Srovnání profesionálních a jiných prvků kontroly vstupu na trhu České republiky

Tomáš Groš

Bakalářská práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

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

Jméno a příjmení:	**Tomáš Groš**
Osobní číslo:	**A11568**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Srovnání profesionálních a jiných prvků kontroly vstupu na trhu České republiky**
Téma anglicky:	**A Comparison of the Professional and Other Access Control Elements in the Czech Republic Market**

Zásady pro vypracování:

1. **Vysvětlete a popište, co jsou prvky kontroly vstupu.**
2. **Zpracujte normy pro kontrolu vstupu a integrované systémy zahrnující ACCESS.**
3. **Vybrané prvky zprovozněte, navrhněte metody testování a zaznamenejte výsledky.**
4. **Zhodnoťte a porovnejte dané prvky.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LAUCKÝ, Vladimír a Rudolf DRGA. Specialní technologie komerční bezpečnosti [online]. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012 [cit. 2015-02-03]. ISBN 978-80-7454-146-9. Dostupné z: http://www.utb.cz/**
2. **LUKÁŠ, Luděk. Bezpečnostní technologie,systémy a management 3. 1. vyd. Zlín: VeRBuM, 2013. ISBN 978-80-87500-35-4.**
3. **ČSN EN 50133-1. Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 1: Systémové požadavky. 1. vyd. Praha: Český normalizační institut, 2001.**
4. **VALOUCH, Jan. Projektování bezpečnostních systémů. Zlín, 2012. ISBN 978-80-7454-230-5. Univerzita Tomáše Bati ve Zlíně.**
5. **FOJTÍK, Daniel. Systémy kontroly vstupu pro kombinované a integrované systémy. Zlín, 2010. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.**

Vedoucí bakalářské práce: **Ing. Hana Charvátová, Ph.D.**
Ústav automatizace a řídicí techniky

Datum zadání bakalářské práce: **6. února 2015**

Termín odevzdání bakalářské práce: **3. června 2015**

Ve Zlíně dne 6. února 2015

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ Fakulta aplikované informatiky

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

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 25.5.2015

.....
podpis diplomanta

ABSTRAKT

Tato práce se zabývá srovnáním profesionálních a jiných prvků kontroly vstupu, které se nacházejí na trhu České republiky. V teoretické části se zabývá základním popisem, co jsou systémy kontroly vstupu a jaké prvky obsahují. Dále popisuje normy vztahující se k systému kontroly vstupu. V praktické části jsou popsány vybrané prvky, které jsou zprovozněny a otestovány. Dále jsou vybrané prvky porovnány a zhodnoceny.

Klíčová slova: systémy kontroly vstupu, elektronické stavebnice, srovnání, klávesnice, bezkontaktní čtečky

ABSTRACT

This work deals with a comparison of professional and other elements of access control, located on the Czech market. The theoretical part deals with the basic description of what they are access control systems and what elements it contains. Further describe the rules relating to the access control system. The practical part describes selected elements that are commissioned and tested. The following are selected elements compared and evaluated.

Keywords: access control systems, electronic kits, compare, keypad, proximity card

Rád bych poděkoval paní Ing. Haně Charvátové, Ph.D. za spolupráci, cenné rady a názory při vypracovávání mé bakalářské práce. Dále bych rád poděkoval panu Ing. Rudolfu Drgovi, Ph.D. za technickou pomoc při vypracovávání této práce. Také panu Jaroslavu Kaufmanovi z firmy ADI Global Distribution za cennou konzultaci a rady, ale především za správné nasměrování. Také bych rád poděkoval mé rodině za pevné nervy a podporu při vypracovávání.

OBSAH

ÚVOD

Tématem této bakalářské práce je srovnání profesionálních a jiných prvků kontroly vstupu na trhu České republiky. V mé práci za profesionální prvky považuji všechna zařízení sloužící pro systém kontroly vstupu, které vyrobily specializované firmy zabývající se tímto odvětvím. Na trhu se nachází mnoho velkých nadnárodních firem, ale i několik ryze českých. Mezi nejznámější patří firmy jako HONEYWELL, CDVI, ROSSLARE, SIEMENS a například i česká firma COMINFO. Jejich výrobky splňují všechny technické a systémové požadavky, které nám určují normy, zákony a nařízení vlády. Jejich výrobky se vyznačují kvalitním provedením a vkusným vzhledovým provedením, díky němuž jsou i cenově dražší. Za jiné prvky kontroly vstupu ve své práci považuji takzvané elektronické stavebnice. Tyto stavebnice jsou vyráběny v mnoha různých provedeních a různých funkcích. Můžeme se setkat se stavebnicemi, umožňujícími například dálkové ovládání, měření a regulování. Dále lze také sestavit různé druhy zabezpečovací techniky a audio techniky, napájecích zdrojů, zábavní techniky apod. Tyto stavebnice jsou dodávány ve formě desky tištěných spojů společně se součástkami a návodem k osazení. Na zákazníkovi je pak, aby si daný výrobek zkompletoval a zprovoznil sám.

Mým úkolem v této bakalářské práci je nejprve popsat, co jsou to systémy kontroly vstupu, z čeho jsou složeny a jaké musí plnit základní úkoly a funkce. Dále popsat veškeré normy, které se systémem kontroly vstupu zabývají. Posléze vybrané výrobky systémů kontroly vstupu sestavit, zprovoznit a odzkoušet. Nakonec dané výrobky porovnat a celkově zhodnotit.

Cílem mé práce je ze získaných informací posoudit základní rozdíly mezi profesionálními výrobky a elektronickými stavebnicemi. Svou prací bych rád přispěl k seznámení se se systémy kontroly vstupu používanými v současné době.

I. TEORETICKÁ ČÁST

1 PODOBA ČINNOSTÍ V PRŮMYSLU KOMERČNÍ BEZPEČNOSTI

V současné době dělíme z hlediska použitých metod ochrany v průmyslu komerční bezpečnosti na: [1]

a) **ochranu osob,**
b) **ochranu majetku.**

V průmyslu komerční bezpečnosti má samozřejmě ochrana osob, zejména pak ochrana života a zdraví, vždy přednost před ochranou majetku.

Dále se dělí ochrana osob a majetku na: [1]

a) **fyzickou ochranu,**
b) **technickou ochranu,**
c) **kombinovanou ochranu.**

1.1 Fyzická ochrana

Jedná se o jednu z nejstarších a nejčastějších forem ochrany osob a majetku. Její nespornou výhodou je, že v případě potřeby lze provést okamžitý zásah k ochraně našich aktiv nebo alespoň snížit riziko škody na minimum. Je prováděna takzvanou živou silou, kde se jedná o strážné, hlídače, hlídací službu nebo policisty. Zajišťování fyzickou ostrahou bývá z pravidla nejnákladnější způsob zajištění bezpečnosti. [1]

1.2 Technická ochrana

Je určena ke zvýšení účinnosti fyzické ochrany objektů, ale bez přímé vazby na fyzickou ochranu, nemůže být efektivní. Tvoří jen dočasnou překážku bránící osobám ke vniknutí do objektu. Na ochranu se používá technických prvků, které lze rozdělit v průmyslu komerční bezpečnosti na: [1]

a) **mechanické,**
b) **elektronické (elektrické),**
c) **smíšené a speciální.**

Tyto prvky lze dále dělit na:

a) **Obvodová (perimetrická) ochrana** - ukazuje narušení obvodu objektu. Obvodem objektu se rozumí jeho katastrální hranice, která je tvořena přírodními nebo umělými bariérami, například potoky, zdmi, ploty. [2]

b) **Plášťová ochrana** - ukazuje narušení pláště budovy. Převážně ji tvoří stěny, okna, dveře, zámky, mříže atd. [2]
c) **Prostorová ochrana** - ukazuje narušení a změny uvnitř budovy. Tvoří ji převážně dveře, zámky, kamerové systémy, systémy kontroly vstupu, poplachové zabezpečovací systémy s detektory narušení. [2]
d) **Předmětová ochrana** - signalizuje napadení nebo neoprávněnou manipulaci s chráněnými předměty. Tvoří je vitríny, skleněné tabule, kamerové systémy, atd. [2]

1.2.1 Mechanická ochrana

Jedná se o ochranu majetku a osob za pomocí mechanických zábranných systémů nebo systémů znesnadňujících vniknutí do chráněného objektu. Mezi tyto prvky řadíme zábranné systémy obvodové, plášťové a předmětové ochrany. Může se jednat o ploty, brány, turnikety, mříže, okna, rolety, zámky, trezory. [1]

1.2.2 Elektronická ochrana

Jedná se o ochranu majetku a osob za pomocí elektrických prvků. Mezi tyto prvky jsou řazeny - elektrická zabezpečovací signalizace, elektrická požární signalizace, uzavřené televizní okruhy, přístupové a docházkové systémy, biometrické identifikační systémy, ochrana dat a informací, satelitní vyhledávání vozidel, zdravotní a nouzová signalizace. [1]

1.2.3 Smíšená a speciální ochrana

Za smíšenou ochranu osob a majetku považujeme kombinaci mechanických zábranných systémů a elektronickou ochranu jako jednoho celku. Zejména se muže jednat o elektronické blokování dveří a kombinované elektromechanické zámky. [2]

Za speciální ochranu osob a majetku považujeme individuální technickou ochranu, chemickou ochranu předmětů a dokumentů a obranné a ochranné technické zákroky. Tato ochrana slouží k nezákonnému umisťování odposlechů a pozorovacích prostředků. [3]

1.3 Kombinovaná ochrana

Kombinovaná ochrana řeší nejvhodnější systémy výše zmíněných ochran, které se využívají ve velkých nebo důležitých podnicích, v inteligentních budovách nebo ve městech při realizaci integrovaného záchranného systému. [3]

2 SYSTÉMY KONTROLY VSTUPU

2.1 Základní popis systému kontroly vstupu

Přístupový systém, takzvané systémy kontroly vstupu, je možné chápat jako určitý soubor opatření k zajištění a evidence 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 jako vždy nejúčinnější je jejich kombinace. Pro vstup nebo odchod z námi zabezpečeného prostoru jsou danému zaměstnanci nebo uživateli přidělena přístupová práva na základě profesní politiky stupně oprávnění nebo určitého časového harmonogramu apod. Po této identifikaci a ověření je buď vstup povolen, nebo zamítnut. Složitější systémy pak mohou sledovat pohyb a přítomnost osob v jednotlivých úsecích nebo za běhu měnit přístupová práva. Obecně lze systém kontroly vstupu popsat a shrnou do tří bodů:

KDO se dostane **KAM** a **KDY**.

Následně je velmi nutné rozlišovat pojmy „přístupové“ a „docházkové“ systémy. Za docházkový systém lze tedy 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 aktiv, informací a dat na základě jednoznačně předepsaných pravidel. [2]

2.1.1 Základní úkoly a funkce systémů kontroly vstupu

Ve spolupráci se všemi fyzickými, mechanickými a elektronickými systémy a jejich kombinacemi lze říct, že plní dva základní úkoly: [1]

a) Řídí pohyb osob v objektu v denním režimu, to zpravidla v době kdy je systém EZS odblokován, nebo jeho část je odblokována a nestřeží. [1]
b) Poskytují informace o pohybu osob v objektu, trvale tyto informace zaznamenávají a sledují. Dále také zaznamenávají místo pohybu a čas. Tím přispívají k ochraně objektu i režimovým opatřením. [1]

Mezi další úkoly, které musí systém plnit, patří především:

- omezení přístupu nepovolaných osob do určitých prostor objektu (sklady, výpočetní centra, kanceláře, nebezpečné provozy), [1]
- omezení přístupu mimo určité časové úseky (zaměstnanci, návštěvníci, noční, denní, úklid, zásobování), [1]
- registrace délky pobytu, doby pobytu, místa a účelu, čítání doby pobytu na pracovišti (fungují jako elektronické píchací hodiny), [1]
- sledování a dokumentování pohybu, místa a času osob a zařízení, monitorování stavu objektu, měření návštěvnosti, vytíženosti pracovníků, materiálu (kopírky, výtahy), zvýšení bezpečnosti technologických provozů, využívání pracovní doby, zamezení zbytečného a nepovoleného pohybu po objektu, dodržování technologických přestávek a činnost provozu atd. [1]

Samotné základní funkce přístupových systémů jsou: [2]

- identifikace,
- zpracování dat,
- ovládání přístupového místa,
- programovatelnost,
- stavová hlášení,
- komunikace (s ostatními systémy nebo bloky),
- styk s uživatelem (optické rozhraní / akustické signály),
- napájení (systému nebo přístupového místa),
- samoochrana (ochrana proti sabotáži, neoprávněné manipulaci).

2.1.2 Kombinace systému kontroly vstupu s ostatními systémy

Systémy kontroly vstupu mohou byt samostatně nainstalovány do chráněného objektu, ale častěji se setkáváme z kombinací s dalším poplachovým systémem. V současnosti se můžeme setkat s těmito kombinacemi:

- **Samostatný systém kontroly vstupu,** umožnuje chráněný vstup do objektu po elektronické identifikaci a propustí osobu do objektu na jednom nebo více místech. [1]

- **Kombinace systému kontroly vstupu a docházkového systému,** umožní nejen vstup do objektu, ale i datové údaje pro zaměstnavatele nebo personální oddělení, aby bylo možno kontrolovat vstup a výstup zaměstnanců do zaměstnání, odchod na oběd, k lékaři, soukromý odchod nebo práci o svátcích. [1]
- **Kombinace přístupového systému a systému pro výdej stravy, pracovních pomůcek nebo materiálu,** umožnuje další kombinaci přístupu do zařízení zaměstnavatele nebo odběr stravy nápojů, nářadí a ostatních pracovních pomůcek. [1]
- **Kombinace kontroly vstupu se zařízením EZS,** umožnuje nejen vstup do chráněného objektu oprávněné osobě, ale současně i na trase přístupu nebo v místnostech, kam je dané osobě umožněn přístup odkóduje systém EZS. [1]
- **Kombinace systému kontroly vstupu se zařízením CCTV,** umožnuje nejen použití, kde je nutné kontrolovat pohyb po objektu, ale i sledovat celkovou činnost osoby nebo osob a mít nepřetržitou kontrolu veškerého pohybu po objektu. Používá se například ve věženích, vojenských skladech, letištích, jaderných elektrárnách, chemických závodech a podobně. [1]
- **Kombinace systému kontroly vstupu se zařízením EPS,** je nejčastější a nejednoduší aplikací. Je použita k zajištění automatického otevření únikových vchodů při detekci požáru systému EPS. [1]
- **Kombinace systému kontroly vstupu s informačními technologiemi**, umožnuje využití informačních technologií, které vyžadují přístup k nim. Ne všechny informace je však možno sdělovat každému a kdykoliv. Vzhledem k omezeným možnostem zapamatovat si kódy a hesla se požaduje, aby přístup byl umožněn po schválení vstupu a vydání přístupového média (přihlašování k počítači, do sítí a různých softwarů, aplikacím, elektronický podpis atd.). Vazebními prvky mezi systémem elektronické kontroly vstupu pro fyzickou kontrolu přístupu a prvky řízení přístupu k informacím jsou:

– **Identifikační karty**

  Jedná se o bezkontaktní kartu, která obsahuje bezkontaktní identifikační část. Ta současně obsahuje výkonný bezpečnostní procesor, informace uživatele, jména a hesla, která jsou v tomto případě převážně uschována na ID kartě. [1]

- **Biometrické prvky**

  Otisky prstu, charakteristiky duhovky oka a další biometrické prvky jsou zpracovány pomocí programového modulu, který umožňuje začlenění biometrické čtečky do existujících softwarových aplikací. U tohoto způsobu je zabezpečená informace uložená v informačním systému, chráněna prostředky operačních systémů a šifrováním a k jejímu zpřístupnění dochází po ověření shody mezi uloženým vzorem a nově sejmutým vzorkem biometrického údaje. [1]

2.2 Struktura systémů kontroly vstupu

Systém kontroly vstupu se jako ostatní systémy skládá z více prvků, které dohromady dávají jeden celek. Obecně se skládá z těchto částí: [4]

- identifikačního prvku,
- snímacího zařízení,
- řídící jednotky,
- centrální jednotky,
- blokovacího zařízení,
- jednotky zápisu,
- napájení.

