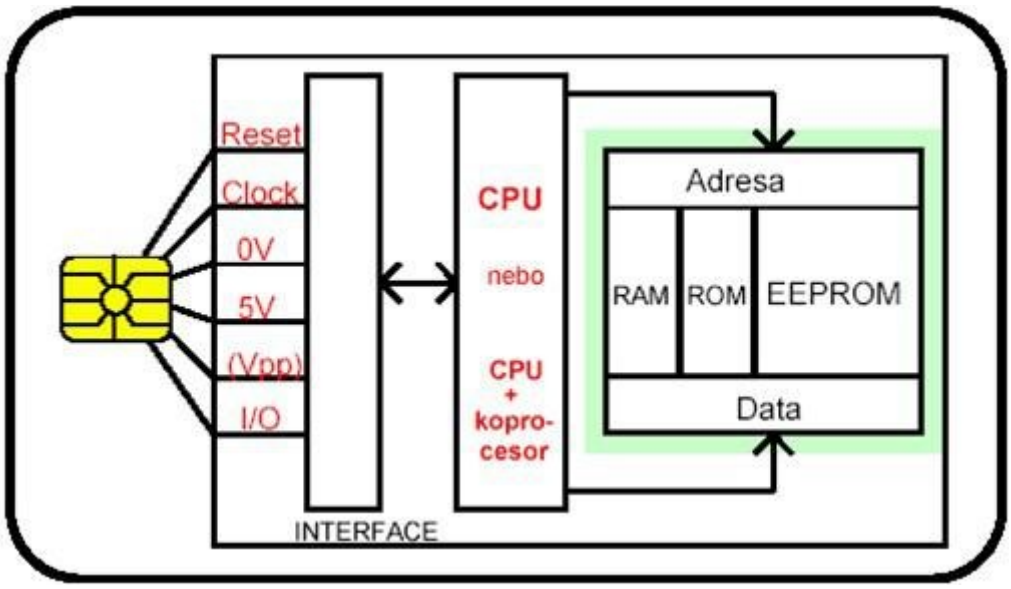
- 1. stopa – obsahuje numerické nebo alfanumerické znaky (79 znaků)
- 2. stopa – obsahuje pouze numerické znaky (40 znaků)
- 3. stopa – obsahuje pouze numerické znaky (107 znaků)

Magnetický pásek je prakticky pouze ve spojení s kartami formátu ID-1 (85,60 x 53,98 mm – formát standardní platební karty), definovaném normou ČSN ISO/IEC 7810 a jiné provedení je spíše výjimečné. Data uložená na kartě jsou dynamická, lze je tedy snadno změnit nebo aktualizovat. Stejně tak životnost uložených dat je velmi dobrá, ale magnetický pásek podléhá fyzickému opotřebení a data je možné pozměnit nebo znehodnotit vystavením silnému magnetickému poli. Snímání dat se provádí nejčastěji protáhnutím karty snímačem. Kartu lze jednoduše zkopírovat nebo pozměnit její obsah, proto ji nelze považovat za důvěryhodný zdroj informace.

Obr. 4 Stopy pro zápis dat na magnetický proužek. Převzato z [2]

1.3.3 Čipy a čipové karty (Smart Cards)

Jedná se o karty vybavené speciálním čipem, případně i vlastním procesorem. Výhodou těchto karet je vyšší bezpečnost, jelikož paměť poskytovaná touto kartou je také chráněna a nelze je jednoduše kopírovat. Přímo na kartě mohou být zaimplementovány kryptografické protokoly a přístup k uloženým datům na kartě je pak tímto zabezpečený. Z tohoto důvodu jsou však čipy složité a náleží k nim potřeba speciálních čteček. V případě čipových karet mimo jiné funkce čipů a jejich umístění definuje norma ISO/IEC 7816. Mohou být jak v kontaktním, tak i bezkontaktním provedení. Velkou nevýhodou u kontaktních systémů pak může být jejich náchylnost k opotřebení kontaktů a celková životnost mechanických částí.



Obr. 5 Blokové schéma čipové karty. Převzato z [3]

1.3.4 Bezkontaktní identifikační systém RFID

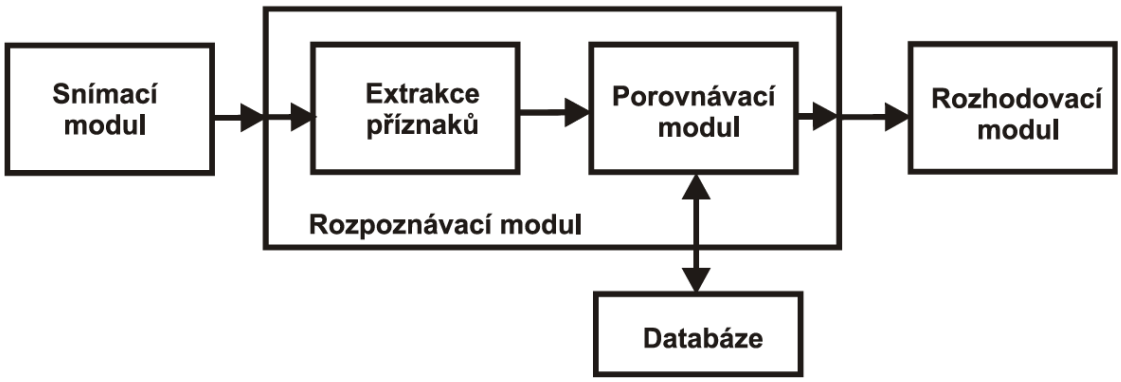
Radio Frequency Identification – bezkontaktní identifikační systém využívající k přenosu informace na krátkou vzdálenost rádiové vlny. Nejčastěji používanými jsou pasivní RFID tagy (obr. 6), které samy nedisponují aktivním napájecím zdrojem.

Vysílač (snímač, čtečka) periodicky vysílá do okolí elektromagnetické pulsy. Pro komunikaci využívají převážně nosnou frekvenci 125 kHz, 134 kHz a 13,56 MHz. Pokud se v blízkosti objeví pasivní RFID čip, využije přijímanou energii k nabití svého napájecího kondenzátoru a odešle odpověď. Pasivní čipy dokáží vysílat buď jedno číslo (elektronické číslo produktu EPC), určené při jejich výrobě, nebo disponují navíc ještě dodatečnou pamětí, do které lze zapisovat a číst další informace.

Obr. 6 RFID tagy. Převzato z [4] [5] [6]

1.3.5 Biometrické identifikační prvky

Biometrické systémy se skládají z několika logických (funkčních) bloků. Princip biometrických systémů popisuje blokové schéma - viz obr. 7.



Obr. 7 Blokové schéma biometrického systému

Biometrický identifikační systém se skládá ze snímacího modulu, rozpoznávacího modulu, databáze a rozhodovacího modulu. Snímací modul slouží k získávání biometrických dat. Rozpoznávací modul se skládá z modulu pro extrakci příznaků a porovnávacího modulu. Pro identifikaci osoby se nepoužívají všechny snímané informace, ale jen některé jejich významné části - tzv. příznaky. S extrahovanými příznaky se uskutečňují různé matematické operace, na základě kterých se realizuje identifikace osoby. Použití extrakce příznaků souvisí s rychlostí celkové identifikace osoby. V porovnávacím modulu se na základě získaných příznaků uskutečňuje porovnávání s daty uloženými v databázi (uživatelů). Závěrečné rozhodnutí, zda snímané údaje jsou shodné s daty uloženými v databázi, se vykonává v rozhodovacím modulu.

Biometrické autentizační systémy pracují ve dvou režimech:

- Registrační (záznamový) režim - biometrická data jsou získána použitím biometrických senzorů a jsou uložena do databáze. K uloženým biometrickým datům jsou přiřazeny jednoznačné identifikační prvky osoby (např. jméno, identifikační čís-

lo,…) pro umožnění autentizace osoby. Biometrická data získaná v tomto režimu jsou označována jako tzv. biometrické etalony a představují reprezentativní (referenční) údaje, s kterými jsou porovnávány následující vzory získávané v průběhu autentizace (v tzv. autentizačním režimu).

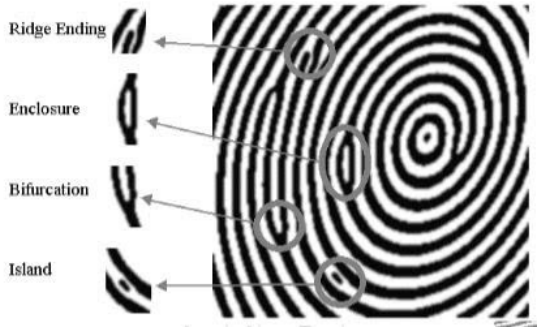
- Autentizační režim - slouží k identifikaci osoby na základě porovnání snímaných biometrických dat s biometrickými daty uloženými v databázi.

Získané etalony mohou být ukládány do interní databáze snímacího zařízení, do síťové databáze nebo přímo na čipovou kartu nositele. V prvních dvou případech se jedná o ověření typu 1:n, kdy je databáze prohledávána celá, což v případě rozsáhlých databází může trvat delší dobu. Je-li etalon uložen na čipové kartě vlastníka, jedná se o ověření typu 1:1, kdy rozhodovací modul je schopen rozhodnout téměř okamžitě. Při použití metody ověřování 1:1 odpadá nutnost udržování databáze a s ní spojené možné problémy jako je například poškození nebo ztráta databáze.

Spolehlivost biometrické identifikace se vyjadřuje dvěma parametry – FFR (False Rejection Rate) a FAR (False Acceptance Rate). FFR je míra pravděpodobnosti, že systém chybně vyhodnotí dva biometrické vzorky stejné osoby odlišně a zamítne tak této osobě přístup. Oproti tomu FAR zase vyjadřuje míru pravděpodobnosti, že systém dva různé biometrické vzorky dvou různých osob vyhodnotí jako totožné a umožní tak přístup jiné osobě.

1.3.5.1 Otisk prstu

Identifikace podle otisku prstu patří do skupiny daktyloskopických identifikací, využívá tedy především papilárních linií na článcích prstů či na dlani člověka. Tvary papilárních linií, jejich průběh a směr jsou u jednotlivých osob odlišné. Podle obrazců, které papilární linie vytvářejí, je možné stanovit několik vzorů, které slouží k základnímu rozdělení všech obrazů. Obrazy papilárních linií se nemění celý život a není možné je odstranit.



Obr. 8 Markanty na otisku prstu. Převzato z [7]

Jako snímače otisků prstů se používají:

- Optické senzory – využívají odlišných vlastností při odrazu světelného paprsku v papilárním terénu snímaného otisku.
- Tlakové senzory – využívají změnu optických vlastností speciálních průhledných polymerů, které vlivem tlaku prstu na polymer mění své optické vlastnosti.
- Odporové senzory – vyhodnocují odpor pokožky.
- Kapacitní senzory – využívají měření elektrické kapacity vznikající mezi senzorem a papilárními liniemi.
- Teplotní senzory – vyhodnocují rozdíly teplot mezi papilárními liniemi a vzduchovými polštářky mezi nimi.
- Elektroluminiscenční senzory - snímací plocha je z několikavrstvého polymeru, který při tlaku vyvinutém stisknutím prstu emituje světlo v místech, kde na ni tlačí papilární linie.
- Ultrazvukové snímače – pomocí zvukových vln jsou schopny rozeznat přilehlé papilární linie od vzdálenějších rýh.

1.3.5.2 Geometrie ruky

Identifikace podle geometrie ruky probíhá za pomocí dvou nebo trojrozměrného měření, kdy se vyhodnocuje tloušťka a délka prstů, šířka jednotlivých kloubů a celkový tvar ruky, který se od určitého věku nemění.