2.2.1 Identifikační prvky

Různých typů identifikačních prvků je v současné době nepřeberné množství. Můžeme je například rozdělit podle styku se snímacím zařízením na kontaktní a bezkontaktní. Nebo podle jejich činnosti či tvaru. Může se jednat například o identifikační kartu, magnetonový proužek, visačku, přívěšek, ale také otisky prstů, oční sítnice a duhovky, hlas a podpis. Je tedy přímo vázán k subjektu identifikace. Subjekt můžeme tedy rozdělit na tří různé způsoby identifikace: [4]

- něco, co subjekt zná a co si pamatuje – heslo, kontrolní otázka,
- něco, co má subjekt fyzicky u sebe – identifikační kartu, přívěšek,
- sám sebou, nebo svými typickými rysy a chováním biometrie.

2.2.1.1 Identifikační prvky vlastnící osoby u sebe

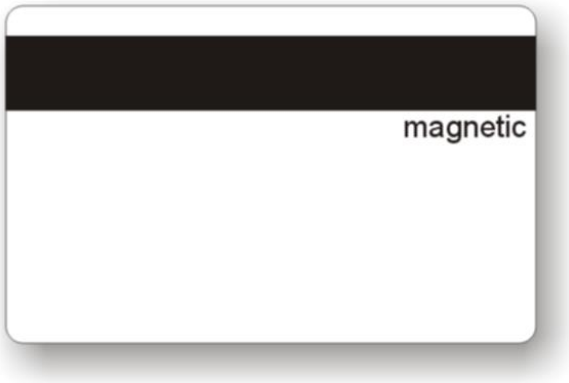
Jde o identifikační prvky, kterými se jednotliví uživatelé prokazují elektronickému systému. Každý tento prvek je přiřazen dané osobě. Obecně se při výběru nosiče informací

v kombinaci se snímacím zařízením přihlíží k určitým aspektům. To je bezpečnost vložené informace, bezpečnost přenosu mezi identifikačním prvkem a snímacím zařízením, spolehlivost identifikace, mechanická trvanlivost nebo opotřebení, kapacita pro případné uložení informace. Podle principu činnosti dále dělíme identifikační prvky na: [4,5]

a) magnetické identifikační karty,
b) optické identifikační prvky s čárovým kódem,
c) indukční identifikační karty,
d) čipové identifikační prvky.

a) Magnetické identifikační karty

Magnetická identifikační karta je plastová destička například kreditní karta, která má svou danou velikost mezinárodními normami, na které je nanesen proužek magnetického nosiče. Informace je zapsána na magnetický proužek pomocí nahrávací hlavy. Zde jsou uloženy všechny údaje včetně oprávnění kam a kdy, může zaměstnanec vstupovat. Zápis informací na magnetický proužek má různé kódování podle použitého systému, ale bývá z pravidla doplněn o čtyřmístný PIN. V současné době jsou již nahrazeny bezpečnějšími systémy, ale nadále se používají v bankovnictví nebo k bezhotovostním platbám. Jejich výhodou je nízká cena, možnost změny záznamu a také možnost na jedné kartě vzájemně sloučit více různých nekompatibilních systémů. Za nevýhody lze považovat jejich snadnou okopírovatelnost, čímž je daná malá bezpečnost, ale i možnost smazání údajů a velká náchylnost na opotřebení. [4,5]



Obr. 1. Magnetická karta. [13]

b) Optické identifikační prvky s čárovým kódem

Čárový kód je řada vertikálních čar o různé tloušťce s mezerami. V současnosti existuje mnoho různých kombinací čar a mezer znázorňující znaky. Princip identifikačních karet s čárovým kódem spočívá v tom, že když přejedeme přes snímací zařízení IR paprskem, černé pruhy se absorbují, zatímco bílé se odrazí. Fotosenzor příjme odražené světlo a převede na elektrický signál, který je slabý pro mezery a silný pro pruhy. Délka elektrického signálu určuje, jaké široké nebo úzké prvky jsou. Signál je dekodérem zapíše do jednotlivých znaků a dekódovaná data se pošlou do počítače. Každý čárový kód se skládá z takzvaného start znaku, zadanou informací, kontrolního součtu a stop znaku. V současnosti se používá více jak padesát druhů čárových kódů. Mezi nejužívanější je 8 nebo 13 místní kód EAN. Čárové kódy jsou buďto nekryté nebo tzv. „maskované“, kdy se jedná buďto o zapouzdřené v PVC folii s ochranou maskovací vrstvou, nebo je nanesen na čárovém kódu maskovací lak, který je propustný přes infračervené světlo speciálních přístrojů. Nevýhodou čárového kódu je, že v současnosti je značné rozšíření a snadná dostupnost ručních infračervených snímačů pro načtení maskovaného čárového kódu. Také je zde riziko vyzrazení číselného ekvivalentu, neboť vlastní provedení čar je zpracováno za pomocí norem, a tak výroba kódové samolepky není problém. [4,5]

c) Indukční identifikační karty

Indukční identifikační karty se tvarově podobají klasickým plastovým identifikačním kartám. Jejich funkčnost pracuje na principu využití elektromagnetické indukce. V plastových kartách je zakódována informace v podobě děrované kovové destičky nebo přesně umístěných vodivých ploch tzv. Wiagendovy karty, popřípadě se zabudovanými rezonančními obvody. Pokud se dostane identifikační prvek do elektromagnetického pole snímače, dochází ke změně homogenity pole přesně stanoveným způsobem. Tyto karty se zasouvají do čtecího otvoru, kde jej lze přečíst čtyřmi různými způsoby zasunutí. Jejich výhodou je zvýšená mechanická pevnost a odolnost proti opotřebení, stabilita záznamu a nesnadná kopírovatelnost. [4,5]

d) Čipové identifikační prvky

Čipové identifikační prvky zaznamenávají informace za pomocí svého paměťového čipu, který bývá z pravidla zalisován do karty, přívěsku, štítku nebo speciálního kovového pouzdra. Identifikační prvek při kontaktu nebo přiblížení se snímačem přečte případně i zapíše informace, dále je pak pošle k dalšímu zpracování. Právě podle způsobu čtení informace se čipové identifikační prvky dělí na dotykové a bezdotykové. [4,5]

- Dotykové čipové identifikační prvky pracují na přímém kontaktu se snímacím zařízením, kde je miniaturní mikročip umístěn na kartě nebo přívěsku. Čipové identifikační karty jsou vyráběny jako obyčejné kreditní karty, jejíž rozměry jsou standardizované po celém světě. Jejich výhodou je vyšší ochrana proti podvodníkům, nižší náklady na provoz. Lze jej také doplnit o magnetický proužek. Další výhodou pro uživatele je možnost grafického potisku například fotografie nebo firemního loga. Nové možnosti přináší i tzv. multifunkční karta, na které lze provádět více aplikací na jedné kartě jako třeba kombinace řidičského a občanského průkazu a zároveň na stejné kartě i elektronickou peněženku a občanský průkaz. Čipové identifikační přívěsky se tvarem podobají mincím, jejich výhodou je, že jsou lehké a dají se nosit na přívěsku pro klíče. Vynikají rovněž odolností vůči vyšším teplotám, jelikož pouzdro bývá vyráběno z nerezové oceli a proto odolává agresivnímu prostředí a nešetrnému zacházení. Jsou řešeny jako dvou-kontaktní prvky se stejným napájením za pomoci snímacího zařízení. [4.5]

- Bezdotykové čipové identifikační karty jsou založeny na principu radiofrekvenční identifikace s nízkofrekvenční, kmitočtově modulovanou technikou přenosu signálu. To znamená, že snímací zařízení reaguje na vzdálenost několika centimetrů až metrů od identifikačního prvku. Hlavními verzemi těchto identifikačních prvků je typ R/O nepřepisovatelný, ale používanější je typ R/W přepisovatelný. Umožnuje ukládat, číst, měnit identifikační kódy a jejich údaje, kde programování se uskutečňuje na dálku danou dosahem snímacího zařízení. Celý tento systém je složen ze tří částí a to identifikačního prvku, antény, snímacího zařízení. Tento systém má nejen výhody pro uživatele, ale také levnější provoz

při vyšším počtu zaměstnanců, kde lze ušetřit na nižším počtu snímačů, protože identifikace je rychlejší. Tyto prvky se u jednotlivých výrobců liší především formou kódování a normou komunikace. Dále je dělíme podle způsobu napájení na aktivní a pasivní. Aktivní identifikační prvky jsou méně používaným typem, jelikož mikrobaterie, jako zdroj pro vysílač a přijímač, je implementován v identifikačním prvku a nutnost měnit baterii, popřípadě celý identifikační prvek, patří mezi nejdražší nevýhody systému. Tyto bezkontaktní identifikační čipové prvky jsou řešeny jako aktivní nízkofrekvenční vysílač, obsahující zákaznický mikročip, který uchovává kódové číslo. Snímač používá vysílače a speciální projektové antény, které vysílají rádiový signál. Identifikační prvek je v nečinnosti dokud se nedostane do aktivního pole antény. Díky využití rádiového signálu nemusí být přímá viditelnost mezi snímačem a identifikačním prvkem. Bezpečnost aktivních identifikačních prvku je zajištěna velkým počtem možných kódů a náročností výroby duplikátu mikročipu. Pasivní identifikační prvky nemají vlastní zdroj a bývají aktivovány za pomoci snímače, který vyšle impulzní nebo nemodulovaný radiofrekvenční signál. Informace je pak zpět poslána modulovaným signálem. Energie pro přenos identifikačního kódového signálu je přijata z elektromagnetického pole, kdy se za pomoci vinutí miniaturní cívky naindukuje dostatečný proud. Podmínkou je dostatečné přiblížení ke snímači. Celkovou výhodou všech aktivních i pasivních čipových identifikačních prvků je nutnost vsunovat či protahovat prvek přes snímací zařízení a tím nedochází k jeho poškození a proto má zvýšenou životnost, není nutná pravidelná údržba snímačů jako u magnetických karet, jsou obtížně padělatelné a kód je udáván převážně u výrobce. Obal je pevný a nelze jej většinou modifikovat. Jelikož pracují v rádiovém spektru a vykazují větší dosah, je možná lokální kontrola pohybu nositele v objektu skrytými snímači, bez vědomí a proti vůli nositele. Využití těchto prvků je různorodé, ale z pravidla je použita na identifikaci osob nebo pohyblivých objektů, jako jsou dopravní prostředky nebo materiál a zboží. [4,5]

Obr. 2. Dotykové a bezdotykové identifikační karty. [14]

2.2.1.2 Identifikační prvky, které si osoba pamatuje

Identifikační prvek si oprávněná osoba zapamatuje a kódovou informaci nosí v paměti. Při vstupu do objektu ji za pomoci kódové klávesnice zadá do vstupního systému. Elektronika porovná oprávněnost vstupního kódu a při správnosti hesla odblokuje přístupové zábrany, jako například dveřní zámky nebo závory apod. Je popřípadě schopna uložit získaný údaj do snímacího zařízení či počítačové databáze. Kódovou informaci lze rozdělit do dvou skupin: [4,5]

a) **Kódová informace je přidělena skupině lidí**, kteří mají oprávněný přístup do prostor objektu. Může jít o zaměstnance jednoho pracoviště, obyvatele domu, apod. Nevýhodou je, že nelze zpětně provést kontrolu, kdy který zaměstnanec vstoupil nebo odešel z objektu. [4,5]
b) **Každá oprávněná osoba má přidělen PIN kód,** díky němu lze zpětně zjistit na základě archivace údajů příchod a odchod jednotlivých pracovníků. Rozeznávají se dva druhy zadávání PIN kódu, a to že PIN kód nastaví operátor řídícího pracoviště nebo PIN kód zná pouze oprávněná osoba, která jej zadá pomocí numerické klávesnice z kontrolního místa. [4,5]

Výhodou tohoto systému je, že kód nelze ztratit, jde snadno měnit a přidělovat telefonicky nebo písemně. Nevýhodou je, že kódová informace je obtížná na zapamatování, neidentifikuje nositele, vyžaduje ruční zadání a lze ji někomu sdělit úmyslně nebo vynutit pod nátlakem. [4,5]

2.2.1.3 Identifikační prvky obsahující biometrické rysy

Snímače biometrických rysů oprávněné osoby jsou jedny z nejmladších identifikačních systémů. Jako rozpoznávací znaky se využívají různé části lidského těla. Díky tomu není třeba pro identifikaci nosit externí identifikační prvek, což je velkou výhodou. Rozpoznávací znaky jsou jedinečné, proto je biometrická identifikace jedna z nejbezpečnějších. Na druhé straně potřebuje složitější snímací zařízení, které musí biometrický znak přečíst a porovnat s databází. Porovnávaná data jsou často velká a zpomalují někdy odezvu celého systému, proto se používají v kombinaci s ostatními identifikacemi z důvodu rychlejší odezvy. Identifikace funguje na principu, že se použije předem definovaný obraz biometrického znaku a při vyhodnocení dochází pouze k porovnání naskenovaného a uloženého znaku. Moderní snímací zařízení provádějí verifikaci a identifikaci určitých biometrických znaků jako například otisky prstů, geometrie ruky, žilového řečiště hřbetu ruky, oční sítnice a duhovky, vizuálního rozpoznání obličeje, analýzy lidského hlasu, dynamiky podpisu, DNA apod. [4]

a) Otisků prstů

Identifikace podle otisku prstu je jednou z nejstarších, neznámějších a nejvíc rozšířených biometrických metod. Patří do skupiny daktyloskopických identifikací, což je nauka o obrazech papilárních linií na vnitřní straně článků prstů a dlaní člověka. Na světě nenajdeme dva jedince se stejnými obrazci papilárních linií. Jsou po celý život relativně neměnné a obrazce jsou neodstranitelné. Metody zachycení otisku prstu jsou buď klasické získání otisku pomocí papíru a inkoustu nebo statické snímání, které je nejčastěji použité v systémech kontroly vstupu. Jsou založeny na elektronickém interaktivním snímání a jsou často začleněny do nejrůznějších technologických zařízení pomocí senzorů, které využívají různých fyzikálních principů. Základní rozdělení těchto senzorů jsou kontaktní a bezkontaktní. Kontaktní senzory pracují na mnoha fyzikálních principech, jako například senzory optické, elektronické, optoelektronické, kapacitní, tlakové a teplotní. Nejrozšířenější jsou ale snímače optické a kapacitní. Optické fungují na principu, že laserový paprsek zespodu osvětluje povrch prstu, který se dotýká průhledné desky a množství odraženého světla závisí na hloubce papilárních linii a brázd. Kapacitní senzor zase funguje tak, že měří elektrickou kapacitu. Senzor je složen z velkého počtu vodivých plošek, které jsou vzájemně odizolovány. Dotykem prstu papilární linie přemostí jednotlivé vodivé plošky v závislosti na jejich tvaru, zatímco brázdy slouží

jako izolanty. Měří se napětí a kapacita mezi vodivými ploškami. U bezkontaktních senzorů patří mezi nejznámější senzory optické a ultrazvukové. U optických senzorů je princip stejný jako u dotykových, kdy světelný paprsek umožnuje snímat otisk na vzdálenost několika milimetrů. Ultrazvukové senzory pracují podobně jako optické. Vysláním zvukových vln s vysokou frekvencí (generovaných zdrojem) směrem k snímané ploše je pak vyhodnoceno odražení zvukové vlny přijímačem. Nevýhodou těchto senzorů je, že na povrchu muže zůstat náš daktyloskopický otisk nebo zůstane pot a nečistoty na prstu či snímacím zařízení a dojde ke špatnému vyhodnocení. [4,5]

Obr. 3. Čtečka otisků prstu. [15]

b) Geometrie ruky

Základní princip vychází z toho, že se od určitého věku nemění specifický tvar ruky člověka. Při identifikaci se měří výška a šířka prstů, ale taky při optickém snímání můžeme získat binární obraz a detekci hran objektu. Funkce snímače spočívá v tom, že do prostoru vymezeného speciálními kolíky vložíme ruku. Systém identifikuje správnou polohu ruky a digitální kamera snímá trojrozměrný odraz dlaně ruky a zjišťuje míry všech prstů. Výsledné údaje se porovnají se záznamem v paměti. Snímač lze aplikovat jak pro fyzickou kontrolu vstupu například v laboratořích, vojenských a jaderných zařízeních, tak pro identifikaci osob jako například přístup k zabezpečeným schránkám bank a elektronickému podpisu. [4,5]

Obr. 4. Čtečka geometrie ruky. [16]

c) Oční sítnice a duhovka

Snímače oční sítnice je velmi přesný biometrický prostředek identifikace. Oční sítnice není viditelný lidský zrakový orgán a k jeho zviditelnění se používají koherentní infračervené světelné zdroje, jejichž cévami je sítnice rychleji absorbována než v ostatních tkáních. Abychom získali odraz prokrvení sítnice, musí daná osoba z krátké vzdálenosti zaostřit na pomocný bod ve čtečce. Slabý záblesk světelného zdroje ultranízké intenzity je pak oční čočkou soustředěn na sítnici a odráží se od ní zpět přes oční čočku do čtečky. Při snímání nevadí kontaktní čočky, ale brýle se musí sejmout. Při použití dvojité čtečky je pravděpodobnost chybného přijmutí minimální. Snímače oční duhovky jsou založeny na principu, že duhovka, což je barevná část lidského oka kolem panenky, má jedinečné informace zakódované v sobě a jsou stabilizovány během prvního roku života a dále se nemění. Duhovka se skládá z náhodně rozmístěných barevných struktur podobným sněhovým vločkám, které jsou dány kombinací specifických anatomických charakteristik. Každá osoba má svou individuální duhovku, která se liší levá od pravé. Při snímání oční duhovky není potřeba žádný fyzický kontakt s optickou jednotkou, stačí pouze standartní videokamera. Nevadí kontaktní čočky ani brýle, protože fotografii a skleněné oko rozpozná, neboť průměr duhovky se neustále částečně mění. [4,5]

d) Vizuálního rozpoznání obličeje

Identifikace osoby na základě rozpoznání obličeje má ve srovnání s metodou otisků prstů nižší identifikační jednoznačnost, ale tato metoda umožňuje bezkontaktní

snímání na poměrně velkou vzdálenost. Identifikace osoby podle její tváře můžeme rozdělit na dvě základní etapy. V první etapě probíhá detekce a lokalizace tváře za pomoci kamery. Scénou může být fotografie nebo reálná situace. Rozpoznání, že se na scéně jedná o lidskou tvář, je velmi složitý identifikační proces. Detekce a lokalizace tváře záleží na typu scény a množství jiných osob, různorodém pozadí i na vzdálenosti od objektivu. Mění se i vizáž samotných tváří, na nichž se promítají i emoce. Ve druhé etapě probíhá automatické nalezení základních identifikačních charakteristik a samotná identifikace tváře známé již z minulosti. V současnosti je velké množství nejrůznějších metod a algoritmů pro počítačové rozpoznání obličeje. To převážně závisí na odlišných klasifikačních kritériích. Lze je například rozlišovat podle toho, jestli se jedná o dvourozměrné nebo třírozměrné obrazy, černobílé a barevné obrazy. Nebo v závislosti na způsobu snímání obrazu rozlišujeme čelní pohledy, pohledy z boku, obecné pohledy a jejich různé kombinace. Z časového hlediska je možné rozpoznávat statické nebo dynamické obrazy. Spektrum využití metody rozpoznání obličeje je velmi široké. Jedná se o zajištění nejrůznějších objektů jako například banky, peněžní ústavy, ale také pro policejní účely, kdy je v současnosti velmi rozšířen monitorovací kamerový systém. [4]

2.2.2 Snímací zařízení

Snímací zařízení neboli čtečky jsou nedílnou součástí systémů kontroly vstupu. Snímací zařízení můžeme dělit podle identifikačního média, jak bylo naznačeno v předchozích stránkách, tak i podle hlediska vykonávaných funkcí, které dělíme na 3 základní skupiny. [2,6]

1) **Základní čtečky**

   Zajistí pouze zadání kódu nebo přečtení identifikátoru a následné poskytnutí těchto údajů nadřazené řídící jednotce. Nemají magnetický kontakt ani vstup pro dveřní kontakt ani tísňové tlačítko. U biometrických čteček jde pouze o předání informace o čísle uživatele. Tyto čtečky se nejčastěji používají u rozsáhlejších systémů. [2,6]

2) **Polointeligentní čtečky**

   Mají vstupy pro dveřní kontakt, tísňové tlačítko, také výstup pro ovládání zámku na dveřích, avšak neprovádí samy vlastní rozhodnutí o přístupu. Je zaslána žádost

hlavní řídící jednotce a čeká se na odezvu. Nejčastěji se k připojení používá sběrnice RS-485. Při kladném potvrzení provede polointeligentní čtečka otevření dveří. [2,6]

3) **Inteligentní čtečky**

   Mají všechny potřebné vstupy a výstupy pro ovládání místa přístupu. Obsahují i vlastní paměť, kde jsou uchovány přístupové údaje. Díky tomu provádějí rozhodnutí o přístupu samostatně a nezávisle. K hlavní řídící jednotce bývají připojeny pomocí sběrnice RS-485. Řídící jednotka v tomto případě pouze zajišťuje aktualizaci přístupových práv ve čtečkách a přijímá od čteček informace o transakci. [2,6]

Čtečky karet můžeme rozdělit podle technologického řešení, kde jdou nejčastěji požívané čtečky RFID, magnetických karet, Wiegand a biometrické čtečky. Samotný výběr čteček nepodléhá tomu na jakou třídu identifikace nebo stupeň zabezpečení je systém kontroly vstupu projektován. Jelikož jsou požadavky na zabezpečení v současnosti poměrně vysoké, využívá se různá kombinace dvou přístupů. Převážně se nezohledňuje do jaké třídy přístupu nebo stupně zabezpečení je systém projektován, ale cílem je posílit nejvíce ohrožená místa, kde hrozí riziko neoprávněného přístupu. Nejčastěji se ale využívá kombinace RFID + klávesnice nebo RFID + otisky prstů. [2,6]

2.2.3 Řídící jednotka

Řídící jednotka je výkonný prvek vstupního systému. Přebírá elektronické signály generované snímači a z uložených informací v paměti rozhoduje o uvolnění nebo naopak zablokování hlídaného vstupu. Moderní řídící jednotky jsou ovládány mikroprocesorem a díky paměťové výbavě disponují schopností zcela samostatně rozhodovat o vstupu nebo vyhodnocovat reálné podněty jako stav dveří, poplachové vstupy. Řídící jednotka je srdcem systému, ovlivňuje celkovou konfiguraci, prověřuje oprávněnost vstupů, aktivuje ovládací prvky, sleduje narušení systému, zaznamenává veškeré identifikace apod. [4]

2.2.4 Centrální jednotka

Centrální jednotka monitoruje a řídí celý systém, provádí jeho obsluhu a programování. Jedná se počítač se specializovaným softwarem, který zajišťuje centrální správu personálních, řídících a ostatních systémových dat mezi PC a řídící jednotkou. Hlavním úkolem je tedy sběr dat z řídících jednotek, jejich vyhodnocení a rychlá reakce v reálném čase. Vyhodnocení těchto údajů je velmi variabilní a dá se filtrovat podle různých kritérií jako například jen pro určitý vstup, osobu či událost. Software by měl být také uživatelsky snadno ovladatelný, lokalizovatelný pro danou národnost apod. [4]

2.2.5 Blokovací zařízení

Jsou další důležitou součástí systémů kontroly vstupu. Realizují fyzické zablokování nebo uvolnění hlídaného vstupu. Mezi nejpoužívanější prvky patří:

- **Elektromagnety –** Používají se k držení dveří v uzavřeném stavu. Jsou velmi spolehlivé a bezúdržbové. [2]
- **Elektromagnetické otvírače –** Nainstalují se do rámu dveří. Princip spočívá v tom, že na závislosti přivedeného napětí se odblokuje nebo zablokuje západka dveří. [2]
- **Elektromechanické/elektromotorické zámky –** Jedná se převážně o samozamykací zámky, kde střelka pozná dovření dveří a následně mechanicky nebo motoricky vysune západku. Instalují se do dveří, zatímco protiplech je v zárubni. [2]
- **Elektromotorické/elektrohydraulické otvírače –** Slouží k automatickému otevírání a zavírání různých typů dveří. Nejčastější využití u bezbariérového vstupu.
- **Motory –** Různé typy motorů k ovládání vrat, závor, turniketů apod. [2]

Použití konkrétního provedení zámku pro daný vstup se zálohováním přístupového systému a s požárními požadavky. Při návrhu je potřeba zajistit, aby během výpadku napájení nedošlo k samovolné změně stavu dveří, turniketů apod. Téměř všechna blokovací zařízení se prodávají v různých variantách jako např. jednostranné, oboustranné, běžné a požární, se zvýšenou robustností, signalizační činností, apod. [2]

3 NORMY V SYSTÉMECH KONTROLY VSTUPU

3.1 Normy v průmyslu komerční bezpečnosti

Jako v jiných oborech, tak i v průmyslu komerční bezpečnosti je většina služeb, výrobků, vlastností použitých komponentů apod. vyspecifikována v normách, které v České republice zajišťuje Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Obecně lze říct, že norma je dokument, poskytující obecné a opakované pravidla, směrnice, požadavky, limity nebo charakteristiky činností nebo jejich výsledků zaměřené na dosažení optimálního stupně uspořádání ve vymezených souvislostech. Normy jsou doporučení, nikoliv příkazy, takže jejich používání je dobrovolné. Povinnost dodržovat požadavky v normách může ale vyplývat z jiných právních aktů jako například právní předpis, smlouvy, pokyn nadřízeného nebo rozhodnutí správního orgánu. [7,8]

Normy pro systémy kontroly vstupu se nacházejí v řadě norem pod názvem ČSN EN 50 130, kde jsou uvedeny všeobecné požadavky pro poplachové systémy. Základní rozdělení je:

- ČSN EN 50131 Poplachové systémy – Elektronické zabezpečovací systémy
- ČSN EN 50132 Poplachové systémy – Systém CCTV
- ČSN EN 50133 Poplachové systémy – Systém kontroly vstupu
- ČSN EN 50134 Poplachové systémy – Systém přivolání pomoci
- ČSN EN 50135 Poplachové systémy – Systémy tísňové
- ČSN EN 50136 Poplachové systémy – Systémy přenosové
- ČSN EN 50137 Poplachové systémy – Systémy přenosové a kombinované [7]

Další číslování norem určuje konkrétní požadavky nebo pravidla a dělí se do sedmi částí, které jsou:

- ČSN EN 5013x -1 Systémové požadavky
- ČSN EN 5013x -2-4 Požadavky na jednotlivé části systému
- ČSN EN 5013x -5 Komunikace, propojení
- ČSN EN 5013x -6 Napájení
- ČSN EN 5013x -7 Pokyny pro aplikace [7]

Nejdůležitější normy v systémech kontroly vstupu tedy jsou:

- ČSN EN 50133-1 Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky
- ČSN EN 50133-2-1 Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 2-1: Všeobecné požadavky na komponenty
- ČSN EN 50133-7 Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace [7]