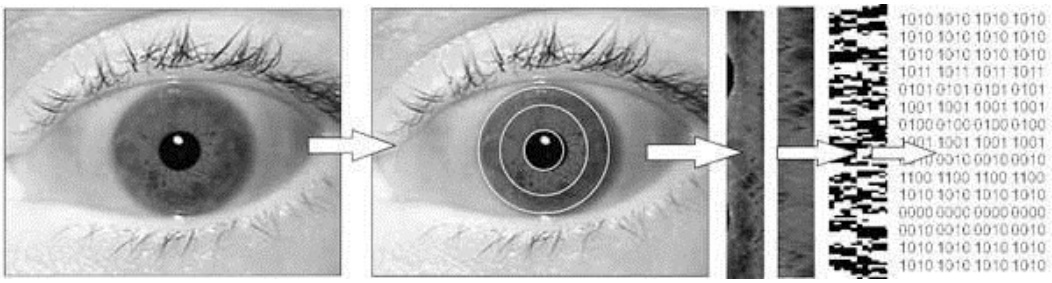
1.3.5.3 Oční sítnice

Oční sítnice není viditelným orgánem a proto je skenována infračerveným koherentním světlem s využitím faktu, že prokrvené cévy oční sítnice toto záření více pohlcují a po její

transformaci do viditelné formy se jeví jako tmavší místa. Vyhodnocení se pak provádí na základě vzoru žilek.

1.3.5.4 Oční duhovka

Oční duhovka je pro biometrickou identifikaci ideální. U každého člověka má unikátní strukturu a poskytuje velké množství vyhodnotitelných markantů. Dokonce i obě duhovky u jedné osoby jsou rozdílné a jedinečné. Získání obrazu oční duhovky je pasivní, identifikace je rychlá, většinou prováděná na základě analýzy barevných skvrnek a je velmi spolehlivá. Zatím neexistuje způsob, jak duhovku padělat.



Obr. 9 Identifikace duhovky. Převzato z [8]

1.3.5.5 Rozpoznání obličeje

V 2D obrazu obličeje jsou vyhodnocovány markanty, jako je například vzdálenost očí, délka očí, délka obočí, délka rtů, výška rtů, velikost ucha, atd. Spolehlivost této techniky závisí na výrazu (mimice) osoby a na úhlu snímání obrazu. Možným zvýšením spolehlivosti je použití 3D rekonstrukce obrazu, což je však nepoměrně výpočetně náročnější. Nevýhodou je, že tvář člověka se s časem mění.

1.3.5.6 Dynamika podpisu

Identifikace podle dynamiky podpisu se vyhodnocuje pomocí speciálního pera. Posuzovanými markanty jsou například tlak pera na podložku, rychlost psaní jednotlivých písmen, sklon písma jednotlivých znaků, délka a trvání tahů při psaní.

1.3.5.7 Dynamika stisku kláves

Identifikace podle dynamiky stisku kláves je obdobou předešlé metody, vhodná pro dálkovou identifikaci v počítačové síti. Každý uživatel má specifické rysy ve stisku kláves – časovou prodlevu mezi jednotlivými stisky. Tato doba je pak vyhodnocována a porovnávána se vzorem.

2 ANALÝZA LEGISLATIVNÍCH POŽADAVKŮ A NOREM

Technická norma představuje nezávazné kvalifikované doporučení a stanovuje základní požadavky na výrobky s ohledem na kvalitu a bezpečnost výrobku, ochranu zdraví a ochranu životního prostředí. Slouží zejména výrobcům pro potřeby certifikace výrobků, stanovuje a definuje termíny a názvosloví, pokyny pro projektování a návrhy, požadavky na dokumentaci, formu zkoušek atd.

2.1 Legislativa ČR

Všechny komponenty přístupových systémů provozovaných v ČR jsou povinovány splňovat požadavky na elektrickou bezpečnost, definovanou normami ČSN EN 60950-1 ED.2 a ČSN EN 60065. Povinností výrobce či dovozce je mít k výrobkům provedeno posouzení o shodě v souladu s ustanovením zákona č. 22/1997 Sb. Na elektrické a elektronické komponenty SKV se vztahují ustanovení nařízení vlády č. 616/2006 Sb. o elektromagnetické kompatibilitě, případně i požadavky telekomunikačních norem, například ČSN EN 50529. V rámci instalace systémů kontroly vstupu je nutné dle nařízení vlády č. 118/2016 Sb. dodržet i požadavky norem vztahující se na elektrické instalace nízkého napětí jako jsou například ČSN EN 33 2000-4-41 Ed.3, ČSN EN 33 2000-5-51 Ed.3 a ČSN EN 33 2000-6 Ed.2. Případ integrace systému kontroly vstupu s jinými poplachovými či nepoplachovými systémy je popsán a definován normou ČSN CLC/TS 50398. V současné době požadavky na systémy kontroly vstupu jsou upraveny technickými normami ČSN EN 60839-11-1, definující požadavky na systém a jednotlivé komponenty a ČSN EN 60839-11-2 definující pokyny pro aplikaci. [9] [10]

Tab. 1 – Názvy jednotlivých norem

ČSN EN 60950-1 ED.2	Zařízení informační technologie - Bezpečnost - Část 1: Všeobecné požadavky
ČSN EN 60065	Zvukové, obrazové a podobné elektronické přístroje - Požadavky na bezpečnost
ČSN EN 50529	Norma EMC pro sítě - Část 1: Telekomunikační sítě po vedení využívající telefonní vedení
ČSN EN 33 2000-4-41 Ed.3	Elektrické instalace nízkého napětí - Část 4-41: Ochranná opatření pro zajištění bezpečnosti - Ochrana před úrazem elektrickým proudem
ČSN EN 33 2000-5-51 Ed.3	Elektrické instalace nízkého napětí - Část 5-51: Výběr a stavba elektrických zařízení - Všeobecné předpisy
ČSN EN 33 2000-6 Ed.2	Elektrické instalace nízkého napětí - Část 6: Revize

ČSN CLC/TS 50398	Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky
ČSN EN 60839-11-1	Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty
ČSN EN 60839-11-2	Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace

2.1.1 Norma ČSN EN 60839-11-1

Tato norma definuje stupně zabezpečení, podobně jako je tomu u poplachových zabezpečovacích a tísňových systémů a stanovuje pro tyto jednotlivé stupně i požadavky na funkce systému kontroly vstupu. Dále norma definuje terminologii, architekturu systému a stanovuje minimální požadavky na elektromagnetickou kompatibilitu a klimatickou odolnost pro jednotlivé stupně zabezpečení. Součásti normy je i definice způsobu provádění zkoušek.

Tab. 2 – Stupně klasifikace [11]

Stupeň	**1**	**2**	**3**	**4**
Úroveň rizika	**Nízké**	**Nízké až střední**	**Střední až vysoké**	**Vysoké**
Aplikace	Organizační prostředky, ochrana majetku nízké hodnoty.	Organizační prostředky, ochrana prostředků nízké až střední hodnoty.	Méně organizačních prostředků, ochrana komerčních prostředků střední až vysoké hodnoty.	Zejména ochrana komerčních prostředků velmi vysoké hodnoty nebo kritické infrastruktury.
Dovednost/znalosti pachatelů/útočníků	Malá dovednost, malá znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií. Malé finanční prostředky pro napadení.	Střední dovednost a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií. Malé až střední finanční prostředky pro napadení.	Velká dovednost a 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 (vojenská zařízení, vládní budovy, výzkum a vývoj, kritická infrastruktura).

2.1.2 Norma ČSN EN 60839-11-2

Tato norma zahrnuje požadavky na plánování, instalaci a uvedení systému kontroly vstupu do provozu, a také na jeho údržbu a dokumentaci pro aplikace uvnitř i kolem budov a prostor. Norma také připouští výjimky pro instalované systémy a definuje tyto výjimky u specifických aplikací.

2.2 Normy a certifikáty pro letecký a vojenský průmysl

Od zadavatele a jeho potencionálních zákazníků jsem získal seznam požadovaných norem a certifikací, které by měla zadavatelská firma splňovat. Cílem bylo tento seznam norem a certifikací prostudovat a vybrat z nich ty, které definují požadavky na přístupové systémy pro dodavatele desek plošných spojů.

2.2.1 Management kvality

- ISO 9001 – Standard, respektive procesně orientovaná norma pro systém řízení kvality. Slouží jako referenční model pro nastavení základních řídicích procesů v organizaci a pomáhá tak neustále zlepšovat kvalitu poskytovaných výrobků nebo služeb.
- ISO 9100 – Celosvětově akceptovaná certifikace řízení kvality v leteckém průmyslu založená na standardu ISO 9001. Tato procesně orientovaná norma upřesňuje všeobecné požadavky normy ISO 9001 a rozšiřuje požadavky zaměřené na kvalitu, včasnost a spolehlivost dodávek.
- ISO 27001 – Norma z oblasti řízení bezpečnosti informací. Norma popisuje vhodný systém řízení, strukturu a procesy pro řízení bezpečnosti informací podle opatření definovaných v ISO 27002. Podle této normy mohou organizace samy definovat rozsah certifikovaného systému. Norma poskytuje záruky za bezpečnost informací a harmonizaci s dalšími normami pro systémy řízení.

2.2.2 České obranné standardy:

- ČOS 051622 (AQAP-2110) - Požadavky NATO na ověřování kvality při návrhu, vývoji a výrobě
- ČOS 051626 (AQAP-2120) - Požadavky NATO na ověřování kvality při výrobě

Tyto ani žádné jiné české obranné standardy přímo nespecifikují požadavky na přístupové systémy u komerčních dodavatelů materiálů. Pouze si vynucují právo přístupu do

zařízení, v nichž jsou prováděny smluvní činnosti. Tyto certifikace zahrnují většinu požadavků, které obsahuje ČSN EN ISO 9001:2016.

2.2.3 Německé vojenské standardy

- VG 96927-2 – Certifikát o shodě s požadavky německého vojenského standardu – Tato norma definuje požadavky v oblasti výroby kabelů, vodičů a jejich obalové a izolační materiály, tedy nedefinuje žádné požadavky na systémy kontroly vstupu.

2.2.4 Normy IPC

Normy IPC obecně nemají k systémům kontroly přístupu žádný vztah. Zabývají se především technickou standardizací v oblasti výroby elektroniky a jsou hojně akceptovány a využívány během celého výrobního cyklu elektrotechnických výrobků – od návrhu desek plošných spojů, přes jejich výrobu až po montáž a testování sestav a hotových výrobků.

- IPC-6013 - Qualification and Performance Specification for Flexible Printed Boards
- IPC-T-50 - Terms and Definition
- IPC-MF-150 - Metal Foil for Printed Wiring Applications
- IPC-FC-231 - Flexible Bare Dielectrics for Use in Flexible Printed Wiring
- IPC-FC-232 - Specification for Adhesive Coated Dielectric Films For Use as Cover Sheets for Flexible Printed Wiring
- IPC-FC-241 - Flexible Metal Clad Dielectrics for use in Fabrication of Flexible Printed Wiring
- IPC-SM-840 - Qualification and Performance of Permanent Solder Mas
- IPC-2221 - Generic Standard on Printed Board Design
- IPC-2223 - Sectional Design Standard for Flexible Printed Boards
- IPC-4101 - Laminate/Prepreg Materials Standard for Printed Boards
- IPC-6011 - Generic Performance Specification for Printed Boards
- IPC-6012 - Qualification and Performance Specification for Rigid Printed Boards
- J-STD-001 - Requirements for Soldered Electrical and Electronics Assemblies
- J-STD-002 - Solderability Tests for Component Leads, Terminations, Lugs, Terminals and Wires
- J-STD-003 - Solderability Tests for Printed Boards
- J-STD-004 - Requirements for Soldering Fluxes

- J-STD-005 - General Requirements and Test Methods for Electronic Grade Solder Paste
- J-STD-006 - General Requirements and Test Methods for Soft Solder Alloys and Fluxed and Non-Fluxed Solid Solder for Electronic Soldering Applications

2.2.5 Americké standardy a normy MIL

Dodané americké normy rovněž nemají žádný vztah k systémům kontroly vstupu. Výjimkou ze seznamu je vládní regulace AE Regulation 190-16, která specifikuje velmi podrobně požadavky na systémy kontroly vstupu, nicméně tato norma platí pouze pro americké armádní objekty v Evropě. Ostatní normy uvedené níže stanovují požadavky na návrh, výrobu a především pak testování desek plošných spojů pro použití v americkém vojenském průmyslu.