3.2 ČSN EN 50133-1

Norma nese název „Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky“. Tato norma definuje požadavky na automatizované systémy kontroly vstupů a komponenty uvnitř a vně budovy. Zahrnuje také systémovou architekturu a všeobecné požadavky, funkční požadavky, definice podmínek okolního prostředí a elektromagnetické kompatibility, komunikaci kontroly vstupu s ostatními systémy. [9]

a) Definice

V této části normy, jsou vypsána základní slova, s kterými se budeme dále v normě setkávat, jako například co je to přístup, systém kontroly vstupu, jednotka řízení vstupu, místo přístupu, úroveň přístupu, výstraha, apod. [9]

b) Základní funkce systémů kontroly vstupu

Zde je vypsáno základních devět funkcí, které jsou: Zpracování, napájení, samoochrana, programování, ovládání místa přístupu, identifikace, zobrazování uživateli, hlášení, komunikace s ostatními systémy. [9]

c) Klasifikace zabezpečení

Zabezpečení systému kontroly vstupu je založeno na čtyřech třídách identifikace a dvou třídách přístupu. Třídy identifikace jsou:

- **Třída identifikace 0** – žádná přímá identifikace. Založena na prostém požadavku o přístup bez identity uživatele. [9]

- **Třída identifikace 1** – informace uložena v paměti. Založena na heslech a osobních identifikačních číslech, atd. [9]
- **Třída identifikace 2** – identifikační prvek nebo biometrie. Založen na použití identifikačních prvků, karet, fyzických klíčů, atd. [9]
- **Třída identifikace 3** - identifikační prvek nebo biometrie spolu s informací uloženou v paměti. Založena na použití kombinace identifikačního prvku, biometrie, informace uležené v paměti. [9]

Třídy přístupů jsou:

- **Třída přístupu A**: Tato třída platí pro místo přístupu, ve kterém požadovaný stupeň zabezpečení nevyžaduje ani časový filtr ani ukládání přístupové transakce. [9]

a) **Třída přístupu B:** Tato třída platí pro místo přístupu, které zahrnuje časové filtry a funkce ukládání. Zahrnuje také podtřídu, která se vztahuje na místo přístupu zahrnující časové filtry, ale bez funkcí ukládání dat. [9]

d) Funkční požadavky pro třídu A a B

V této části jsou podle základních funkcí kontroly vstupu vypsány určité požadavky podle třídy identifikace. Například jsou různé požadavky pro zpracování pro třídu identifikace 3 než pro třídu identifikace 1. U některých funkcí jsou speciálně napsány doplňkové požadavky pro třídu přístupu B. [9]

e) Požadavky na komponenty kontroly vstupů

V této části normy jsou sepsány požadavky, které musí daný výrobek splňovat, aby mohl projít danými zkouškami. Například na vliv prostředí, teplo a chlad vniknutí vody, vibrace, změny síťového napětí, apod. [9]

f) Značení a identifikace

Všechny komponenty systémů kontroly vstupu musí být označeny. Na štítku musí být minimálně uvedeny informace o jméně organizace odpovědné za shodu výrobku, typ výrobku, údaje výrobce, veškerá označení, která požadují další normy a předpisy. [9]

V současné době platí i nová norma ČSN EN 60839-11-1 s názvem „ Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty“. Tato norma souběžně platí s normou ČSN EN 50133-1. Od 11. 6. 2016 norma ČSN EN 60839-11-1 nahrazuje normu ČSN EN 50133-1, která tímto datem pozbývá platnosti. Tato norma do značné míry rozšiřuje všechny body z normy ČSN EN 50133-1 jako například nové definice, zvýšil se rozsah a podrobnosti zpracování funkčních požadavků, které jsou klasifikovány podle úrovně rizika oproti předchozímu založení na třídách identifikace a třídách přístupu. [12]

3.3 ČSN EN 50132-2-1

Norma nese název „Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 2-1: Všeobecné požadavky na komponenty“. Tato norma převážnou část svých bodů přejímá a odkazuje na normu ČSN EN 50133-1. Jsou zde uvedeny pokyny, které má výrobce uvést v dokumentaci o výrobku. Dále jsou zde uvedeny specifické požadavky pro rozhraní místa přístupu a identifikační zařízení. [10]

3.4 ČSN EN 50133-7

Norma nese název „Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace“. Tato norma zahrnuje pokyny pro návrh systému, instalaci, předání, provoz a údržbu systémů kontroly vstupu. [11]

a) Definice

Pro účely této normy platí definice uvedené v ČSN EN 50133-1, ale i definice nové jako například co znamená kontrola přítomností, přístupová místa degradovaný režim, apod. [11]

b) Všeobecné podmínky

Zde je určeno, že systém kontroly vstupu zahrnuje všechny konstrukční a organizační náležitosti společně se zařízením požadovaným k ovládání vstupů. Dále také, že zavedení systému kontroly vstupu se skládá z pěti bodů. Projektem (návrh) systému, instalací systému, předání systému, provoz a údržbou systému. [11]

c) Návrh systému

Požadavky na návrh se konzultují s kupujícím a dalšími zainteresovanými stranami. Po získání informací od zákazníka a na základě výsledku analýzy rizik se bere v úvahu pro každé přístupové místo několik věcí. Jedná se například o vztah k ostatním systémům, klasifikace zabezpečení, vstupu a výstupu, četnost průchodu uživatelů, požadavky na hlášení, apod. [11]

d) Instalace

Jsou zde uvedeny všeobecné podmínky, ale i podmínky pro zařízení, napájecí zdroj, kabeláž a revizi. Jedna ze základních podmínek je, že zařízení se má instalovat podle pokynů výrobce. Při výběru místa instalace se zohledňuje přístupnost a snadnost používání. Kabelové trasy se mají volit tak, aby představovali nejkratší vzdálenost mezi zařízeními. Cílem revize je potvrdit, že vyhovuje požadavkům návrhu systému. [11]

e) Předání, provoz a údržba

Zde je určeno, že po předání od projektové a instalační firmy, je odpovědný za provoz kupující. Správce pak zajišťuje školení seznámení a poskytnutí písemných instrukcí uživatelům, aktualizaci databáze, apod. K zajištění správné funkce systému se mají provádět v dohodnutých intervalech údržba, prověrky, prohlídky a servis. Měla by být prováděna inspekční a servisní organizací. [11]

f) Dokumentace

Zde je stanoveno, že dokumentace je prováděna v jazyce odsouhlaseném kupujícím a má být přizpůsobena rozsahu a složitosti instalovaného systému. Provádějící projektant má jasně stanovovat zabezpečovaný a kontrolovaný prostor, umístění identifikačních a ovládacích zařízení, klasifikaci každého přístupového místa. Dokumentace pro revizi má obsahovat návod k obsluze, popis instalovaného systému, umístění zařízení, příslušné kabelové trasy, podrobné výkresy propojení. [11]

3.5 ČSN CLC/TS 50398

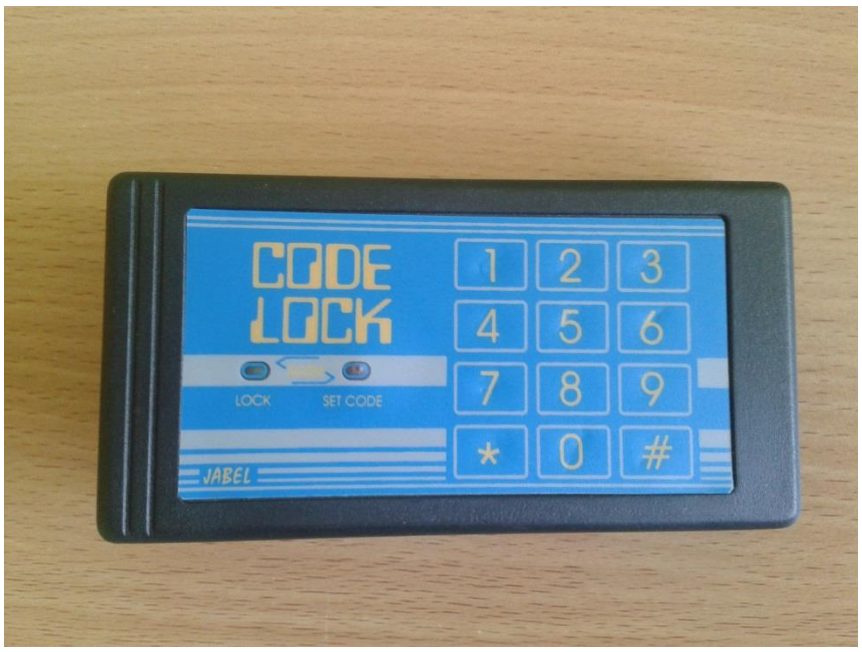
Norma nese název „Poplachové systémy – Kombinované a integrované systémy - všeobecné požadavky“. Jedná se v současné době o jedinou technickou normu, která řeší propojení poplachových a nepoplachových aplikací. Za poplachové systémy jsou v normě zařazeny všechny poplachové systémy a dále rovněž systémy elektrické požární signalizace a poplachové systémy výtahů. Za nepoplachové systémy považuje například norma osvětlení, vytápění, klimatizaci, ventilaci, zavlažování, vysoušení, správu budov, dopravní aplikace, atd. Norma následně řeší definici základních pojmů, popis základních konfigurací integrovaných poplachových systémů, systémové požadavky, dokumentace a školení, použití, montáž a spolehlivost integrovaných poplachových systémů. [17]

II. PRAKTICKÁ ČÁST

4 ELEKTRONICKÉ STAVEBNICE

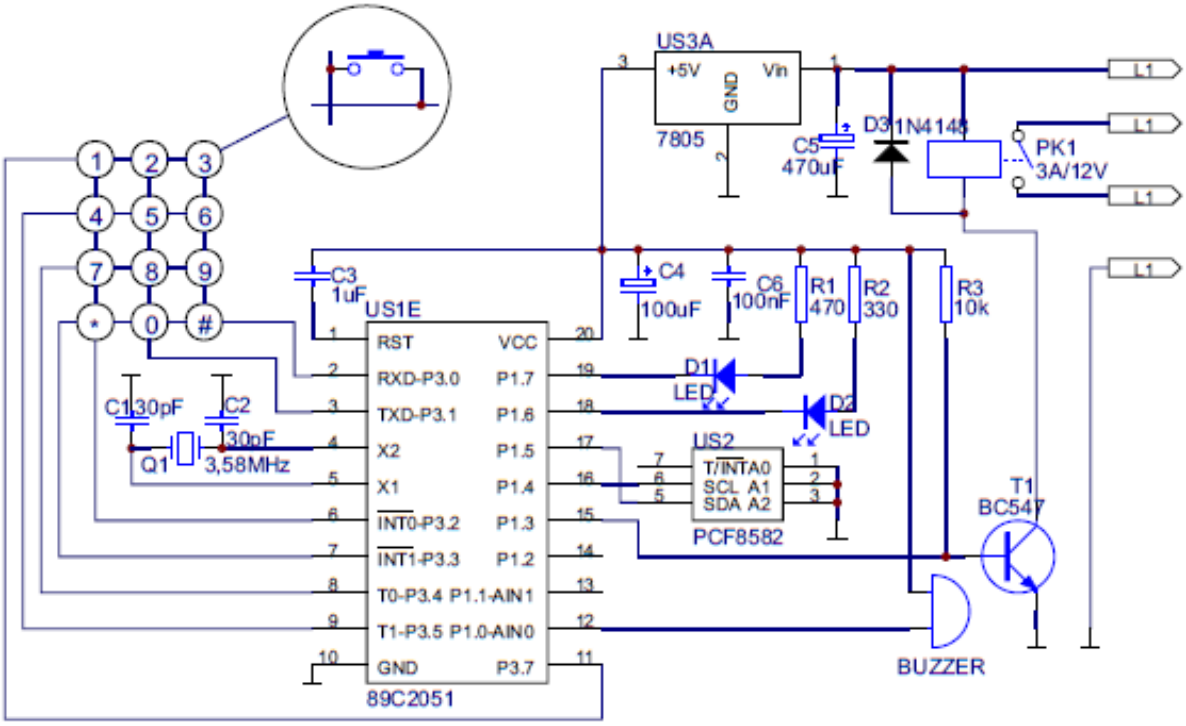
V současné době se lze setkat s celou řadou elektronických stavebnic, které jsou určeny jak pro děti, tak pro dospělé, kteří se rádi zabývají elektronikou. Elektronické stavebnice můžeme rozdělit na dvě základní provedení, jedny jsou tzv. výukové stavebnice a druhé jsou tzv. stavebnice elektronických modulů. Výukové stavebnice lze chápat jako soustavu elektronických prvků, které jsou určeny k jednorázovému nebo opakovanému sestavování různého počtu obvodů, jež jsou určeny svými technickými parametry. Tyto stavebnice jsou převážně určeny k výuce elektrotechniky nebo fyziky na základních nebo středních školách. Dále také dětem, které nemají žádné nebo jen částečné zkušenosti v oblasti elektroniky. Stavebnice elektronických modulů oproti výukové je složena z plošného spoje a součástek pro osazení. Tyto stavebnice jsou určeny pro sestavení a oživení dle dodávaného návodu. Jsou určeny pro dospělé, kteří mají vyšší zkušenosti v oblasti elektroniky. Zde je zapotřebí mít určité technické vybavení jako například pájku, cín, voltmetr, apod. Stavebnice se vyrábí v různých provedeních, kde se jedná například o dálkové ovládání, regulátory, měřiče, různé druhy zabezpečovací a akustické techniky.

4.1 Kódový zámek J – 205



Obr. 5. Kódový zámek J-205.