- AE Regulation 190-16 – Part Instalaation Access Control
- MIL-P-50884 - Flex Manufacturing and Performance
- MIL-STD-2118 - Flex Design Standard
- MIL-STD-100 - Engineering Drawing Practices
- MIL-STD-105 - Sampling Procedures and Inspection Tables
- MIL-STD-129 - Marking for Shipment and Storage
- MIL-STD-130 - Identification for Marking
- MIL-STD-202 - Test Methods for Electronic Equipment
- MIL-STD-2000 - Soldering and Assembly
- MIL-STD-45662 - Calibration System Requirements
- DOD-D-1000 - Engineering Drawings
- DOD-STD-100 - Engineering Drawing Practices
- MIL-S-13949 - Plastic Sheet, Laminate, Metal Clad
- MIL-C-14550 – Copper Plating (Elektrodepozitní)
- MIL-I-43553 – Ink Marking, Epoxy Base
- MIL-G-45204 – Gold Plating (Elektrodepozitní)
- MIL-I-45208 – Inspection System Requirements
- MIL-Q-9858 – Quality Program Requirements
- MIL-P-81728 – Plating Tin Lead (Elektrodepozitní)
- MIL-P-55110 – Printed Wiring Boards

- QQ-N-290 – Nickel Plating (Elektrodepozitní)
- MIL-STD-471A - Maintainability Verification/Demonstration/Evaluation
- MIL-STD-472 – Maintainability Prediction
- MIL-STD-690 - Failure Rate Sampling Plans and Procedures
- MIL-STD-750 - Test Methods for Semiconductor Devices
- MIL-STD-781 - Reliability Testing for Engineering Development, Qualification and Production
- MIL-STD-882 – System safety
- MIL-STD-883 - Test Method Standard Microcircuits

2.2.6 Akreditace NADCAP

NADCAP (National Aerospace and Defense Contractors Accreditation Program) je celosvětový akreditační program pro dodavatele výrobků a materiálů v leteckém, vesmírném a obranném vojenském průmyslu. Tento program stanovuje požadavky na systém řízení kvality a řízení procesů, používané materiály a metody testování – tedy se nijak primárně nevyjadřuje k systémům pro kontrolu vstupu.

3 SOUČASNÁ ŘEŠENÍ PŘÍSTUPOVÝCH SYSTÉMŮ

3.1 Rozdělení snímacích zařízení – čteček

Snímací zařízení, neboli čtečky, lze dělit přirozeně podle typu snímaných médií nebo podle vykonávaných funkcí na níže uvedené.

3.1.1 Základní čtečky

Takovéto čtečky zajišťují pouze zadání kódu nebo přečtení identifikačního média, které dále poskytnou nadřazené řídicí jednotce k dalšímu zpracování. Jiné je to v případě biometrických čteček, které porovnání nasnímaných vzorků s uloženými etalony provádí interně a dále nadřazené jednotce poskytují informace např. o čísle identifikovaného uživatele. Komunikačním rozhraním pro tento typ čteček je hojně rozšířený protokol Wiegand.

3.1.2 Polointeligentní čtečky

Polointeligentní čtečky mají v sobě navíc zabudovány všechny potřebné vstupy a výstupy pro ovládání přístupového místa. Samotné rozhodování o povolení či zamítnutí přístupu však provádí stále nadřazená řídicí jednotka.

3.1.3 Inteligentní čtečky

Inteligentní čtečky na rozdíl od polointeligentních disponují i pamětí pro uložení konfigurace a přístupových práv. Rozhodnutí o povolení či zamítnutí přístupu se pak provádí přímo ve čtečce. Řídicí jednotka pak pouze zajišťuje aktualizaci přístupových práv ve čtečce a přijímá od čtečky informace o transakcích a dalších událostech.

3.2 Topologie a architektura přístupových systémů

3.2.1 Autonomní systémy

Autonomní systém je přístupový bod, tedy maximálně dvě snímací zařízení, řídicí jednotka a ovládaný prvek případně stavové snímače. Řídicí jednotka má v sobě naprogramována a uložena všechna přístupová práva a případně i paměť pro záznam historie událostí. Tento systém je vhodný pro samostatné řízení prostupů s nízkými nároky na bezpečnost. Příkladem mohou být třeba autonomní dveřní zámky s integrovanou čtečkou.

3.2.2 Modulární systémy

Koncepce modulárního systému je vhodná pro rozsáhlejší systémy s větším počtem přístupových míst a řídících jednotek. Všechna přístupová místa jsou centrálně řízena jedním řídicím prvkem (PC, ústředna – hlavní řídicí jednotka). Nejčastěji se využívá hvězdicové nebo sběrnicové topologie. V případě sběrnicové topologie se nejčastěji pro komunikaci mezi přístupovými místy a centrálním prvkem používá sběrnice RS-485, která je komunikačním standardem a je schopná komunikovat po metalickém vedení až na vzdálenost 1200 m. Jednotlivé prvky SKV mezi sebou mohou komunikovat i pomocí sítě ethernet reprezentující hvězdicovou topologii.

Z hlediska možných konfigurací jednotlivých modulárních prvků SKV můžeme topologie přístupových systémů rozdělit na:

- Sběrnicově propojené řídicí jednotky prostupů
- Sběrnicově propojené inteligentní čtečky
- Sběrnicově propojené systémy s převodníky LAN
- IP řídicí jednotky (kontroléry)
- IP čtečky

3.2.2.1 Sběrnicově propojené řídicí jednotky prostupů

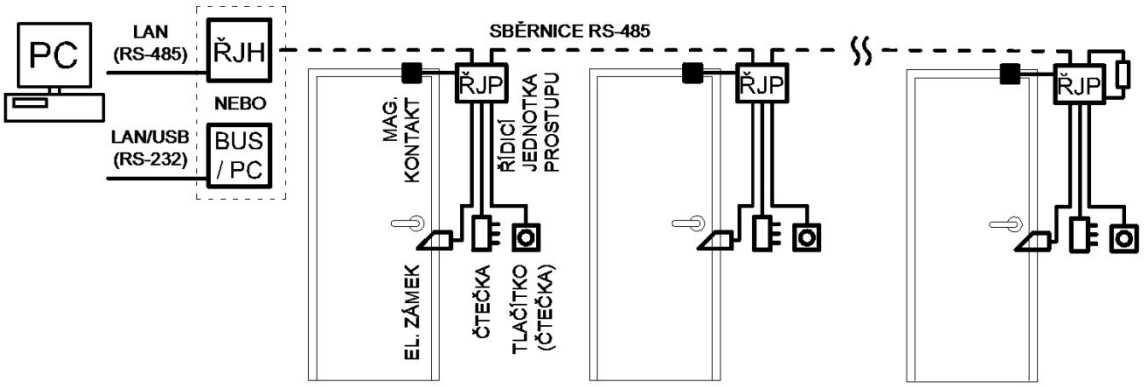
Všechny kontroléry prostupů jsou propojeny pomocí sběrnice (obr. 10) s hlavní řídicí jednotkou nebo prostřednictvím převodníku přímo s řídícím PC. Používání řídících kontrolérů poskytuje nejvyšší variabilitu z hlediska volby možných typů čteček, které jsou připojovány nejčastěji standardizovaným komunikačním rozhraním Wiegand.

Výhody:

- vyšší spolehlivost za použití hlavní řídicí jednotky
- větší variabilita z hlediska použití snímacích zařízení

Nevýhody:

- počet kontrolérů na sběrnici RS-485 je omezen na 32
- rychlost komunikace a odezvy je nepřímo úměrná délce vedení
- problém s impedančním zakončením sběrnice



Obr. 10 Sběrnicové spojení řídicích jednotek. Převzato z [12]

3.2.2.2 Sběrnicově propojené inteligentní čtečky

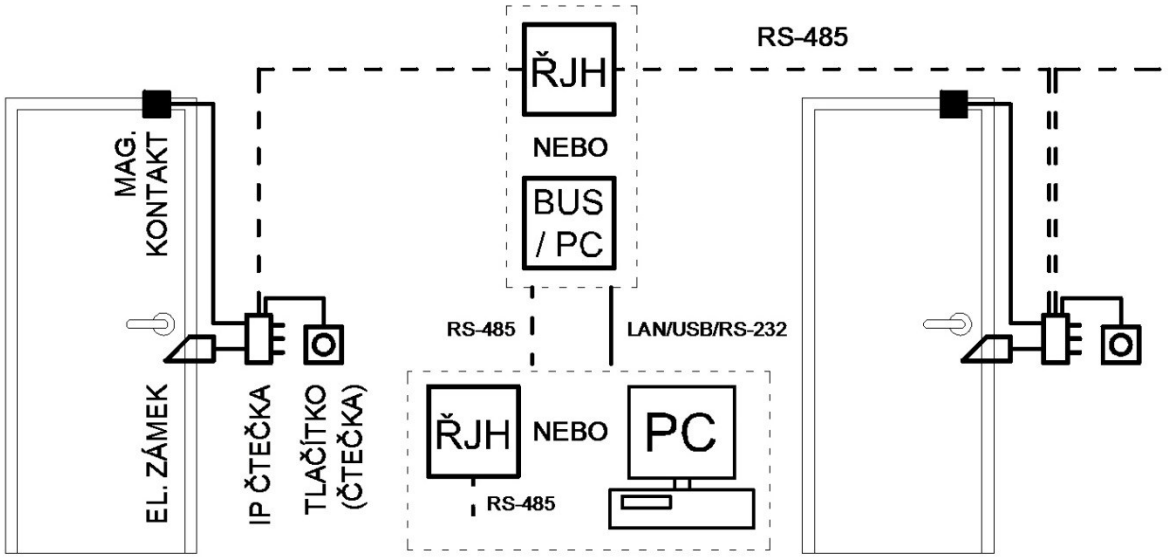
Při použití polointeligentních nebo inteligentních čteček je možné propojit je sběrnicí RS-485 napřímo bez potřeby použití řídicích jednotek (obr. 11). Inteligence rozhodující o povolení či zamítnutí přístupu se pak nachází přímo v inteligentní čtečce nebo v hlavní řídící jednotce nebo v řídícím PC.

Výhody:

- jednoduchost kabeláže
- možnost sesíťování více řídicích jednotek

Nevýhody:

- omezené portfolio tohoto typu čteček



Obr. 11 Sběrnicové propojení inteligentních čteček. Převzato z [12]

3.2.2.3 Sběrnicově propojené systémy s převodníky LAN

Všechny topologie, které využívají sběrnici RS-485, mohou být doplněny převodníky na jiný typ komunikačního rozhraní, například LAN. K distribuci informací šířících se po sběrnici RS-485 se následně využívá ethernetová síť. Toto řešení je výhodné, zvláště pokud již ethernetová síť existuje a odpadá tak nutnost instalace nové kabeláže.