Tato elektronická stavebnice je vyráběna polskou firmou Jabel, která navrhuje a vyrábí elektronické zařízení již 20 let. Tento výrobek se na trhu České republiky prodává za cenu okolo 700 Kč. Jedná se tedy o stavebnici elektronického kódového zámku, který je převážně určen k ovládání jednoho elektronického dveřního zámku. Celá stavebnice je umístěna v plastikové skřínce se stupněm krytí IP42 o rozměrech 128x67x29 mm. Umožnuje tedy umístění zařízení poblíž zamknutých dveří, kde nehrozí mechanické poškození. Srdcem obvodu je jednokanálový mikroprocesor AT89C2051 s vnitřní pamětí typu FLASCH. V něm nahraný program obsluhuje klávesnici a ovládá vnější zařízení (relé, LED a piezoelement). K mikroprocesoru je připojena také paměť EPROM uchovávající zapsané kódy po dobu výpadku napájecího napětí. Zámek umožnuje použít pouze jeden dvanáctimístný numerický kód. Celá klávesnice je napájena externím napětím o velikosti 12V/100mA. [18]



Obr. 6 Schématické zapojení J-205. [19]

4.1.1 Kompletace výrobku

4.1.1.1 Pájení

Pájení je metoda spojování součástí roztaveným pomocným materiálem, tzv. pájkou s nižší teplotou tavení než mají spojované součásti, které se při tom neroztaví. Rozlišujeme dva druhy pájení tzv. měkké a tvrdé, které závisí na teplotě tavení pájky. Měkké pájení se provádí do teploty 450°C. Nad touto teplotou se jedná už o pájení tvrdé. Metody pájení rozlišujeme podle způsobu ohřevu pájených součástí a pájky na lokální nebo celoobjemové. Lokální ohřev při měkkém pájení se uskutečňuje dotekem horkého tělíska, které je součástí tzv. páječky. Nejčastěji je ohříváno elektricky, např. přímým průchodem elektrického proudu u tzv. transformátorové páječky, nebo nepřímo elektrickým topným tělesem. Při samotném pájení se kovové součástky nejdříve páječkou zahřejí a přidáním roztavené pájky se spojí. Pájka vytvoří po vychladnutí pevné mechanické a elektrické spojení. [20]

4.1.1.2 Seznam použitých součástek

Tab. č. 1. Seznam součástek J-205. [19]

Označení	Název a velikost součástky	Označení	Název a velikost součástky
US1	AT89C2051	R3	10kΩ
US2	PCF8582	C1, C2	30pF
US3	78L05	C3	1µF
T1	BC547	C4	100µF
D1	LED 3mm červená	C5	470µF
D2	LED 3mm zelená	C6	100nF
D3	1N4148	-	Relé 12V/3A
Q1	Krystal 3,58Mhz	-	Patice DIL 8 a 20
S1-S12	Tlačítka 4mm	-	Piezoelement 12 mm
R1	470Ω	-	Krabička Z34
R2	360Ω	-	Deska tištěných spojů

4.1.1.3 Postup kompletace výrobku

Před začátkem osazení výrobku jsem nejprve zkontroloval podle přiloženého návodu, zda byly dodány všechny komponenty potřebné pro kompletaci. Po kontrole jsem si připravil veškeré nástroje, které budu potřebovat. Při pájení plošných spojů je nejlepší použít mikropájku, protože při použití transformátorové pájky může dojít k poškození citlivějších součástek, například mikroprocesoru. Dále jsem používal k pájení cín a kalafunu, aby mohlo dojít k mechanickému spojení mezi plošným spojem a součástkou. Pro zjištění správné velikosti a označení vývodů součástek jsem použil multimetr a PC. Multimetr k zjištění velikosti rezistorů a kondenzátorů a pomocí PC jsem na internetu dohledal označení vývodů u složitějších součástek. Před úplným začátkem bylo třeba zkontrolovat desku tištěných spojů, zda jsou vyvrtány všechny otvory, jestli se vejdou do krabičky a zda jsou všechny vodivé cesty shodné se schématickým zapojením uvedeným v návodu. Po kontrole a přípravě všech nástrojů jsem přešel k vlastní kompletaci. Na plošný spoj jsem nejprve připájel svorku mezi dvěma vodivými cestami na plošném spoji, kde jsem použil jakýkoliv měděný drát o malém průměru. Dále jsem připájel dvě patice DIL 8 a 20, na které jsem pak po úplné kompletaci dosadil mikroprocesor a paměť EPROM. Posléze jsem přešel k napájení všech rezistorů R1 až R3 a pokračoval k napájení kondenzátorů C1 až C6. U kondenzátoru C4 a C5 bylo potřeba dávat pozor na správné umístění podle polarity, jelikož se jedná o elektrolytické kondenzátory. Po připájení kondenzátorů jsem připájel tranzistor T1 a stabilizátor US3. Zde je třeba dbát na přesné umístění jejich nožiček. Poté jsem pokračoval diodou D3 a keramickým rezonátorem Q1. A posléze připájení piezoelementu a relé. Ze strany tištěných spojů bylo potřeba ještě připájet tlačítka S1 až S12 a diody D1 a D2. U diod jsem si dával pozor na to, aby byly zapojeny správným směrem, tedy aby vývody katody a anody byly umístěny podle schématického zapojení a u tlačítek jsem se zaměřil na správné usazení všech vývodů, aby nedošlo k mechanickému propojení a zkratu. Dbal jsem také o výšku všech tlačítek a diod, aby mohly být přesně umístěny do krabičky. Na koncové vývody pro napájení a relé je možno připájet svorkovnice, abychom mohli posléze přišroubovat drátové propojení, nebo jako v mém případě, je možné připájet dráty přímo k tištěnému spoji. Na konec jsem na připájené patice umístil mikroprocesor a paměť US1 a US2. Zde jsem se zaměřil na to, aby byly umístěny správným směrem a nedošlo k záměně vývodů. Osazený tištěný spoj jsem přišrouboval k přední části krabičky čtyřmi šroubky, aby nedocházelo k prohýbání plošného spoje při stisku tlačítek.

4.1.2 Oživení a otestování všech možností výrobku

Po úplné kompletaci výrobku jsem provedl poslední kontrolu správnosti osazení před zapojením napájecího napětí. Výrobek jsem nejprve připojil k elektronickému zámku a posléze k nastavitelnému zdroji stejnosměrného napětí. Elektronický zámek je přímo napájen z výrobku. Napětí jsem nenastavil přímo 12 V, ale jen polovinu a postupně jsem přidával na požadované napětí. Zda výrobek funguje, jsem ověřil tím, že při stlačení jakéhokoliv tlačítka zazněl krátký tón z piezoelementu.

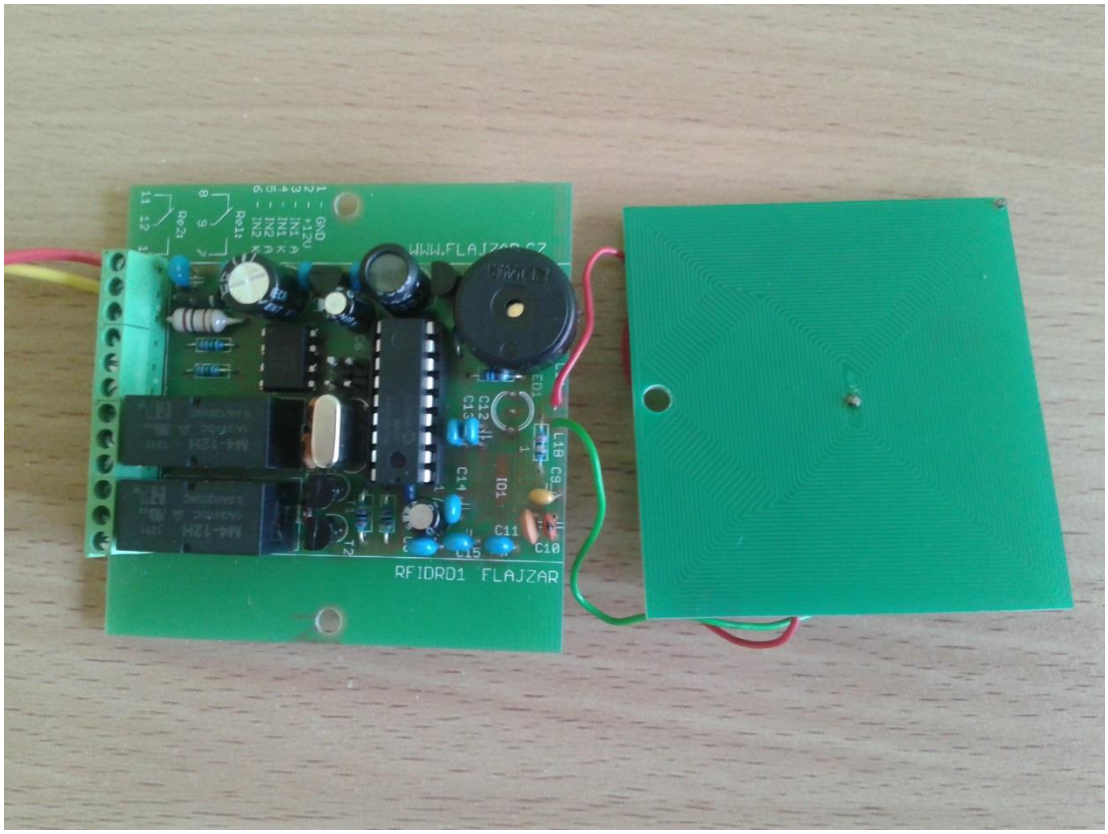
Po oživení jsem přešel k samotnému programování výrobku, které jsem provedl pomocí numerické klávesnice. Nejprve bylo potřeba naprogramovat kód pro otevření zámku. Jako první jsem stlačil na klávesnici tlačítko [0], které mně umožnilo samotné programování. Posléze tlačítko [#]. Zároveň začala blikat červená dioda D1. Nyní jsem mohl zadat vybraný kód o maximální délce 12 číslic. Pokud bych zadal delší kód, zazněl by dlouhý tón z piezoelementu a zhasla dioda D1 a musel bych programovat znovu. To se naštěstí nestalo. Po zadání zvoleného kódu (1, 4, 7) a potvrzení konce programování stlačením [#] zároveň zhasla dioda D1. Pokud bych chtěl změnit kód, musel bych napsat nejprve původní kód. Posléze zmáčknout [#] a zároveň by začala blikat dioda D1. Napsal jsem nový kód (1,2,3,4,5,6) zase zmáčknul [#], zhasla dioda D1 a nový kód byl naprogramován. Pokud by došlo ke ztrátě nebo zapomenutí kódu je zde možnost po demontáži zkratovat se zemí vývod č. 14 u mikroprocesoru a na několik sekund odpojit od zdroje. Dojde k vynulování paměti a je možno znovu naprogramovat nový kód.

Pro samotné otevření zámku jsem nejprve napsal zvolený kód a stlačil tlačítko [*]. Tím došlo k sepnutí relé, které je signalizováno rozsvícením zelené diody D2. Podle přiložené dokumentace je relé sepnuto asi 2 sekundy. Podle mého měření je průměrná doba 3 sekundy. Čas bohužel nelze nijak nastavovat. Po špatně zadaném kódu dojde k signalizaci pomocí dlouhého tónu z piezoelementu. Jak jsem měl možnost vyzkoušet, pokud dojde třikrát po sobě ke špatně zadanému kódu, je aktivován alarm. Ten po dobu 30 sekund vydává přerušovaný tón z piezoelementu a zároveň blikají obě diody D1 a D2. Žádnou další funkci výrobek neumožnuje.

Pro otestování výrobku jsem se řídil návodem funkčních zkoušek v normě ČSN EN 50133-1. [9] V souladu s návodem jsem naprogramoval výrobek na jednu platnou uživatelskou informaci. Po jeho zadání byl povolen přístup. To výrobek splňoval. Dále bylo třeba zkusit zadat pět po sobě neplatných informací a ověřit zda nedojde k povolení přístupu. Výrobek

povolil zadat jen tři a pak se rozezněl alarm. Dále jsem také prověřil veškeré postupy uvedené v návodu a tím také ověřil existenci uvedených vlastností. Také jsem ověřil podle návodu, zda u výrobku při odpojení elektrického napětí dojde k odpojení elektronického zámku, k čemuž v mém případě došlo.

4.2 Bezkontaktní identifikace RFID 2



Obr. 7. Bezkontaktní identifikace RFID 2.

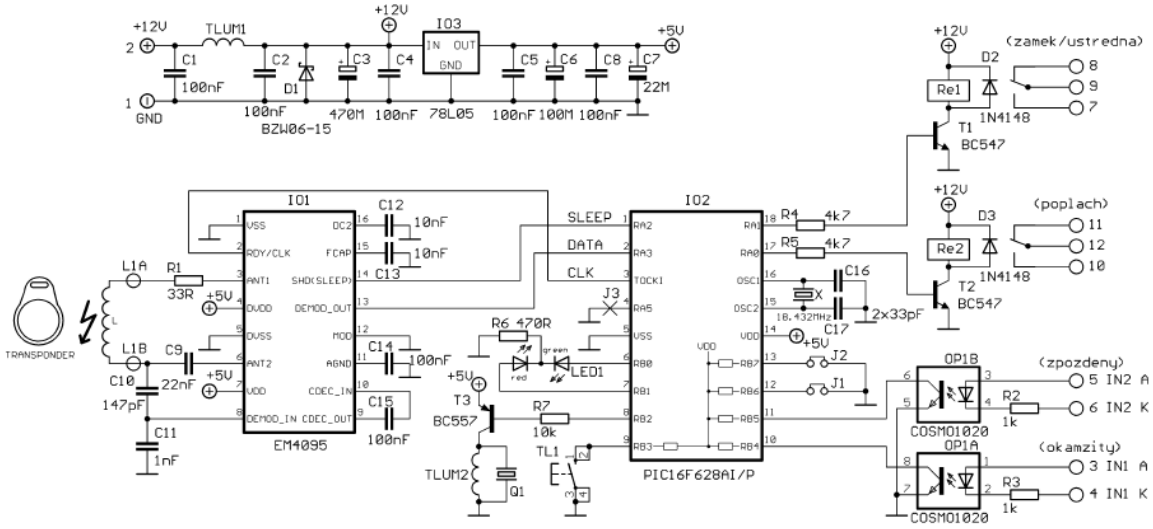
Tato elektronická stavebnice je vyráběna Českou firmou FLAJZAR s.r.o., která se dlouhá léta zabývá samostatným vývojem elektronických zařízení a přístrojů, s následnou kusovou a sériovou výrobou. Tento výrobek byl zakoupen od firmy GM elektronic, spol. s.r.o., která jej prodává za cenu 835 Kč [30]. Součástí stavebnice je deska cívky, řídící deska, všechny součástky a jedna karta na vyzkoušení. Konstrukce bezdrátové identifikace RFID je na bázi mikroprocesoru PIC. Konstrukce se skládá ze dvou desek: deska cívky, kterou si můžeme případně navinout sami, je ale potřeba přizpůsobit kondenzátory a deska elek-

troniky, na které je vše od dekodéru, přes řídící mikroprocesor, zdrojovou část až po výstupní relé. Velkou výhodou je možnost ukrytí snímací cívky pod libovolný nevodivý materiál a také, pro dosažení maximální bezpečnosti, možnost samostatného vyvedení cívky na vzdálenost minimálně 30 cm. Napájení 12V / klidový odběr cca 35mA, pokud drží relé max. 200mA. Rozměry desky cívky jsou 61 x 57 mm a desky elektroniky 67 x 67 mm. Rozměry jsou navrženy tak, aby se celá stavebnice dala umístit do krabice standardního vypínače. Dále je možnost uložení až 25ti transpondérů do paměti. Stavebnice pracuje na frekvenci 125kHz s kódem ASK Manchester. Konstrukce byla navržena jako univerzální, takže máme výběr z několika pracovních režimů:

1) Ovládání elektromagnetického dveřního zámku - přiblížením transpondéru sepne výstupní relé po dobu 5 vteřin.

2) Zapínání a vypínání libovolného spotřebiče nebo ústředny - po přiblížení transpondéru je zapnuto relé, po dalším přiblížení relé rozepne.

3) Kompletní zabezpečovací ústředna - prostřednictvím dvou vstupů můžeme připojit čidla pohybu a dveřní kontakty. Máme k dispozici vstup zpožděný a okamžitý. Na výstupech dvě relé: jedno relé slouží např. pro ovládání nějakého vyššího zařízení (při aktivaci ústředny sepne, pokud je ústředna deaktivována, rozepne), druhé jako výstup na sirénu. [21]



Obr. 8. Schématické zapojení RFID 2. [22]

4.2.1 Kompletace výrobku

4.2.1.1 Seznam použitých součástek

Tab. č. 2. Seznam součástek RFID 2. [21]

Označení	Název a velikost součástky	Označení	Název a velikost součástky
IO1	EM4095 SMD	C7	47µF/10V
IO2	PIC16F628AI/P	C12,C13	10nF
IO3	Stabilizátor 78L05 TO92	C10	100pF+47pF
T1,T2	BC547B	C11	1nF
T3	BC557B	C9	22nF
D1	transil BZW06-15	C16,C17	33pF
D2, D3	1N4148	Q1	Piezoměnič PT1540P
OP1	Dvojitý optočlen COSMO1020	X1	Krystal 18,432MHz HC49
R1	33Ω	Re1,Re2	M4-12H
R2, R3	1kΩ	TL1	P-B1720 (4,4mm)
R4, R5	4,7 kΩ	TLUM1	100uH/165mA/axial
R6	470Ω	TLUM2	33mH radial
R7	10kΩ	LED1	Dvoubarevná LED 3mm červená/zelená
C1,2,4,5 C8,14,15	100nF	J1.J2	Zkratovací kolík 2x2 + 2 x jumper
C3	470µF/16V		Patice DIL 18 pro IO2
C6	100µF/16V		4 x trojitá svorkovnice 3,5 mm
L1	Plošná leptaná cívka RFIDC1	L2	Plošný spoj RFIDRD1

4.2.1.2 Postup kompletace výrobku RFID 2

Před začátkem osazení výrobku jsem nejprve zkontroloval podle přiloženého návodu, zda byly dodány všechny komponenty a součástky potřebné pro kompletaci. Po kontrole jsem si připravil veškeré nástroje, které budu potřebovat. Jako u předešlé kompletace výrobku J – 205 jsem použil mikropájku, cín a kalafunu. Dále multimetr a PC potřebné k zjištění hodnoty a vývodů součástek. Před úplným začátkem jsem zkontroloval desku tištěných spojů, jestli jsou provrtány všechny otvory, a jestli jsou správně vedeny všechny vodivé cesty podle přiloženého návodu. Na desce tištěného spoje je předem již připájen integrovaný obvod IO1 v podobě SMD součástky, aby podle výrobce mohlo dojít ke zmenšení celého zařízení. Jako první jsem připájel na desku tištěných spojů dvě drátové propojky, které jsou umístěny pod IO2 a TLUM1. Posléze jsem na místo IO2 připájel patici DIL 18 a čtyři svorkovnice. Dále jsem přešel k připájení všech rezistorů R1 až R7 a diod D1 až D3 a pokračoval jsem v napájení kondenzátorů C1 až C17. U kondenzátorů C3,C6 a C7 jsem si dával pozor na správnou polaritu při umisťování, jelikož se jedná o elektrolyty. Kondenzátor C10 je složen ze dvou paralelně zapojených kondenzátorů o velikosti 100 a 47 pF. Další částí, kterou jsem připájel, byly tranzistory T1 až T3 a stabilizátor IO3. U těchto součástek jsem musel myslet na správné umístění nožiček na plošném spoji. Pokračoval jsem v dalším osazování součástek, a to relé Re1, Re2 krystalické součástky X1 dvou tlumivek TLUM1 a TLUM2 a zkratovací kolíky J1,J2. Posléze jsem umístil piezoměnič Q1 a optočlen OP1. U optočlenu OP1 jsem se zaměřil na jeho správnou orientaci, aby nedošlo k záměně vývodů a jejich poškození vyšším napětím. Ze strany tištěných spojů jsem umístil tlačítko TL1 a diodu LED1. Posléze za pomocí drátového propoje jsem spojil desku plošných spojů RFIDRD1 s cívkou RFIDC1 a nakonec do patice DIL 18 mikroprocesor IO2. U všech součástek majících na plošném spoji vývody blízko u sebe, jsem dával pozor, aby při pájení nedošlo ke galvanickému propojení za pomoci cínu.

4.2.2 Oživení a otestování funkčnosti výrobku

Před oživením jsem nejprve provedl pečlivou kontrolu celého výrobku, jestli byl správně osazen a vytáhl jsem z patice mikroprocesor IO2. Posléze jsem jej připojil k nastavitelnému zdroji stejnosměrného napětí o velikosti 12V a omezení proudu na 120mA. Po tomto zapojení jsem změřil napětí za stabilizátorem, jestli odpovídá velikosti napětí 5V. Odpovídal. Pokud napětí odpovídá, nastavitelný zdroj můžeme vypnout a do patice zasunout mikroprocesor IO2. Po připojení k elektronickému zámku na relé Re1 by měl po zapnutí na-

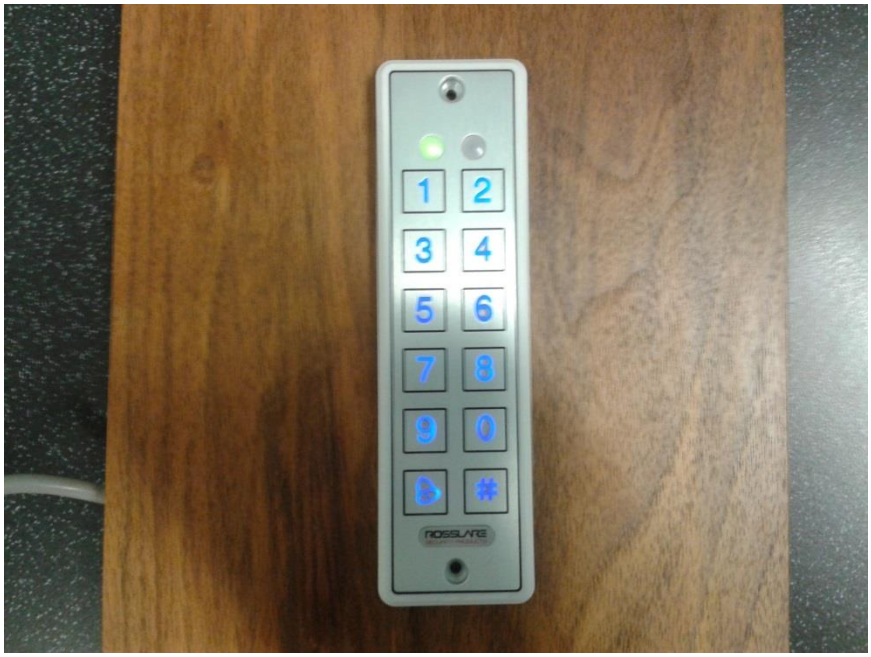
pájecího napětí výrobek fungovat. Nejprve bylo ale potřeba uložit transpondér do paměti výrobku. Při prvním spuštění jsem musel paměť smazat a naformátovat. To jsem provedl za pomoci dlouhého podržení tlačítka TL1 do doby než se ozvala sestupná melodie a červená LED1 začala blikat. Po zhasnutí LED1 byla paměť naformátována. Tento postup provádíme, i když dojde ke ztrátě transpondéru a je potřeba jej smazat z paměti. Nevýhodou je, že se smažou všechny uložené transpondéry a je tedy potřeba je uložit znovu. Ukládání samotných transpondérů jsem prováděl za pomoci tzv. učícího modu, pomocí tlačítka TL1, které jsem stlačil po dobu asi jedné vteřiny, než se rozsvítila červená LED1 a ozvalo se trojí krátké pípnutí. Nyní po přiložení transpondéru byl jeho kód načten a uložen do paměti. Paměť je schopna si uložit až 25 transpondérů. Pokud je paměť zaplněna, dojde po přiložení dalšího transpondéru k hlubšímu tónu z piezoměniče a zhasne červená LED1. Tuto funkci jsem odzkoušet tak, že jeden transpondér jsem přiložil vícekrát. Tím došlo k zaplnění paměti. Učící režim je možné ukončit krátkým stisknutím tlačítka TL1 nebo je automaticky ukončen do 45 vteřin po přiložení posledního transpondéru. Výrobek pracuje v několika pracovních módech, které jdou nastavit pomocí propojek J1 a J2. V prvním modu slouží jako ovládání elektromagnetického zámku, který lze nastavit, když jsou J1 a J2 neosazeny. V tomto modu po přiblížení transpondéru, sepnulo relé Re1 na dobu asi 5 vteřin. Při měření byla průměrná doba 4 vteřiny. Ostatní vývody jsou nevyužity. V druhém módu je J1osazen a J2 neosazen a slouží k aktivaci a deaktivaci elektromagnetickému zámku nebo ústředny. Při přiblížení transpondéru relé Re1 sepnulo, při dalším přiblížení rozepnulo. Ve třetím módu je J1 neosazen a J2 osazen. V tomto módu se jedná o kompletní zabezpečovací ústřednu. Střídavým přibližováním transpondéru aktivujeme a deaktivujeme vstupy ústředny, kde Re1 střídavě zapíná a vypíná podobně jako v modu dva. Re2 slouží k zapínání poplachové sirény. Pro účely této práce jsem zkoušel jen mód jedna a dva. V těchto pracovních modech po přiblížení oprávněného transpondéru bylo signalizováno krátkým pípnutím piezoměniče a krátké zasvícení zelené LED1. Na neuložené transpondéry výrobek nereagoval. Vzdálenost, na kterou je transpondér aktivován závisí na velikosti cívky. Pro cívku L1 dodávanou k výrobku je po změření maximální vzdálenost 5 cm. Tato hodnota byla zjištěna pomocí změření deseti vzdáleností a výpočtem jejich průměrné hodnoty. Kompletní otestování výrobku probíhalo podle návodu od výrobce a podle návodu na funkční zkoušky uvedené ČSN EN 50133-1[9], kde jsem v podstatě odzkoušel, jestli výrobek povolí přístup platné informace nebo jestli potvrdí přístup neplatné a ověřil jsem si postupy uvedené v návodu. Při odzkoušení jestli dojde k uvolnění elektronického zámku

po odpojení elektrického napětí od přístroje, byl výsledek negativní, tedy došlo k jeho uvolnění.

5 PROFESIONÁLNÍ SYSTÉMY KONTROLY VSTUPU

Za profesionální systémy kontroly vstupu jsou považovány výrobky vyráběné specializovanými výrobci, zabývajícími se tímto odvětvím. Mezi tyto firmy patří HONEYWELL, CDVI, ROSSLARE, SIEMENS, COMINFO, apod. Jejich výrobky splňují všechny technické a systémové požadavky, které nám určují normy, zákony a nařízení vlády České republiky a jsou prodávány u specializovaných prodejců.

5.1 Kontrolér AYC- E65



Obr. 9. AYC-E65.

Kontrolér AYC-E65 je výrobkem mezinárodní firmy Rosslare Security Products. V České republice lze výrobek zakoupit za cenu okolo 6000 Kč. Kontrolér AYC-E65 je tzv. konvertibilní přístupová řídicí jednotka v úzkém antivandal provedení. Může být instalován ve vnitřním i venkovním prostředí a je odolný standardním povětrnostním podmínkám. Jednotka má vestavěnu bezkontaktní čtečku EM karet a modře podsvícenou piezoelektrickou dotekovou klávesnici pro konfiguraci a správu jednotky nebo pro zadávání PINů. Kontrolér řídí přístup až pro 500 uživatelů, z nichž každý může mít v paměti jednotky zadán primární, příp. i sekundární identifikační prvek – typicky kartu a PIN. Ve spojení s tzv. inteligentním zdrojem funguje jednotka jako běžný přístupový kontrolér s reléovými výstupy pro ovládání zámku nebo jiných prvků umístěných ve zdroji, tedy typicky na zabezpečené

straně dveří. Bez připojení k tomuto zdroji funguje konvertibilní kontrolér jako běžná čtečka EM karet s vestavěnou klávesnicí. V tomto režimu jej tedy lze připojit k libovolnému jinému kontroléru, docházkovému terminálu nebo zabezpečovací ústředně s rozhraním Wiegand pro připojení čtečky/klávesnice. Mezi základní funkce, které kontrolér umožnuje je volitelná délka PINů (až 8 číslic), 3 úrovně uživatelů a režimů (běžný, bezpečnostní a bypass). V běžném režimu je dveřní zámek zablokován až do načtení platného identifikátoru. V bezpečnostním režimu musí být zadán jak primární, tak sekundární identifikátor například PIN a karta. V režimu bypass jsou podmínky vstupu do sledované oblasti rozdílné podle typu zámku. Úrovně uživatelů se dělí na běžný, bezpečnostní a master. Rozdíl mezi uživateli je v počtu identifikátorů a způsobu průchodu v různých režimech. Dále je také možnost připojení odchodového tlačítka, nastavitelná doba otevření zámku i typu připojení zámku, funkci pro zablokování po opakovaném zadání neplatných identifikátorů. Lze nastavit celkem deset režimů funkce pomocného vstupu/výstupu, včetně sledování nedovřených dveří, násilně otevřených dveří, přemostění, sledování stavu dveří, běžného nebo bezpečnostního režimu, ovládání LED stavu dveří. Obsahuje pomocný vstup a výstup, který lze nejčastěji využit jako dveřní kontakt (pomocný vstup) a prvek pro signalizaci nedovření nebo násilného otevření dveří (pomocný výstup). Možnost také připojení odchodového tlačítka. Kontrolér je napájen napětím 5 až 16V stejnosměrného napětí s maximálním proudovým odběrem 105 mA. Maximální čtecí dosah EM karet jsou 4 cm. Obsahuje dvě třístavové LED jedna režimová a druhá dveřní. Kontrolér pracuje v rozsahu teplot od -30 do 65°C a vlhkosti prostředí od 0 do 95%. Kontrolér je umístěn v kovovém pouzdře a má rozměry 155 x 44 x 9 mm a krytím IP68. Má také vestavěný optický a tranzistorový tamper. Ten slouží v případě, že dojde k neoprávněné manipulaci s kontrolérem, např. jeho sejmutím ze zdi nebo otevřením neoprávněnou osobou, vestavěný sabotážní (tamper) kontakt stav detekuje a vyvolá událost sabotáže. [23]