Výhody:

- možnost použití existujících rozvodů sítě ethernet

Nevýhody:

- komunikační rychlost je stále omezena komunikační rychlostí sběrnice RS-485

3.2.2.4 IP řídicí jednotky (kontroléry)

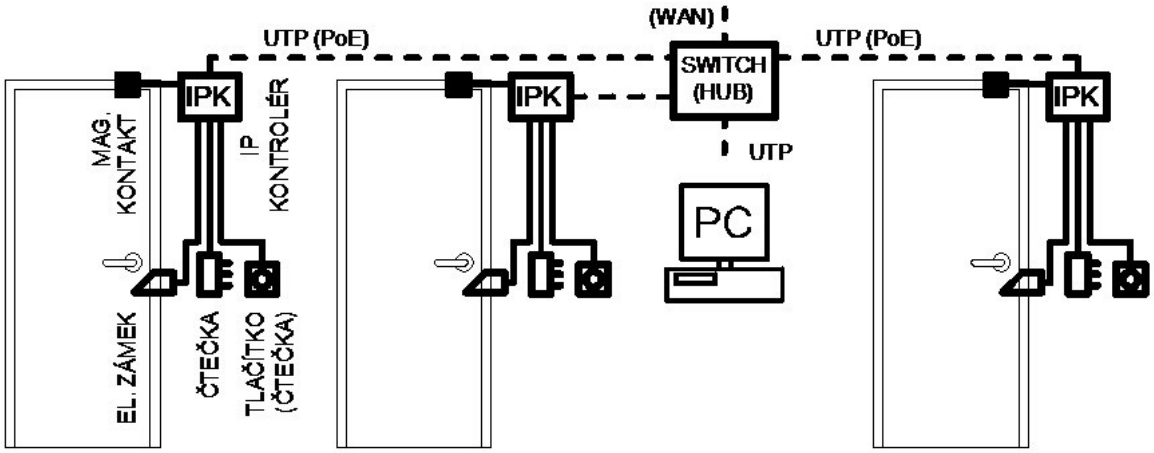
Řídicí jednotky mají rozhraní LAN a jsou propojeny nejčastěji k řídicímu PC právě prostřednictvím sítě LAN nebo WAN (obr. 12). Toto řešení je obzvláště vhodné pro rozsáhlé systémy, kdy počet možných připojených řídicích jednotek je dán rozsahem volných IP adres v síti. Přenos informací může být pomocí kabelů, optických kabelů na velké vzdálenosti, bezdrátově pomocí WiFi. Mimo jiné se zde nabízí i možnost využití technologie PoE. Řídicí jednotky mohou samy iniciovat spojení a snížit tak zatěžování sítě zbytečně opakovanými dotazy. V případě, že je však síť připojena i k síti WAN zde vyvstává riziko možného napadení LAN sítě zvenčí.

Výhody:

- možnost použití existujících rozvodů sítě ethernet
- vysoká komunikační rychlost
- počet prvků v síti je omezen počtem IP adres

Nevýhody:

- možnost napadení ze sítě WAN



Obr. 12 Konfigurace s IP kontroléry. Převzato z [12]

3.2.2.5 IP čtečky

Jedná se převážně o inteligentní čtečky vybavené ethernetovým rozhraním, které se připojují k řídicímu PC prostřednictvím LAN sítě (obr. 13). Většina IP čteček umožňuje napájení po UTP kabelu, tzv. PoE, což usnadňuje instalaci záložního napájení pro systém.

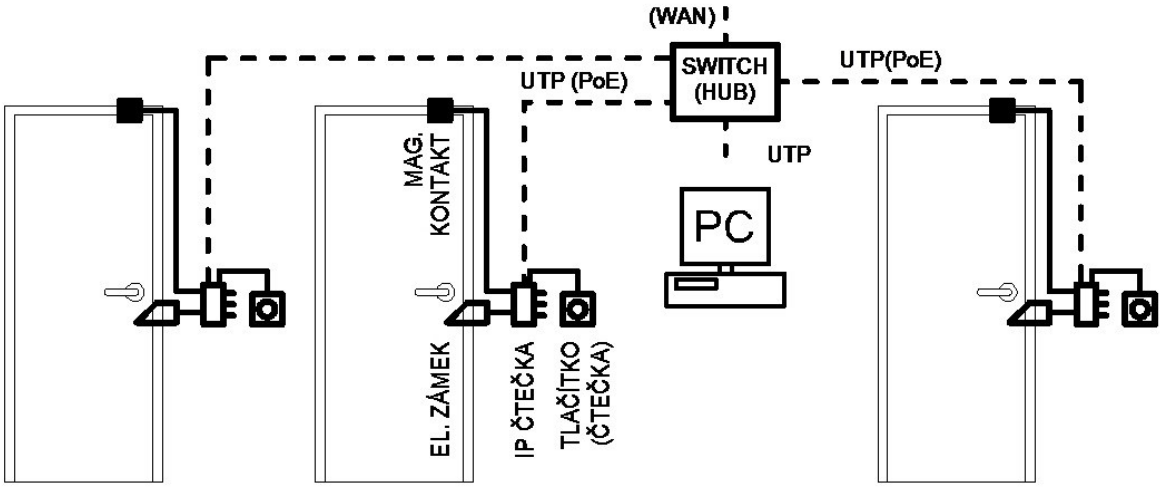
Jelikož čtečka je instalována na nechráněné straně sledovaného prostoru, je důležitá její ochrana proti podvržení falešné informace neoprávněnou osobou. Podvržení informace je možné cestou podvržení paketu s falešnou identifikací osoby odkudkoliv ze sítě LAN (případně i WAN), což je také pro případného útočníka nejpohodlnější možnost, kdy neriskuje vlastní odhalení při manipulaci se čtečkou. Další možností sabotáže je záměna IP čtečky za jinou čtečku nebo zařízení, které bude její provoz simulovat. Poslední zmíněnou událost by však čtečka měla být schopná jednoduše detekovat pomocí sabotážního kontaktu.

Výhody:

- možnost napájení PoE
- velmi jednoduché rozšíření systému
- výpadek jedné čtečky neovlivní ostatní části systému

Nevýhody:

- vyšší cena těchto typů čteček
- teoreticky jednodušší napadení přístupem ke kabeláži



Obr. 13 Konfigurace s IP čtečkami. Převzato z [12]

3.2.3 IP technologie a cloud

Komunikační sítě využívající technologie TCP/IP jsou dnes již naprosto běžné a všudypřítomné, tudíž se jejich využití v přístupových systémech přímo nabízí. Komunikace je omezena mezi dvěma prvky na vzdálenost 100 m, nicméně tuto vzdálenost lze prodlužovat téměř donekonečna takzvanými opakovači. Opakovačem je v této síti v podstatě každý nekoncový prvek (switch, router). Oproti často používané sběrnici RS-485 nabízí podstatně vyšší přenosové rychlosti a možnost využití napájení PoE. Po jediném kabelu jsou tedy přenášena data i poskytováno napájení. Podle standardu IEEE 802.3af je koncovému zařízení garantován výkon 12,95W. Toto omezení je potřeba zohlednit při výběru ovládaného zařízení (např. zámku) v případě, že je PoE využito i k napájení těchto prvků.

Výrobci prvků SKV nabízí i možnost připojení systému kontroly vstupu, postaveném na IP technologii připojení do cloudu (obr. 14). Propojení s cloudem umožňuje správu a monitoring systému odkudkoliv a nabízí se i možnost využití mobilních aplikací. Zálohou nastavení pro jednotlivé řídicí jednotky či čtečky pak umožňuje velmi jednoduchou a rychlou výměnu komponenty například při její poruše nebo poškození. Cloudové řešení také umožňuje téměř okamžitou automatickou aktualizaci všech funkcionalit systému.

Obr. 14 Inteligentní IP čtečka
eSmartReader ES-510/W.
Převzato z [13]

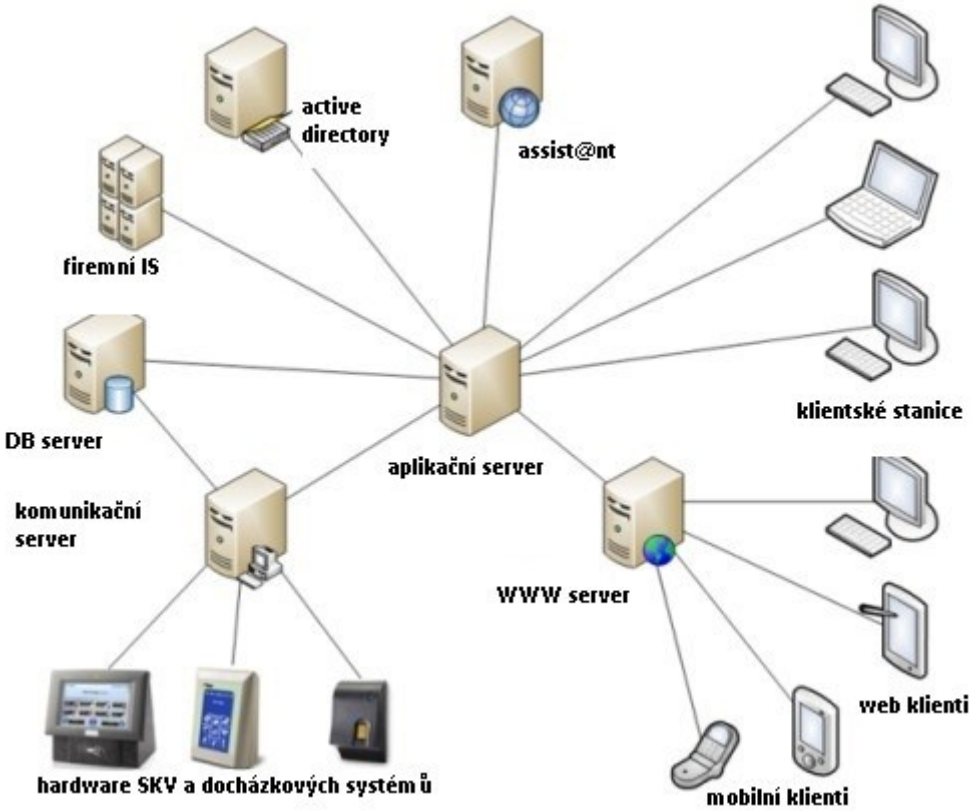
3.2.4 Architektura sítě

Síťová komunikace je komunikace po síti, která probíhá ve vrstvách. Tyto vrstvy jsou rozděleny podle důležitosti činností, které jsou při řízení komunikace vykonávány. Každá vrstva sítě je definována službou, která je poskytována vyšší sousední vrstvě, a funkcemi, které vykonává v rámci svého protokolu. Protokoly jsou souhrnem pravidel, formátů a procedur, které určují výměnu údajů mezi dvěma či více komunikujícími prvky. Užívanou skupinou protokolů jsou protokoly TCP/IP, využívající čtyř vrstev. U nejnižší vrstvy – vrstvy síťového rozhraní se počítá s tím, že zde budou využity takové přenosové mechanismy, jaké jsou k dispozici, a které nejsou součástí TCP/IP protokolů. Může jít třeba o Ethernet, Wi- Fi , ADSL atd. Komunikace po síti je tedy rychlá a velkoobjemová data, jako jsou například biometrické údaje, nejsou problémem.

Rozsáhlejší systémy kontroly vstupu využívají nejčastěji tří vrstvé architektury (obr. 15) s následujícím uspořádáním:

- První vrstva je uživatelské prostředí (terminály, čtečky, hardware SKV)
- Druhá vrstva je vlastní aplikace nebo program (aplikační server)
- Třetí vrstvou je databáze uživatelů a přístupových práv (SQL server)

Volba architektury (může být i jednovrstvá – soustřeďuje veškerou inteligenci do jediného centrálního prvku - nebo dvouvrstvá) by měla odpovídat účelu a typu sítě, technologickým a finančním možnostem, počtu uživatelů sdílejících informace. Jak již bylo zmíněno, nejčastěji se tedy u rozsáhlejších přístupových systémů používá třívrstvá architektura, která odděluje vrstvu uživatelského prostředí využívanou čtečkami a dalším hardwarem, vrstvu aplikace a vrstvu databáze (databázový server) čímž je dosažen optimální výkon systému a stabilita. [10]



Obr. 15 Znázornění třívrstvé architektury. Převzato z [12]

II. PRAKTICKÁ ČÁST

4 NÁVRH PŘÍSTUPOVÉHO SYSTÉMU

Návrh přístupového systému v nově vznikající budově pro výrobu plošných spojů je navržen v souladu s požadavky konzultovanými se zadavatelskou firmou. Všechny komponenty SKV budou instalovány uvnitř budovy, odpovídající třídě prostředí II (vnitřní všeobecné).

4.1 Charakteristika objektu

Budova středně velké firmy o počtu 60 zaměstnanců se nachází v průmyslovém areálu s volným přístupem pro veřejnost na kraji města Prahy. V okolí budovy se tedy nacházejí pouze komerční objekty a skladovací prostory. V těsné blízkosti objektu sídlí i soukromá bezpečnostní služba, které bude zaštiťovat zabezpečení budovy. Plánovaná výroba v budově bude probíhat od 6:00 do 21:00.