5.1.1 PS-C25T

Jedná se o inteligentní napájecí zdroj se dvěma napájecími moduly a dvěma reléovými výstupy pro konvertibilní kontroléry řady AYC. Napájecí napětí střídavého je 230V. Výstupní napětí je 2×12V/1,2A. Provozní teplota -10 až 50°C. Umístěn v bílém kovovém krytu. [24]

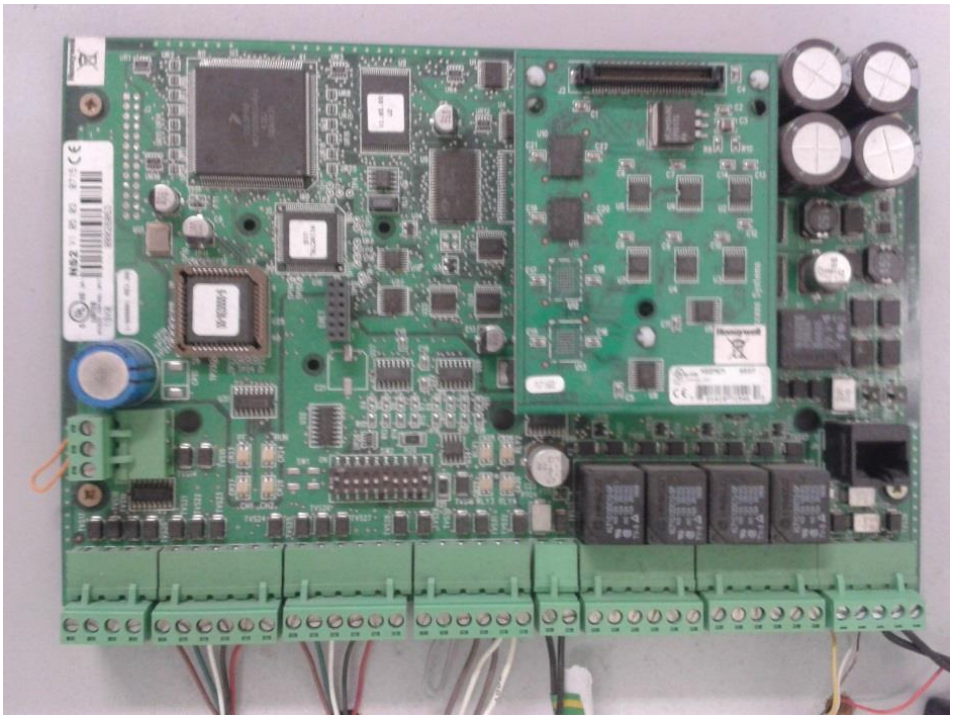
5.1.2 Otestování základních možností AYC-E65

Kontrolér AYC-E65 s napájecím zdrojem PS-C25T byl pro účely odzkoušení zapůjčen od firmy ADI Global Distribution. Kontrolér byl dodán již umístěn a zabudován na dřevěné desce. Byl propojen se zdrojem PS-C25T, a proto nebyla nutná žádná další montáž. Zdroj jsem tedy mohl zapojit přímo do sítě 230V a zároveň s tím se spustil i samotný kontrolér. Poznal jsem to podle toho, že tlačítka byla osvětlena modře a režimová LED svítila zeleně. To označuje, že kontrolér je v běžném režimu. Pokud by LED svítila červeně nebo oranžově znamenalo by to, že kontrolér je v režimu bezpečnostním nebo bypass. Přepínání mezi běžným a bezpečnostním režimem probíhalo tak, že jsem na klávesnici nejprve zadal továrně nastavený kód 3838. Režimová LED se rozblikala červeně. Po stisknutí [#] pro potvrzení změny a LED zůstala svítit červeně a tím jsem se dostal do bezpečnostního režimu. Zpět do běžného režimu se dostaneme obdobně s rozdílem, že LED svítí a bliká zeleně. Přepnutí mezi běžným a bypass režimem funguje taky stejně s rozdílem, že režimová LED svítí a bliká oranžově a kód pro přepínání není nastaven továrně, ale musíme si jej určit sami. Veškeré programování jsem prováděl pomocí klávesnice. Abych mohl započít samotné programování, musel být nejprve kontrolér nastaven v běžném režimu. Do programovacího režimu jsem se dostal tak, že jsem dvakrát stisknul klávesu [#] během 0,5 sekundy. Režimová LED zhasla a LED stavu dveří se rozsvítil červeně. Posléze bylo třeba zadat tovární kód 1234 pro vstup do programovacího režimu. Kód byl platný a LED stavu dveří se rozsvítil zeleně. K opuštění z programovacího režimu došlo, když jsem do 1minuty nezmáčknul žádné tlačítko nebo dvakrát stisknul klávesu [#]. Jestli je kontrolér zpět v běžném režimu, bylo zjištěno pomocí LED stavu dveří, které zhasnulo. Režimová LED se rozsvítila zeleně. Pokud chceme změnit programovací kód, aby nebylo možno používat továrního nastavení, vstoupíme nejprve do programovacího režimu, stiskneme tlačítko 3, zároveň se rozsvítí režimová LED zeleně. Zadáme nový programovací kód a kontrolér se automaticky vrátí zpět do běžného režimu, to poznáme tak, že uslyšíme 3 krátké pípnutí a LED stavu dveří zhasne. Tuto skutečnost jsem také ověřil. Pro změnu továrního kódu pro přepínání běžného a bezpečnostního režimu jsem postupoval obdobně, s tím rozdílem, že místo stisknutí tlačítka 3 jsem zmáčknul tlačítko 4. Dále jsem nastavoval funkci zámku, tedy jeho dobu sepnutí relé pro uvolnění dveřního zámku po zadání platného kódu. Ověřil jsem také jak nastavit chování zámku a dobu aktivace sirény při alarmových stavech. Relé lze nastavit na dva režimy běžný a reverzní. V běžném režimu relé po platném kódu spíná na přednastavenou dobu a v reverzním režimu je relé sepnuto a po zadání plat-

ného kódu relé rozepne na požadovanou dobu. Pro nastavení funkce zámku jsem tedy nejprve přešel do programovacího režimu, stisknul klávesu 6 a zároveň se režimová LED rozblikala zeleně. Poté jsem vytvořil čtyřmístný kód pro nastavení. První číslice může být 0 pro běžný režim zámku nebo 1 pro reverzní režim zámku. Druhá číslice určuje po jakou dobu má být aktivní siréna při alarmovém stavu v rozsahu 0 až 9 minut. Třetí a čtvrtá číslice ukazuje dobu uvolnění zámku v rozsahu 0 až 99 sekund. Já jsem tedy nastavil kód 0225, znamená to, že relé je v běžném režimu, doba aktivace sirény je 2 minuty a zámek bude uvolněn na 25 sekund. Po zadání čtyřmístného kódu, se kontrolér vrátil do běžného režimu. To jsem poznal tak, že jsem uslyšel 3 pípnutí a režimová LED se rozsvítila zeleně a LED stavu dveří zhaslo. Dále je možnost nastavení blokace kontroléru v případě, že dojde k několika po sobě následujících zadáních neplatného kódu. Blokaci jsem poznal podle toho, že režimová LED byla zhasnuta, LED stavu dveří blikal červeně a bzučák každé 2 sekundy pípnul. Naprogramování jsem prováděl tak, že jsem nejprve vstoupil do programovacího režimu. Stisknul klávesu 6 a zadal čtyřmístný kód. První číslice je vždy 4. Druhá číslice určuje počet po sobě následujících neplatných kódů v rozsahu 0 až 9 pokusů. Třetí a čtvrtá číslice určuje délku blokace kontroléru v rozsahu 0 až 99. Zadaná hodnota je vynásobena 10 sekundami, což odpovídá rozsahu 0 až 990 sekund. Kontrolér nám umožnuje zadávání primárních i sekundárních kódů. Primární kód se používá v běžném režimu a sekundární kód pak slouží v bezpečnostním režimu jako druhý identifikační prvek. Pro zadávání primárních a sekundárních kódů existují dva způsoby jak je zadávat do paměti kontroléru. Já jsem ověřil standartní metodu, kdy známe paměťovou pozici uživatele, kterou programujeme. Metoda vyhledání kódu se používá k zadání sekundárního kódu, je-li už předem definován primární kód. V mém testování jsem použil pouze standartní metodu. Nejprve jsem vstoupil do programovacího režimu a stisknul klávesu 7. Zároveň se LED stavu dveří rozsvítila oranžově. Zadal jsem tříměstné číslo paměťové pozice v rozsahu 001 až 500 pro zadání primárního nebo sekundárního kódu. Zvolil jsem pozici číslo 005, jelikož tato paměťová pozice byla prázdná. To jsem poznal podle toho, že režimová LED se rozblikala zeleně. Pokud by měla paměťová pozice již primární kód, režimová LED se rozbliká červeně a je možno zadat sekundární kód. Pokud by měla paměťová pozice primární i sekundární kód, bzučák nám dlouze pípne a kontrolér se vrátí do běžného režimu, což jsem také v praxi ověřil. Po rozblikání režimové LED jsem zadal svůj primární kód, tedy napsání PINu 14420 na klávesnici. Kód byl platný a přestala blikat režimová LED. Dále jsem zadal sekundární kód, v mém případě jsem přiložil bezkontaktní kartu. Pokud chceme ukládat

kódy na další paměťové pozice, zmáčkneme [#]. Jestli již nechceme nic zadávat, zmáčkneme dvakrát [#] a vrátíme se do běžného režimu. Jestliže chceme smazat kód, nejprve vstoupíme do programovacího režimu a stiskneme klávesu 8. zároveň se režimová LED rozsvítí červeně. Dále jsem zadal na klávesnici třímístné číslo paměťové pozice, kterou jsem chtěl smazat. Režimová LED se rozblikala červeně. Zadal jsem nový programovací kód, bzučák třikrát krátce pípnul a kontrolér se vrátil do běžného režimu. Posléze jsem provedl funkční zkoušky podle ČSN 50133-1 [9], zda bude povolen přístup po zadání platné uživatelské informace. Přístup byl povolen. Odzkoušel jsem pět po sobě neplatných informací, zda nebude potvrzeno povolení přístupu. Přístup nebyl povolen. Rovněž jsem se snažil prověřit veškeré možné postupy na kontroléru, které byly v návodu pro obsluhu uvedeny. Zjistil jsem, že ke kontroléru nebylo v mém případě možné připojit žádné další zařízení, jelikož byl výrobek zapůjčen a byl usazen v dřevěné desce, kde byly jeho napájecí vývody zataveny v plastu. Proto nemohla být provedena zkouška s odpojením elektronického zámku.

5.2 Honeywell NS2



Obr. 10. Honeywell NS2.

NS2 je dvoučtečkový kontrolér (panel) zajišťující řízení přístupu pro dvoje dveře. NS2 je koncipován jako autonomní kontrolér s vlastní pamětí karet (až 10000 držitelů karet) a pamětí událostí (až 100000 událostí) nebo (ve spolupráci s odpovídajícím programem) jako on-line kontrolér monitorovaný prostřednictvím softwaru v reálném čase. Paměť panelu je zálohována pomocí kondenzátoru. Při výpadku hlavního napájení i záložní baterie zálohuje tento kondenzátor paměť panelu a hodiny reálného času po dobu jednoho týdne. Komunikace mezi počítačem a panelem je zajištěna prostřednictvím sériového kabelu RS-232, nebo volitelně sběrnicí RS-485 prostřednictvím odpovídajícího komunikačního převodníku. Na každé sběrnici RS-485 může být připojeno až 31panelů. Pokud je potřeba komunikovat s řídicími jednotkami na větší vzdálenost, lze s výhodou využít jako komunikační médium síť typu LAN nebo WAN s rozhraním Ethernet. Panel NS2 lze instalovat buď samostatně, a to pomocí krytu ENC10 (jeden panel v krytu) nebo do rozvaděčové skříně. Panel má rozměry 152 x 229 mm a dokáže pracovat v teplotách od 0 až 49°C a může být skladován v teplotách od -55 až 85°C a ve vlhkosti od 0 do 85%. Svorky pro připojení vstupních a výstupních prvků jsou uspořádány podle účelu použití. Začínají vstupy pro napájecí napětí a komunikaci po RS-485 na pravé straně desky panelu a pokračují zprava doleva přes výstupy relé, svorky pro pomocné napájení, vstupy pro dveřní prvky až ke svorkám pro připojení čteček. Svorkovnice pro připojení tamper (sabotážního) kontaktu a vstupu pro signalizaci výpadku napájecího zdroje je umístěna na levém okraji desky panelu. Panel obsahuje několik signalizačních LED, které ukazují stav napájení, systému a relé. Pro napájení panelu můžeme použít 16,5 V střídavého napětí nebo stejnosměrné napájení 24 V. Jednotka NS2 poskytuje na svých svorkách výstupní napětí 12Vss, 600 mA pro napájení čteček a pomocný napájecí výstup pro obecné použití (kromě napájení zámků a jiných indukčních zátěží). [25]

5.2.1 Programu WIN-PAK PRO

WIN-PAK optimalizuje výkon systému a celkové náklady na vlastnictví tím, že podporuje více platforem Honeywell, včetně řízení přístupu, kamerového dohledu a narušení z jediného uživatelského rozhraní. WIN-PAK PRO je plně 32-bitová aplikace, která může pracovat v prostředí Windows a skládá se ze tří základních modulů – databázového serveru, komunikačního serveru a klientské pracovní stanice. Pro dokonalou funkčnost programu WIN-PAK je potřeba PC s dostatečnou hardwarovou konfigurací. WIN-PAK PRO umož-

ňuje uživateli definovat časové zóny, komunikační smyčky, panely, karty, držitele karet a jiné informace. Záznamy v databázích lze snadno editovat, prohledávat nebo třídit. Uživatel si rovněž může nechat zobrazit a vytisknout širokou škálu zpráv s informacemi o zařízeních, kartách, držitelích karet nebo o historii. WIN-PAK PRO používá tzv. mapy podlaží pro monitorování a ovládání řady běžných funkcí kontroly vstupu. Mapa podlaží zobrazuje v grafické podobě jednotlivá zařízení – dveře, panely, vstupy, výstupy nebo prvky CCTV systému. Díky zobrazení systémových zařízení (abstract zařízení – ADV) má uživatel přehled i o stavu systémového hardwaru a možnost tato zařízení dálkově ovládat. Dveře tak lze například zamknout nebo odemknout pomocí ADV v mapě, pohled z CCTV kamery může uživatel přepnout z jednoho monitoru na jiný. Oblasti řízení lze definovat přidáním zařízení do mapy řízení, která rovněž umožňuje zařízení dálkově ovládat. Okna událostí a alarmů zobrazují alarmy spolu s ostatními systémovými informacemi ve formě seznamu. [26]

5.2.2 HID iCLASS R10

Obr. 11. HID iCLASS R10.