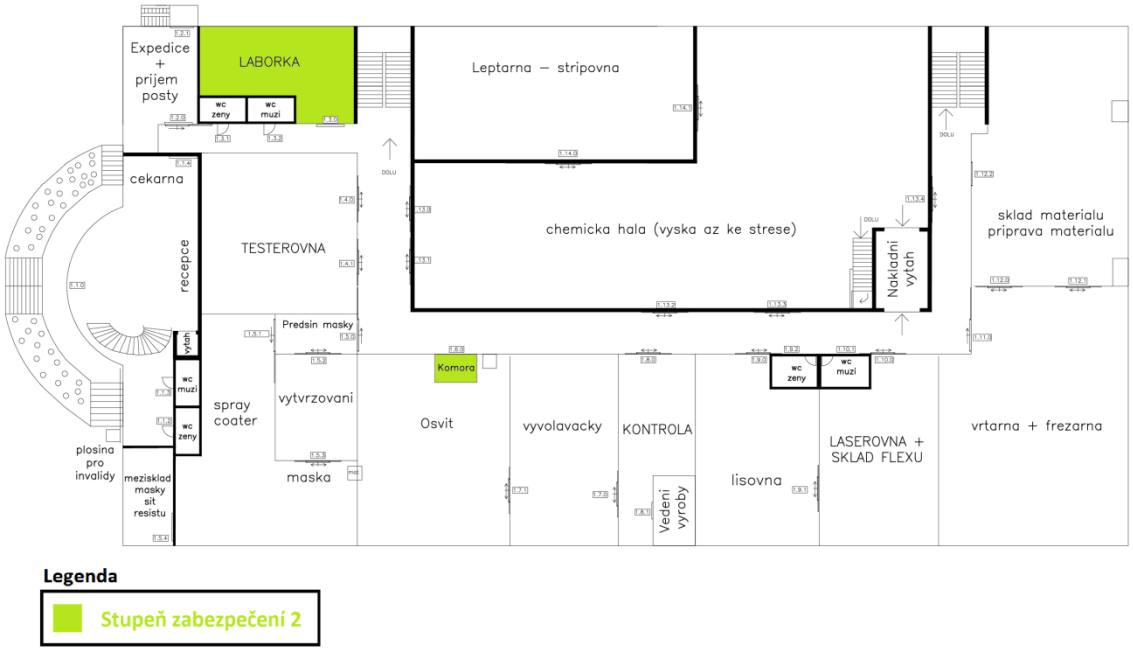
V budově budou instalovány CNC stroje a výrobní linky velmi vysoké hodnoty, ovšem vzhledem k jejich rozměrům a hmotnosti v řádu několika tun je zde riziko krádeže naprosto minimální. Z historie firmy za posledních 20 let zde docházelo pouze k menším krádežím kancelářských potřeb a osobních věcí ze strany zaměstnanců firmy. Systém kontroly vstupu se bude instalovat především za účelem omezení a kontroly pohybu zaměstnanců. Omezením pohybu zaměstnanců a monitoringem jejich pohybu se docílí i zvýšené ochrany drobného majetku firmy. Omezení přístupu do vybraných prostor bude vyžadováno i plánovaným managementem kvality.

Při plánování systému kontroly vstupu bylo nutné počítat i s pohybem autonomních robotů (obr. 16). Původně jsem zamýšlel propojit systém řízení pohybu robotů se systémem SKV, což výrobce robotů by byl schopen umožnit a poskytnout rozhraní pro komunikaci s SKV, ale toto řešení by bylo finančně velmi náročné.

Obr. 16 Mobilní robot OMRON LD60. Převzato z [14]

4.2 Přízemí

Vstup do budovy je možný hlavním vchodem v přízemí (obr. 17) nebo přes mezisklad materiálu bočními vraty určenými pro příjem materiálu ze strany parkoviště. Hlavní vchod je nezabezpečen přístupovým systémem, protože je požadován volný průchod pro zákazníky firmy přímo k otevřené recepci, která se nachází přímo naproti hlavnímu vchodu. Recepce zároveň zajišťuje funkci fyzické ostrahy v minimálním počtu dvou osob na směnu a kontroluje, kdo do budovy vstupuje. Výtah a dveře umožňující vstup z prostoru recepce do výrobní části budovy budou zabezpečeny systémem kontroly vstupu. Hlavní točité schodiště je reprezentativním a designovým prvkem a žádné prvky SKV pro omezení nebo kontrolu prostupu zde nejsou žádoucí, což umožňuje volný průchod do haly v prvním patře.



Obr. 17 Půdorys přízemí.

4.3 Suterén

V suterénu (obr. 18) se nachází druhý možný vchod do celé budovy určený primárně pro příjem materiálu přes nákladovou plošinu. Paralelně s nákladní plošinou je i schodiště. Tyto vchody budou monitorovány systémem CCTV. V suterénu bude většina prostor vybavena systémem pro kontrolu vstupu stupněm zabezpečení 2. Vyšší stupeň zabezpečení 3 byl zvolen pro prostory záložního napájení celé budovy, neboť je to velmi důležitý prvek pro celou firmu. Byť jen krátkodobý výpadek napájení by narušil provoz především che-

mických linek, jejichž restart je časově náročný a pro firmu by to znamenalo nemalý ušlý zisk.

Obr. 18 Půdorys suterénu.

4.4 První patro

V prvním patře (obr. 19) se nacházejí především administrativní kanceláře a prostory. Stupeň zabezpečení 3 v tomto patře budou mít dva prostory, a to serverovna a archiv podkladů. V serverovně bude kromě síťových prvků umístěna také zabezpečovací ústředna a hlavní řídicí jednotka systému kontroly vstupu. Přestože celá budova má vlastní generátor elektrického proudu a záložní bateriové napájení, počítá se samostatným záložním napájením pro přístupový systém umístěným v racku spolu s dalším záložním napájením pro servery a další systémy.

Archiv podkladů si zasluhuje vyšší stupeň zabezpečení, protože má vysokou hodnotu pro firmu. Jsou zde skladovány takzvané kupóny. Kupóny jsou malé desky plošných spojů, které se vyrábí současně s deskami plošných spojů pro koncové zákazníky firmy a archivují se za účelem možnosti zpětné kontroly a vyšetřování v případě reklamace desky plošných spojů zákazníkem. Kupóny se standardně uchovávají minimálně jeden rok u speciálních zakázek. V případě, že se jedná o desky plošných spojů dodávané do vojenského a leteckého průmyslu, existuje zde požadavek na uchovávání těchto kupónů po dobu mini-

málně patnácti let. Možnost manipulace s kupóny ve smyslu jejich ovlivňování je minimální, ovšem jejich ztráta nebo destrukce by mohla pro firmu znamenat velmi závažný problém. Proto bude přístup do místnosti archivu umožněn jen velmi malému počtu stabilních a prověřených zaměstnanců.

Obr. 19 Půdorys prvního patra.

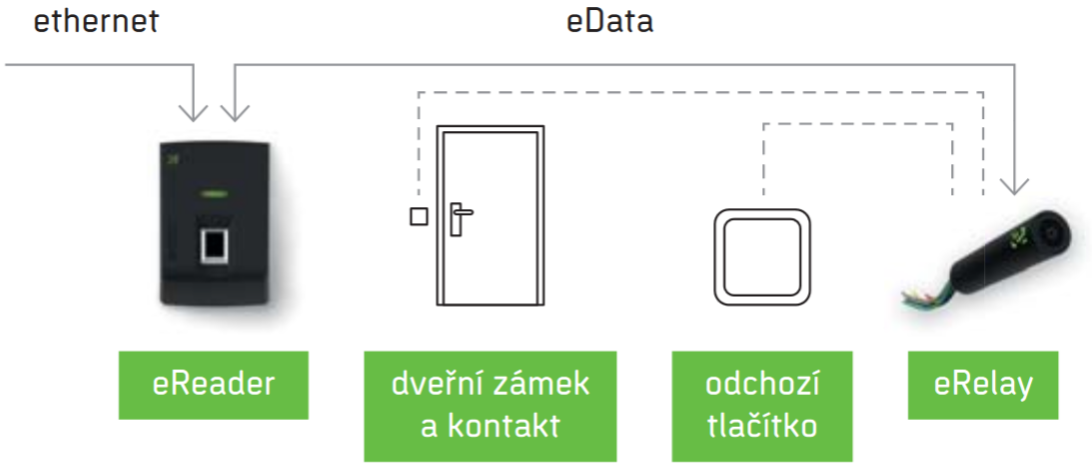
5 PŘEDSTAVENÍ ŘEŠENÍ AKTION

Pro demonstraci konkrétního řešení systému kontroly vstupu jsem vybral modelovou řadu Aktion eSeries od české firmy EFG CZ spol. s r.o. Firma působí na trhu již 20 let, je tedy jistě spolehlivým partnerem s dostatkem zkušeností v oboru. Nabízí jednotné, jednoduché modulární řešení přístupového systému zastřešeného softwarem Aktion NEXT. Tento systém je certifikován pro stupeň zabezpečení 3 a v případě použití grafické nadstavby (ALVIS, C4, apod.) je schopen vyhovět i požadavkům pro stupeň zabezpečení 4.

Produkty řady Aktion eSeries splňují všechny požadavky zadavatele. Vyhovují z hlediska jednoduchého ovládání a správy systému, designu, propojení pomocí LAN sítě a nabízí možnost napájení celého systému přes datové UTP kabely pomocí technologie PoE. Pomocí integračního modulu také otevírá široké možnosti integrace s jinými systémy a možnosti rozšíření funkcí.

Typická konfigurace přístupového bodu je jedna nebo dvě inteligentní čtečky (jedna master, druhá v podřízeném režimu slave). Čtečky mají vestavěné vstupy a výstupy primárně určené pro dveřní kontakt a elektromagnetický zámek. Čtečky mezi sebou komunikují po sběrnici eData a komunikace je pro zvýšení bezpečnosti šifrována protokolem AES 256. Další zvýšení bezpečnosti je možné použitím zařízení eRelay (obr. 20), které zajišťuje bezpečnou komunikaci přes datovou sběrnici eData mezi čtečkou a elektrickým zámkem, případně i dveřním kontaktem (obr. 21). Zařízení eRelay se instaluje přímo do zárubně dveří, čímž se se zaručuje vyšší bezpečnost proti zneužití.

Obr. 20 eRelay. Převzato z [14]



Obr. 21 Možnosti připojení bezpečnostního zařízení eRelay. Převzato z [15]

Inteligentní čtečky řady eSeries disponují funkcí nouzového režimu v případě výpadku sítě LAN a vlastní pamětí událostí. V nouzovém režimu se standardně přístupy osob vyhodnocují na základě platných karet uložených v paměti čtečky s podmínkou, že karta byla alespoň jednou použita ve standardním režimu online. Vlastní ochrana hardwaru je řešena pomocí optického tamperu. Sběrnice eData umožňuje propojit jednotlivé komponenty z řady eSeries šifrovanou komunikací až na vzdálenost 10 m. Stejně tak veškerá komunikace probíhající po síti LAN je šifrována protokolem AES 256 pro maximální ochranu proti zneužití. Z hlediska napájení PoE umožňují připojení komponent (např. dveřního el. zámku) s maximálním odběrem stejnosměrného proudu 340mA při napětí 12V. Kromě klasické podoby dveřního systému se v zabezpečované budově počítá i s automatickými posuvnými dveřmi, jejichž výkonové prvky jsou napájeny z vlastního okruhu a spínaný ovládací obvod nepřesáhne hodnotu zatížení stejnosměrným proudem 50mA.

5.1 eSmartReader

Jedná se o inteligentní čtečku, vyráběnou ve dvou variantách. V provedení ES-310, kdy se jedná pouze o bezkontaktní čtečku karet čipů, nebo v provedení ES-510 která má navíc i snímač otisku prstů (obr. 22). Z designového hlediska jsou pak nabízeny ve dvou barevných variantách – bílá a černá. Čtečka disponuje barevným dotykovým displejem s možností programování vlastního grafického uspořádání a vlastních speciálních funkcí. Tato čtečka může také fungovat jako docházkový terminál.

Obr. 22 eSmartReader ES-310 (vlevo) a ES-510 (vpravo). Převzato z [14]

Tab. 3 – Technické parametry zařízení eSmartReader

Napájecí napětí	12V DC nebo PoE třída 0 (standard IEEE 802.3af)
Komunikační rozhraní	Ethernet 10/100 Mbit
Průměrný proudový odběr	270 mA
Max. Proudový odběr	320 mA
Frekvenční pásmo RFID	13,56 MHz (Mifare, Desfire)
Formát karet	ISO/IEC 14443A, 14443B (Mifare, Desfire)
Čtecí vzdálenost	1 - 7 cm
Datový vstup pro externí snímač/relé	eData (max. vzdálenost 10m), připojení kabelem UTP
Biometrický senzor	Kapacitní, 256 x 360 pixelů, 508 DPI, 4 mil. Cyklů
Vstupy (možno konfigurovat)	BUTT - tlačítko, DOOR - dveřní kontakt
Výstupy (možno konfigurovat)	12 Vout/GND pro napájení externího zařízení (eRelay, eReader) KNO nebo KNC pro připojení nízkoodběrového elektronického zámku
Paměť	2 MB
Kapacita paměti	131070 událostí / 3120 posledních platných karet
Obvod reálného času	Ano
Displej	4.3” TFT, 480x272px, 16bit, dotykový
Vnější rozměry (š x v x h)	84 mm x 199,5 mm x 55 mm
Krytí	IP 40

5.2 eReader

Tato inteligentní čtečka je vyráběna rovněž ve dvou variantách. Verze pouze s bezkontaktním snímáním je označena jako model ER-310 a verze s bezkontaktním snímačem a snímačem otiskem prstů je vydána pod označením ER-510 (obr. 23). Barevná provedení jsou nabízena bílá, černá a šedá. Tyto jednoduché čtečky s integrovanou řídicí jednotkou narozdíl od čteček eSmartReader disponují rozhraním Wiegand pro možnost připojení obyčejných levnějších čteček.

Obr. 23 eReader ER-310 (vlevo) a ER-510 (vpravo). Převzato z [14]

Tab. 4 – Technické parametry zařízení eReader

Napájecí napětí	12V DC nebo PoE třída 0 (standard IEEE 802.3af)
Komunikační rozhraní	Ethernet 10/100 Mbit
Průměrný proudový odběr Master (Slave)	148 mA (73mA)
Max. Proudový odběr Master (Slave)	200 mA (100 mA)
Frekvenční pásmo RFID	13,56 MHz (Mifare, Desfire)
Formát karet	ISO/IEC 14443A, 14443B (Mifare, Desfire)
Čtecí vzdálenost	1 - 7 cm
Datový vstup pro externí snímač/relé	eData (max. vzdálenost 10m), připojení kabelem UTP

Biometrický senzor	Kapacitní, 256 x 360 pixelů, 508 DPI, 4 mil. Cyklů
Vstupy (možno konfigurovat)	BUTT - tlačítko, DOOR - dveřní kontakt
Výstupy (možno konfigurovat)	12 Vout/GND pro napájení externího zařízení (eRelay, eReader) KNO nebo KNC pro připojení nízkoodběrového elektronického zámku
Paměť	2 MB
Kapacita paměti	131070 událostí / 3120 posledních platných karet
Obvod reálného času	Ano
Displej	Ne
Vnější rozměry (š x v x h)	80,4 mm x 121,5 mm x 39 mm
Krytí	IP 40

5.3 eXpander

Univerzální integrační a ovládací modul v průmyslovém provedení (obr. 24). Jedná se v podstatě o přídavné vstupně/výstupní rozhraní, umožňující ovládání samotného přístupového systému (například ze strany EPS) nebo ovládání jiných systémů a funkcí ze strany SKV. Disponuje také dvěma vstupy s rozhraním Wiegand, pro možnost rozšíření přístupového systému.

Obr. 24 Zařízení eXpander. Převzato z [15]

5.4 eBox

Jedná se o hlavní řídicí jednotku nebo spíše centrální server, který zajišťuje řízení sítě inteligentních snímačů. Zprostředkovává rovněž komunikaci mezi těmito snímači a databází. Prodává se jako samostatně závěsný modul s ochranným tamperem nebo ve verzi pro montáž do rackové skříně.

Obr. 25 eBox ve verzi pro montáž do rackové skříně. Převzato z [14]

Tuto jednotku je možné nahradit cloudovým řešením, které však splňuje požadavky stupně zabezpečení maximálně 2 a je tedy pro případ této práce nevhodný.

5.5 AXR-110

Toto zařízení nepatří do řady eSeries, jedná se o obyčejný snímač bezkontaktních identifikátorů (RFID) technologie MIFARE (13,56 MHz) disponující rozhraním Wiegand (obr. 26). Tato čtečka je vhodná do páru k inteligentní čtečce eReader. Má zvýšený stupeň krytí a lze ji tedy případně instalovat i ve venkovním prostředí. Její úzké provedení zase umožňuje instalaci na zárubeň dveří.

Obr. 26 Úzký bezkontaktní snímač AXR-110.

Převzato z [14]

Tab. 5 – Technické parametry bezkontaktního snímače AXR-110

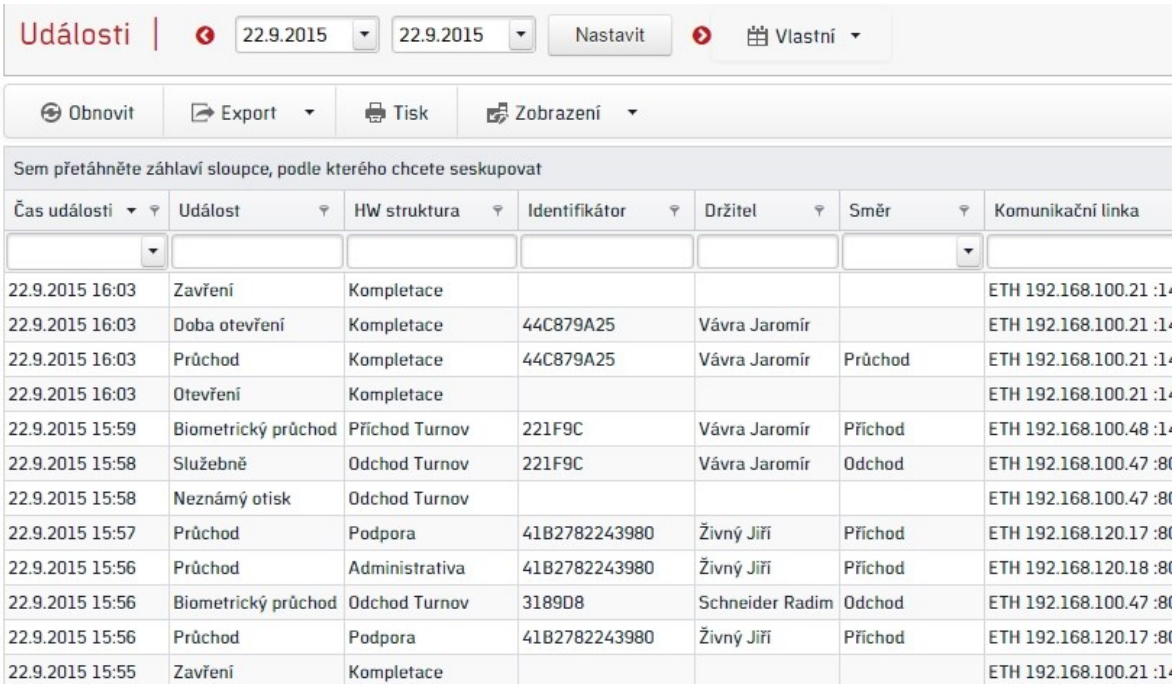
Napájecí napětí	12V DC
Max. Proudový odběr Master (Slave)	75 mA
Frekvenční pásmo RFID	13,56 MHz
Rozhraní	Wiegand 26/42 bitů
Vnější rozměry (š x v x h)	42 mm x 120 mm x 40 mm
Krytí	IP 54

5.6 Software Aktion.NEXT

Software Aktion.NEXT se stará o kompletní správu systému a přesahuje možnosti klasických přístupových systémů. Software mimo jiné umožňuje:

- **Přímé ovládání systému** – slouží ke vzdálenému ovládání konkrétních zařízení z počítače nebo mobilního zařízení.
- **Definici a správu přístupových práv**
- **Módy otevírání** - umožňuje nastavit u jednotlivých snímačů v určitý čas povolení či zamezení vstupu. Lze například nastavit, že v konkrétní dobu je zcela zakázán vstup do budovy i držiteli platné karty nebo je vstup v určitém časovém rozmezí povolen komukoliv, případně pouze při přiložení platné karty.

- **Správu identifikačních tokenů**
- **Monitoring průchodu** - umožňuje sledování průchodu osob na požadovaných snímačích nebo terminálech. K jednomu monitoru lze přiřadit libovolný počet vybraných zařízení, počet monitorů je neomezený. Při průchodu osoby se zobrazí fotografie včetně uživatelsky přednastavených údajů.
- **Prohlížení událostí** – Agenda Události (obr. 27) poskytuje detailní přehled komplexního řízení přístupu, například přiložení neznámé karty, průchody osob, neoprávněné přístupy, změny stavu (otevřeno, zavřeno) a další.



Čas události	Událost	HW struktura	Identifikátor	Držitel	Směr	Komunikační linka
22.9.2015 16:03	Zavření	Kompletace				ETH 192.168.100.21 :1
22.9.2015 16:03	Doba otevření	Kompletace	44C879A25	Vávra Jaromír		ETH 192.168.100.21 :1
22.9.2015 16:03	Průchod	Kompletace	44C879A25	Vávra Jaromír	Průchod	ETH 192.168.100.21 :1
22.9.2015 16:03	Otevření	Kompletace				ETH 192.168.100.21 :1
22.9.2015 15:59	Biometrický průchod	Příchod Turnov	221F9C	Vávra Jaromír	Příchod	ETH 192.168.100.48 :1
22.9.2015 15:58	Služebně	Odchod Turnov	221F9C	Vávra Jaromír	Odchod	ETH 192.168.100.47 :8
22.9.2015 15:58	Neznámý otisk	Odchod Turnov				ETH 192.168.100.47 :8
22.9.2015 15:57	Průchod	Podpora	41B2782243980	Živný Jiří	Příchod	ETH 192.168.120.17 :8
22.9.2015 15:56	Průchod	Administrativa	41B2782243980	Živný Jiří	Příchod	ETH 192.168.120.18 :8
22.9.2015 15:56	Biometrický průchod	Odchod Turnov	3189D8	Schneider Radim	Odchod	ETH 192.168.100.47 :8
22.9.2015 15:56	Průchod	Podpora	41B2782243980	Živný Jiří	Příchod	ETH 192.168.120.17 :8
22.9.2015 15:55	Zavření	Kompletace				ETH 192.168.100.21 :1

Obr. 27 Prohlížení událostí. Převzato z [14]

Tento software také podporuje další integraci do bezpečnostních systémů jako je C4, Alvis nebo IP kamerový systém Ateas.

6 KRITÉRIA PRO HODNOCENÍ DODAVATELŮ ACS

Kritéria a požadavky na systémy kontroly vstupů, podle kterých lze vybírat dodavatele je celá řada. Cílem je zvolit nejlepší možný kompromis mezi všemi požadovanými kritérii.

6.1 Požadavky na dodavatele

Jedním z hlavních požadavků na dodavatele je jeho spolehlivost a kvalita. U dodavatele, respektive u výrobce, je zárukou kvality délka jeho působení na trhu (například alespoň 10let) a případně také reference od jiných subjektů. Je žádoucí, aby dodavatel byl schopen poskytnout servis, aktualizace, náhradní díly a případně další komponenty pro budoucí rozšíření systému po co nejdelší možnou dobu.

Dalším kritériem pro výběr dodavatele je schopnost dodání systému od jeho objednání až po jeho instalaci a délka poskytované záruky.

6.2 Požadavky na systém, funkce a vazby

Hlavním požadavkem je, aby se celý systém dal ovládat z jednoho místa. Tento požadavek by měl být schopen splnit dnes již každý dodavatel na trhu. Stejně tak je velmi důležitá přehlednost a jednoduchost programového vybavení, aby obsluhu systému zvládl člověk s běžnými znalostmi a zkušenostmi v oblasti práce s PC.

Požadavkem zadavatele je, aby identifikace osob byla možná biometricky i pomocí předmětu (bezkontaktní karty) zároveň na všech frekventovaných místech. V prostorech s méně častým pohybem osob jako jsou například strojovny a některé typy skladů je pak možné použít čtečky bez biometrické identifikace, a to především z důvodu finanční úspory. Biometrická identifikace se předpokládá za pomoci otisku prstu a neměla by příliš zdržovat uživatele systému. K tomu je požadovaná identifikace za pomocí předmětu mimo jiné také proto, že někteří zaměstnanci mají odmítavý postoj k biometrické identifikaci a nechtějí poskytnout svá biometrická data k dispozici zaměstnavateli. Dalším důvodem jsou zaměstnanci pracující s chemií a barvami, kteří mají velmi často znečištěny ruce během své pracovní doby, což znemožňuje jejich identifikaci za pomoci otisku prstů. Z tohoto důvodu by jim mohly být přiděleny i identifikační předměty, které jsou bezkontaktní a odolné vůči znečištění.

Propojení jednotlivých přístupových bodů je vyžadováno pomocí UTP kabeláže, tedy s využitím sítě LAN. LAN síť je oddělena od přístupu k síti WAN a částečně sdílena se sítí

pro vzdálenou správu strojů a výrobních linek, systém kontroly vstupu však zde bude mít vyhrazenou vlastní virtuální privátní síť (VPN). K zajištění napájení jednotlivých přístupových bodů je maximálně preferováno použití PoE.

Další požadavky na přístupový systém:

- snadné rozšíření systému
- možnost definice přístupových bodů
- možnost rozdělení do zón
- možnost definice jednotlivých uživatelů a jejich práv
- možnost definice časových omezení
- automatická ochrana systému
- možnosti integrace s jinými poplachovými a nepoplachovými systémy

V neposlední řadě je důležitým kritériem pro výběr viditelných prvků (čteček) také jejich design a to především těch, umístěných v reprezentativní vstupní části budovy tak, aby nenarušovaly okolní estetiku a firemní kulturu.

6.3 Požadavky na speciální funkce

6.3.1 Antipassback

Jedná se o funkci přístupového systému, kdy je povolení ke vstupu do jedněch prostor podmíněn korektním opuštěním předchozích prostor. Opakovaný vstup je tedy podmíněn výstupem, což eliminuje možnost průchodu více osob na jeden token a zároveň se tak zvyšuje bezpečnost systému. Použití této funkce si tedy vynucuje, aby průchozí místo bylo vždy opatřeno snímacím zařízením na vstupu i výstupu.

Tato funkce bude v návrhu aplikována pro všechny prostory s třetím stupněm zabezpečení.

6.3.2 Interlock

Funkce interlock, neboli pásmová (či komorová) propusť, umožňuje do daného prostoru vstoupit některými z dveří, pouze pokud se v prostoru již někdo nenachází. Jakmile někdo do takto zabezpečeného prostoru vstoupí, není dovnitř vpuštěn nikdo další, dokud osoba zabezpečený prostor sama neopustí.

Tato funkce je požadována v přestupové komoře pro zajištění vyšší čistoty prostředí v prostoru pro osvit.

6.4 Možnosti integrace

Při posuzování možností integrace s poplachovými systémy je rozhodující, zda firma již nějaký systém má a případně na jakých prvcích a na jakém vedení je tento systém postaven. Zadavatelská firma zatím žádný nemá a v budoucnu jej bude řešit soukromá bezpečnostní agentura, která ovšem nepočítá s integrací přístupového systému do poplachového zabezpečovacího systému.

Žádoucí naopak bude, aby systém bylo možné integrovat s elektrickou požární signalizací (EPS). EPS je vždy samostatným systémem a v případě požáru a s tím spojené evakuace je nutné zajistit odblokování všech přístupových bodů blokujících únikové cesty.

6.5 Výhody a nadstandardní přínosy

V poslední řadě lze při výběru dodavatele také přihlédnout k nadstandardním nabídkám a přínosům, jako je třeba možnost propojení systému kontroly vstupu s cloudovou technologií. Lze posuzovat i technické výhody, jako například složitost instalace.

7 ODHAD BUDOUCÍHO VÝVOJE

Potenciál budoucího vývoje přístupového systému v zadavatelské firmě vidím především v oblasti integrace s jinými nepoplachovými systémy.

Docházkový systém

Firma si přála zachovat svůj stávající docházkový systém, avšak po zaběhnutí firmy v nové budově a vypršení platnosti licencí pro stávající docházkový systém by zde mohlo dojít k integraci se systémem kontroly vstupu.

IT systémy

Z hlediska zvýšení informační bezpečnosti a ochrany dat se zde nabízí možnost využít identifikační prvky přístupového systému i k řízení přístupu do sítě a přihlašování uživatelů k PC. To se řeší pomocí čtečky připojené přímo k PC (obr. 28) podpořené příslušným bezpečnostním softwarem, instalovaném na daném počítači. Uživatel se přihlásí ke svému PC a po opuštění místnosti je jeho PC zablokován.

Obr. 28 USB čtečka karet
OMNIKEY. Převzato z [15]

Ovládání pracovišť

Firma řeší problém, kdy zaměstnanci zapomínají vypínat zařízení na svých pracovištích. Jedná se především o počítače nebo ovládací stanice k výrobním linkám. Tato zařízení pak běží zbytečně 16 hodin denně a spotřebovávají elektrickou energii, což firmu ročně stojí nemalou finanční částku. Bylo by tedy možné softwarově propojit systém kontroly vstupu s hlavním serverem, který je schopen po síti LAN rozesílat požadavky na vypnutí nebo zapnutí jednotlivých pracovních stanic. Systém kontroly by při rozpoznání vstupu osoby do budovy poslal požadavek na hlavní server firmy, který by nastartoval příslušné pracoviště osoby a při jejím odchodu z firmy by zase toto pracoviště vypnul. To by přineslo ne-

jen úsporu finančních prostředků, ale zároveň zvýšilo pracovní komfort pracovníkům na pracovištích, kterých se tento problém týká. Start některých pracovních stanic je časově náročný, takže by se ušetřil i čas, protože stanice by startovala během toho, co se její obsluha převléká v šatně.

ZÁVĚR

V úvodu práce jsem popsal, co to jsou přístupové systémy, principy jejich fungování a jejich stávající možnosti. Zaměřil jsem se především na možnosti identifikace, protože právě ty jsou nepostradatelnou součástí systému kontroly vstupu. Objasnil jsem princip činnosti procedur ověřování identity a shrnul jejich hlavní výhody a nevýhody. Dále jsem vysvětlil, na jakých principech fungují biometrické snímače a proces biometrické identifikace, která je v dnešní době poměrně drahá, ale moderní. Nejčastěji rozšířená je metoda identifikace podle otisku prstu. Ve třetí kapitole jsem pak uvedl, v jakých konfiguracích lze systémy kontroly vstupu projektovat a s jakými možnostmi a funkcemi lze počítat, neboť je v této době je schopen splnit každý tradiční výrobce prodávající na českém trhu (Honeywell, Aktion, Jablotron,…). Svůj prostor v teoretickém úvodu by si jistě zasloužili i akční komponenty SKV, ovšem k popsání veškerých možností a komponent přístupových systémů v této bakalářské práci není prostor.

Cílem mé bakalářské práce bylo především zpracovat normy a certifikace, které by se vztahovaly k problematice řešení přístupových systémů v budovách subdodavatelů výrobků pro vojenský a letecký průmysl. Toto téma jsem si vybral na podnět mého zaměstnavatele, který plánuje stavbu nové výrobní budovy spojené se získáním potřebných certifikací a dodržení příslušných norem. Ačkoliv to není na první pohled z této práce zřejmé, časově nejnáročnějším úkolem bylo zjistit, které normy a certifikace bude potřeba splnit a získat. Po zdlouhavém vyjednávání se zahraničními potenciálními zákazníky firmy se mi podařilo sestavit seznam norem a certifikací, jejž požadují po svých subdodavatelích v průmyslovém odvětví výroby plošných spojů. Očekáváním byly speciální požadavky na řízení přístupu k materiálům a polotovarům v průběhu celé výroby včetně záznamu historie. Z pozdějšího prostudování seznamu požadavků však vyplynulo, že toto je požadováno až na vyšším stupni kompletaci výrobků a nikoliv u subdodavatelů, jako jsou výrobci plošných spojů, kde je požadována především ochrana dat a dodržování kvality výroby. Jediné normy explicitně pojednávající o požadavcích na přístupové systémy jsou normy české.

V praktické části jsem provedl návrh přístupového systému v nově vznikající výrobní budově, který se jeví jako nejvýhodnější. Stanovení požadovaných úrovní stupně zabezpečení bylo konzultováno se zadavatelem a vzhledem k bezproblémové historii ve firmě ustupovala potřeba vyššího zabezpečení především potřebě plynulého a rychlého provozu firmy. Budova byla za pomoci SKV logicky rozdělena na reprezentativní část pro zákazníky a

výrobní část, kde především v přízemí je velká potřeba neomezeného pohybu téměř všech zaměstnanců dohromady s automatizovanými roboty. Obecně totiž platí nepřímá úměra mezi mírou zabezpečení a mírou komfortu uživatelů systému.

Dále byla stanovena kritéria pro výběr případného dodavatele systému kontroly vstupu spolu s hlavními požadavky na funkce a další možnosti systému. V budoucím vývoji přístupového systému ve firmě vidím velký potenciál, proto v poslední části této práce zmiňuji hlavní směry, kterými by se měla po zaběhnutí firma ubírat.

SEZNAM POUŽITÉ LITERATURY

1. Snímání čárového kódu lineárním CCD. *Wikimedia.* [Online] 13. 4 2006. [cit. 12. 4 2018.] Dostupné z: https://commons.wikimedia.org/wiki/File:Barcode_reader.png.

2. ELEKTROREVUE. Magnetické karty a jejich principy ukládání dat. Elektrorevue.cz [online]. ©2009 [cit. 2018-04-22]. Dostupné z: http://www.elektrorevue.cz/clanky/02054/index.html.

3. Hanáček, P. a Matyáš, V. Čipová karta v informačních systémech [online]. Brno : Datakon, 2003 [cit. 2018-03-10]. Dostupné z: www.fit.vutbr.cz/~hanacek/papers/Datakon03.pdf.

4. KENEX. RFID čip pro IP videotelefony HIKVISION. Kenex.cz. [onli-ne]. ©2018. [cit. 2018-04-26]. Dostupné z: https://www.kenex.cz/prislusenstvi-pro-videotelefony/rfid-cip-pro-ip-videotelefony-hikvision/.

5. BARCODE TECHNOLOGIES. RFID Hang Tag. Barcode-uk.com. [online]. ©2017. [cit. 2018-04-26]. Dostupné z: https://www.barcode-uk.com/group/rfid-products/rfid-labels-tags/barcode-technologies/rfid-hang-tag.

6. ACTIVE ROBOTS. RFID Tag – Watch with Adjustable Strap. Active-robots.com. [online]. ©2017. [cit. 2018-04-26]. Dostupné z: https://www.active-robots.com/3917-0-t5577-rfid-tag-watch-with-adjustable-strap.html.

7. Papilogramas. *Papiloscopia.* [Online] 2002. [cit. 15. 4 2018.] Dostupné z: http://www.papiloscopia.com.br/estudo_das_papilas.html..

8. VESMÍR. Identifikace skenem duhovky. Vesmir.cz [online]. ©2011 [cit. 2018-04-19]. Dostupné z: https://vesmir.cz/cz/casopis/archiv-casopisu/2011/cislo-2/identifikace-skenem-duhovky.html.

9. LUKáŠ, Luděk a kolektiv. *Bezpečnostní technologie, systémy a management IV.* 1. vydání. Zlín : Radim Bačuvčík - VeRBuM, 2014. 978-80-87500-57-6.

10. LUKÁŠ, Luděk a kolektiv. *Bezpečnostní technologie systémy a management I.* 1. Vydání. Zlín : Radim Bačuvčík - VeRBuM, 2011. 978-80-87500-5-7.

11. ČSN EN 60839-11-1. *Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

12. HUSÁK, Miroslav, Tomáš VÍTEK a Tomáš TEPLÝ. Přístupové systémy (3). *atpjournal.* [Online] 26. 7 2012. [cit. 20. 3 2018.] Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/pristupove-systemy-3.html?page_id=15353.

13. eSmartReader ES-510/W. *Aktion.* [Online] 28. 9 2014. [cit. 1. 5 2018.] Dostupné z: http://www.aktion.cz/evidence-dochazky/mala-firma-do-50-zamestnancu.html#terminal.

14. Mobile Robot. *OMRON.* [Online] 2018. [cit. 22. 5 2018.] Dostupné z: https://industrial.omron.eu/en/products/mobile-robot.

15. Moderní řízení přístupu. *AKTION.* [Online] 2018. [cit. 15. 5 2018.] Dostupné z: http://www.aktion.cz/reseni/elektronicka-kontrola-vstupu/prumyslova-vyroba.html.

16. Katalogový list eSeries. *Aktion.* [Online] 26. 5 2016. [cit. 15. 5 2018.] Dostupné z: http://www.aktion.cz/aktion_cs/download/katalogove-listy/eseries.pdf.

17. SUNTECH COMPUTER. Omnikey 3121 externí kontaktní čtečka Smart card. Suntech.cz [online]. ©2011 [cit. 2018-05-20]. Dostupné z: https://vesmir.cz/cz/casopis/archiv-casopisu/2011/cislo-2/identifikace-skenem-duhovky.html.

18. KŘEČEK, Stanislav. *Příručka zabezpečovací techniky.* Vyd. 2. Blatná : Blatenská tiskárna, 2003. 80-902938-2-4.

19. LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management III. Zlín : Radim Bačuvčík - VeRBuM, 2013. 1. Vydání.

20. NAVAROVÁ, Šárka, Tomáš KYNCL a Kamil ŠTĚTINA. Projektování přístupových a docházkových systémů. *ADI Global Distribution.* [Online] 24. 3 2011. [cit. 10. 2 2018.] Dostupné z: https://www.adiglobal.cz/iiWWW/cz/Produkty110.nsf/wp/projektanti_prihlasen/$file/Projektovani_pristupovych_systemu.pdf.

21. ROSOL, Ivo. Moderní docházkové a přístupové systémy. *SystemOnLine.* [Online] 10 2010. [cit. 10. 2 2018.] Dostupné z: https://www.systemonline.cz/hrm-personalistika/moderni-dochazkove-a-pristupove-systemy.htm.

22. ŠTĚTINA, Kamil a Tomáš KYNCL. Úvod do přístupových systémů. *ADI Global Distribution.* [Online] 13. 7 2009. [cit. 10. 2 2018.] Dostupné z:

https://www.adiglobal.cz/iiWWW/cz/Produkty110.nsf/wp/projektanti_prihlasen/$file/Uvod_do_prist_systemu.pdf.

23. ČSN CLC/TS 50398. *Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009.

24. ČSN EN 60839-11-2. *Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016.

25. Uživatelský manuál eSmartReader. *Docházka online.* [Online] 4. 4 2017. [cit. 20. 5 2018.] Dostupné z: https://www.dochazkaonline.cz/manuals/esmartreader.pdf.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Access Control System
CCTV	Uzavřený televizní okruh
ČSN	Česká norma
EMC	Elektromagneticp
EN	Evropská norma
EPS	Elektrická požární signalizace
FAR	False Acceptance Rate – Míra chybného přijetí
FRR	False Reject Rate - Míra chybného odmítnutí
ISO	Mezinárodní norma
IT	Informační technologie
KNC	Kontakt relé – v klidu sepnutý
KNO	Kontakt relé – v klidu rozepnuty
LAN	Local Area Network
PC	Personal Computer – Osobní počítač
PoE	Power over Ethernet – napájení po ethernetové síti
RFID	Radiofrekvenční identifikace
RS-485	Komunikační sběrnice
SKV	Systém kontroly vstupu
SQL	Structured Query Language – strukturovaný dotazovací jazyk
TCP/IP	Sada protokolů pro komunikaci v počítačové síti
USB	Universal Seriál Bus
VPN	Virtual Private Network
WAN	Wide Area Network

SEZNAM OBRÁZKŮ

Obr. 1 Blokové schéma přístupového bodu 12
Obr. 2 Blokové schéma přístupového systému 13
Obr. 3 Čtení čárového kódu. Převzato z [1] 16
Obr. 4 Stopy pro zápis dat na magnetický proužek. Převzato z [2] 16
Obr. 5 Blokové schéma čipové karty. Převzato z [3] 17
Obr. 6 RFID tagy. Převzato z [4] [5] [6] 18
Obr. 7 Blokové schéma biometrického systému 18
Obr. 8 Markanty na otisku prstu. Převzato z [7] 20
Obr. 9 Identifikace duhovky. Převzato z [8] 21
Obr. 10 Sběrnicové spojení řídicích jednotek. Převzato z [12] 30
Obr. 11 Sběrnicové propojení inteligentních čteček. Převzato z [12] 30
Obr. 12 Konfigurace s IP kontroléry. Převzato z [12] 32
Obr. 13 Konfigurace s IP čtečkami. Převzato z [12] 33
Obr. 14 Inteligentní IP čtečka *eSmartReader ES-510/W*. Převzato z [13] 34
Obr. 15 Znázornění třívrstvé architektury. Převzato z [12] 35
Obr. 16 Mobilní robot OMRON LD60. Převzato z [14] 37
Obr. 17 Půdorys přízemí. 38
Obr. 18 Půdorys suterénu. 39
Obr. 19 Půdorys prvního patra. 40
Obr. 20 eRelay. Převzato z [14] 41
Obr. 21 Možnosti připojení bezpečnostního zařízení eRelay. Převzato z [15] 42
Obr. 22 eSmartReader ES-310 (vlevo) a ES-510 (vpravo). Převzato z [14] 43
Obr. 23 eReader ER-310 (vlevo) a ER-510 (vpravo). Převzato z [14] 44
Obr. 24 Zařízení eXpander. Převzato z [15] 45
Obr. 25 eBox ve verzi pro montáž do rackové skříně. Převzato z [14] 46
Obr. 26 Úzký bezkontaktní snímač AXR-110. Převzato z [14] 47
Obr. 27 Prohlížení událostí. Převzato z [14] 48
Obr. 28 USB čtečka karet OMNIKEY. Převzato z [15] 52

SEZNAM TABULEK

Tab. 1 – Názvy jednotlivých norem 22
Tab. 2 – Stupně klasifikace [11] 23
Tab. 3 – Technické parametry zařízení eSmartReader 43
Tab. 4 – Technické parametry zařízení eReader 44
Tab. 5 – Technické parametry bezkontaktního snímače AXR-110 47

SEZNAM PŘÍLOH

Příloha P I CD

Příloha P II Půdorys suterénu budovy

Příloha P III Půdorys přízemí budovy

Příloha P IV Půdorys prvního patra budovy

Příloha P V Návrh SKV - suterén

Příloha P VI Návrh SKV - přízemí

Příloha P VII Návrh SKV – první patro

PŘÍLOHA P I: CD

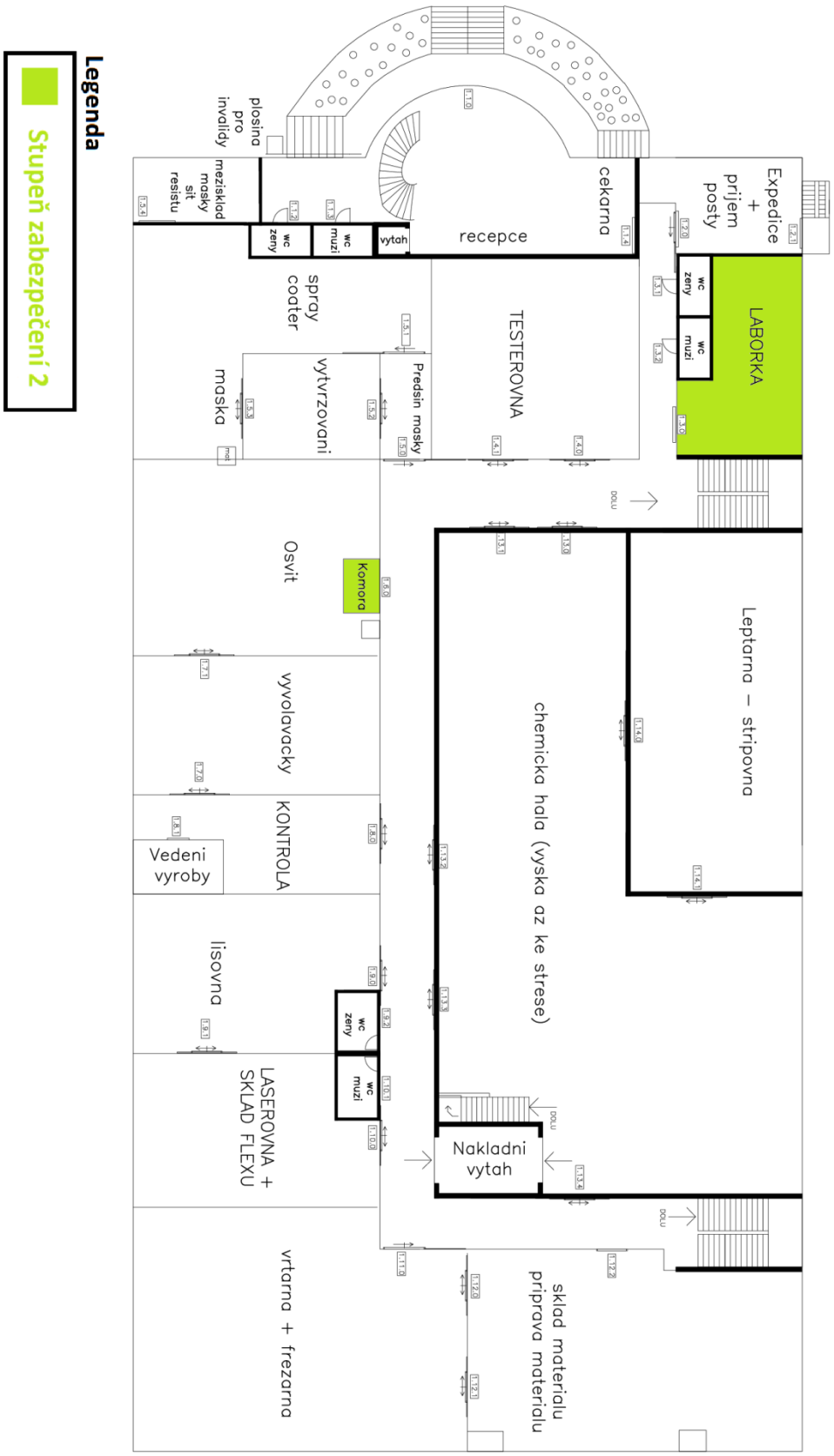
K této práci je přiloženo CD, na kterém je uložena elektronická verze této bakalářské práce ve formátu pdf a přílohy ve formátu zip.

Adresářová struktura přiloženého CD:

- .\bakalarska_prace_stipekj.pdf
- .\Prilohy.zip

PŘÍLOHA P II: PŮDORYS SUTERÉNU BUDOVY

PŘÍLOHA P III: PŮDORYS PŘÍZEMÍ BUDOVY



PŘÍLOHA P IV: PŮDORYS PRVNÍHO PATRA BUDOVY