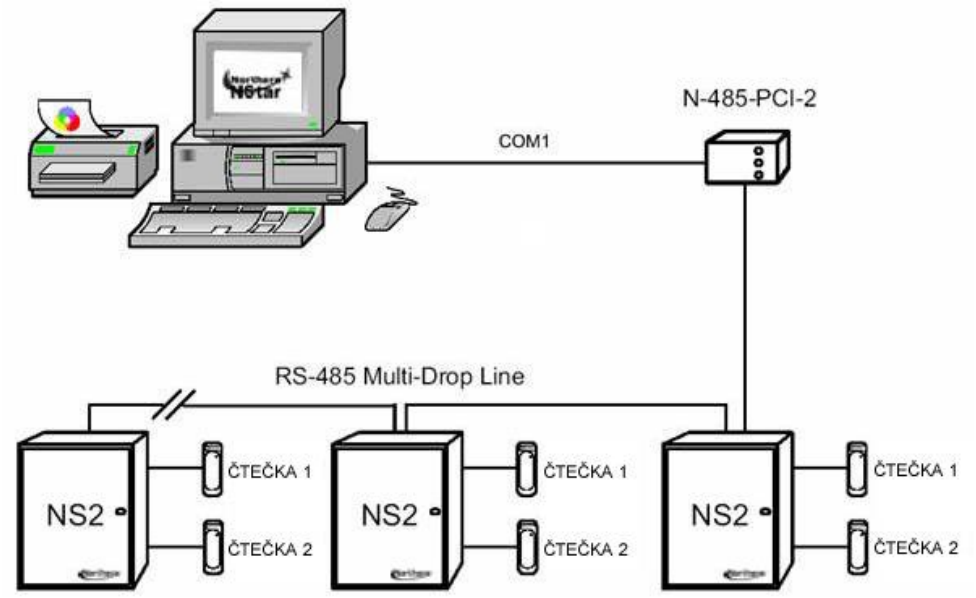
Bezkontaktní čtečka HID iCLASS R10, která je založena na technologii čtení karet iClass, Mifare, DESFire i s podporou SIO objektů. Čtečka pracuje s pracovní frekvencí 13,56 MHz na maximální čtecí dosah 7,1 cm. Napájecí napětí má od 5 do 16 V stejnosměrného napětí a odběrem 45 mA. Výstupním formátem je technologie Wiegard. Čtečka obsahuje piezoelement a LED s šesti volitelnými stavy. Je umístěna v četném krytu o rozměrech 103 x 48 x 23 mm a krytím IP 55. Její pracovní teplota je od -35 až do 65°C a do vlhkosti od 5 do 95 %. Cena této čtečky se pohybuje kolem 2600 Kč. [27]

5.2.3 Převodník N-485-PCI-2

Řada převodníků N-485 se používá pro lokální nebo dálkové propojení řídících jednotek na sběrnici RS-485. N-485-PCI-2 slouží pro přímé propojení počítače s řídícími jednotkami. Použití převodníku umožňuje zvýšení komunikační rychlosti, integrity dat i odolnost vůči okolnímu rušení. Převodník lze použít se všemi jednotkami řady NS2 a všemi verzemi programu WIN-PAK. Jeho rozměry jsou 50,8 x 98,4 x 139,7 mm. Připojení pomocí kabelu s charakteristickou impedancí 120 Ω a kapacitou menší než 20,3 pF. Je napájen 9 až 16V stejnosměrného nebo střídavého napětí. Komunikační rychlost je maximálně 38,4 kBd. [28]

5.2.4 Otestování Haneywell NS2 v programu WIN-PAK.

Panel NS2 s dvěma čtečkami HID iCLASS R10 byl již nainstalován na laboratořích D309. Za pomoci sběrnice RS-485 a převodníku N-485-PCI-2 jsem ho propojil s příslušným PC, na kterém byl nainstalován program WIN-PAK. PC i panel s NS2 jsem zapojil do elektrického napětí. PC do zásuvky na 230V střídavého napětí a NS2 na nastavitelný zdroj stejnosměrného napětí.



Obr. 12. Ukázka zapojení NS2 po sběrnici RS 485 do PC.

V programu WIN-PAK jsem musel nejprve provést propojení s NS2. Program jsem spustil a přihlásil se do něj pomocí zvoleného uživatelského jména a hesla. Posléze jsem v programu nastavil jazyk na češtinu pro lepší práci v programu. Podle návodu, který je umístěn na PC jsem provedl propojení WIN-PAKu s NS2 přes sběrnici RS 485. V hlavním okně programu WIN-PAK je na horní liště základní panel nástrojů, které lze v programu použít. Jsou to Soubor, Zobrazit, Účet, Ovládání, Karty, Systém, Zprávy, Konfigurace, Okno, Nápověda. Hned pod ní se nachází tlačítka panelu nástrojů, které jsou Přihlášení, Výběr účtu, Dynamické okno alarmů a potvrzení, Okno událostí, Okno map podlaží, Nalezení karty, Databáze karet, Zprávy, Nápověda, Odhlášení. V programu již byly po předchozím používání nastaveny časové zóny, vytvořena mapa podlaží a přidány hardwarové komponenty přístupového systému do mapy podlaží, určené přístupové úrovně, definováni držitelé karet a čísla karet a spojené s držiteli karet, definován veškerý hardware v přístupovém systému pro fiktivní softwarovou společnost. Nejdříve jsem se tedy pokusil přidat nového držitele karty, kterému jsou jednotlivé karty vydávány. Držitelé karet musí mít přiděleny alespoň dva údaje a to jméno a příjmení. Karty mají v programu definované následující vlastnosti: číslo karty, přístupovou úroveň a status, je-li karta aktivní, neaktivní, ztracená, apod. Aby mohla být karta aktivní, musí mít přidělenou platnou přístupovou úroveň. Novou kartu jsem tedy přidal kliknutím na položku Karty a v menu kliknu zase na položku Karty, což otevřelo databázi karet. Kliknutím na tlačítko Přidat se otevřelo okno záznamu karty se zobrazenou záložkou Vlastnosti karty. Do pole Číslo karty jsem zadal číslo přidávané karty, které jsem zjistil fyzicky napsané na kartě, která byla k dispozici na učebně D309. Z výklopného seznamu v poli Přístupová úroveň jsem vybral úroveň, kterou jsem se rozhodl kartě přidělit. V mém případě kancelář_zaměstnanci. Implicitně je nastaveno, že je karta aktivní. Pokud chceme nastavit datum aktivace, klikneme na tlačítko Změnit v poli Datum aktivace a pomocí kalendáře nastavíme den, měsíc, rok, kdy má být karta aktivní. Toto jsem tedy provedl také v praxi. Jestliže chceme, aby byla karta platná jen v omezeném období, klikneme na tlačítko změnit v poli Datum expirace a pomocí kalendáře zadáme konec její platnosti. Pokud chceme omezit počet použití karty, zadáme hodnotu do pole Počet použití, kde může být maximálně 4095 použití. Pro neomezený počet použití ponecháme v poli přednastavenou hodnotu 0. Proto jsem i já ponechal hodnotu 0. Po zadání všech vlastností karty jsem ji uložil pomocí tlačítka Ok. Samotné držitele karet a informace o nich jsem přidal pomocí menu Karty a označením položky Držitelé karet, přičemž se otevřelo okno databáze držitelů. Po zmáčknutí tlačítka Přidat se otevřelo okno s aktivní

položkou Základní informace. Zadal jsem údaje o držiteli do kolonek Jméno a Příjmení. Posléze jsem držiteli přidělil kartu kliknutím na záložku karty a tlačítkem Přidělit bylo otevřeno okno Výběr kliknutím na Najít pro zobrazení seznamu dostupných karet a výběru karty s odpovídající přístupovou úrovní. Tlačítkem Ok jsem se vrátil na záložku Karty. Po zadání všech požadovaných údajů jsem celý záznam uložil kliknutím na tlačítko Ok. Jelikož jsem se rozhodl, že danou kartu již využívat nebudu, přistoupil jsem tedy ke smazání karty. V menu Karty jsem kliknul na položku Karty a otevřelo se mně okno databáze karet. Vybral jsem kartu ke smazání, označil a zmáčknul tlačítko Smazat. Programem jsem byl vyzván k potvrzení smazání karty. Potvrdil jsem tedy Ano. Smazání držitele karty se provádí obdobně pouze s rozdílem, že v menu karty klikáme na položku Držitelé karet. Dále jsem odzkoušel základní funkce, jako vyhledání karet s posledními informacemi o místě a času použití karty, systémové události, které zobrazují názvy, časy a data systémových aktivit, okno alarmů, kde se zobrazují alarmy a události na čtečkách v okamžiku, kdy se odehrávají. Také okno map podlaží, díky němuž lze na mapě ovládat všechna zařízení na ní umístěná. Jako například odemknutí a zamknutí dveřního zámku, obnovení časových zón, potvrzování a mazání alarmů u všech zařízení. Na podobném principu také funguje Mapa zařízení, kde jsou stromově zobrazena všechna zařízení umístěná v systému. Také umožnuje potvrzovat a mazat alarmy a dálkově ovládat. Dále jsem odzkoušel funkci Sledování a přehledy, která umožnuje lokalizovat držitele karty. Okno přehledů obsahuje dva panely. Levý zobrazuje sledované a přehledové oblasti s jejich čtečkami. Pravý panel pak poskytuje informace o kartách a jejich držitelích. Záznam obsahuje číslo karty, její status, držitele karty, čtečku, čas a datum. Posléze jsem odzkoušel základní funkce celého systému uvedené v normě ČSN EN 50133-1[9]. Přesvědčil jsem se, zda byla platná přístupová informace potvrzena a došlo k uvolnění elektrického zámku. Postupně jsem zadával neplatné přístupové informace. Toto bylo provedeno použitím neuložené identifikační karty. Ověřil jsem si, že pokud používám neuloženou kartu, systém na ni vůbec nereaguje. Dále jsem odpojoval zařízení od elektrického proudu a zkoušel, jestli došlo k uvolnění elektrického zámku. V tomto případě k odpojení nedošlo. Na závěr jsem odzkoušel, zda systém funguje podle návodu pro obsluhu. Vše fungovalo podle mého předpokladu v souladu s návodem.

6 ZHODNOCENÍ A POROVNÁNÍ VÝROBKŮ

U veškerých komponentů systémů kontroly vstupu musí být před uvedením na trh provedeno posouzení shody parametrů s požadavky technických předpisů, které nám určuje zákon č. 22/1997 Sb. [31], o technických požadavcích na výrobky. Na základě úspěšného posouzení shody je nutné, aby výrobce označil výrobek značkou CE a vydal ES prohlášení o shodě. Jednotlivé druhy požadavků zákona č. 22/1997, Sb., jsou upřesněny v nařízeních vlády. Na elektrické a elektronické komponenty systémů kontroly vstupu se vztahují nařízení vlády č. 616/2006 Sb. [31], o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility a nařízení vlády č. 17/2003 Sb., [31] kterým se stanoví technické požadavky na elektronická zařízení nízkého napětí. Vybraných komponentů, převážně komunikačních respektive bezdrátových prvků, se týká nařízení vlády č. 426/2000 Sb. [31], kterým se stanovují technické požadavky na rádiová a na telekomunikační koncová zařízení, opět ve spojení s nařízením vlády č. 17/2003 Sb. Dále jsou požadavky na komponenty systémů kontroly vstupu popsány v technických normách ČSN EN 50133-1 a ČSN EN 501332-1[9,10], kde jsou přesně uvedeny požadavky na elektrickou bezpečnost, elektrickou kompatibilitu, kryty napájení, zkoušky vlivu prostředí a rozhraní místa přístupu. U elektronických stavebnic se posouzení shody neprovádí. Podle zákona č. 22/1997 Sb., o technických požadavcích na výrobky se elektronická stavebnice považuje za polotovar a ne za finální výrobek. Tato stavebnice je určena pro radioamatéry. Z toho důvodu nemůže výrobce převzít odpovědnost za špatnou činnost zařízení. U nařízení vlády č. 616/2006 Sb., je uvedeno, že se zkoušky neprovádí pro elektronické stavebnice se součástkami určenými pro radioamatéry, proto nemohou být splněny veškeré požadavky předepsané v normách. Samotné výrobky použité v této práci byly srovnány podle jejich základních vlastností.

6.1 Porovnání stavebnice J-250 a AYC-E65

Tab. č. 3. porovnání klávesnic J-250 a AYC-E65.

	J-250	**AYC-E65**
Napájení	16 Vss	5-16 Vss
Proudový odběr	100 mA	105 mA
Kapacita uživatelů	1	500
Délka PINu	dvanáctimístná	osmimístná
Čtečka bezkontaktních karet	NE	ANO
Úroveň uživatelů	1	3
Krytí	IP42	IP68
Samoochrana	NE	ANO
Signalizace	ANO	ANO
Doba otevření zámku	2 sekundy	nastavitelná
Komunikace s jinými zařízeními	NE	ANO
Výstup	1x relé	2x relé
Speciální funkce	NE	ANO
Cena	cca 700 Kč	cca 6 000 Kč

Elektronická stavebnice J-205 je napájena 16V stejnosměrného napětí podobně jako AYC-E65, který je napájen 5 až 16V stejnosměrného napětí a oba dva výrobky jsou napájeny z externího zdroje napětí. Proudový odběr u AYC-E65 je 105mA podobně jako J-205, která má 100 mA. J-205 si pamatuje pouze jednoho uživatele s délkou jeho PINu na dvanáct čísel. Oproti tomu AYC-E65 si pamatuje až 500 uživatelů, ale jejich délka PINu je jen osmimístná. AYC-E65 má také v sobě zabudovanou čtečku bezkontaktních karet, což výrobek J-205 neobsahuje. AYC-E65 umožnuje rozeznávat tři úrovně uživatelů (běžná, bezpečností a bypass). U výrobku J-205 to opět není možné, protože má pouze jednu uživatelskou úroveň. AYC-E65 je umístěná v úzkém antivandal provedení pro vnější a vnitřní umístění s krytím IP68 a obsahuje optický a tranzistorový tamper. J-205 je umístěna v plastovém krytu, který umožnuje použití pouze ve vnitřních prostorách a krytím IP42 a neobsahuje žádný tamper. Dále AYC-E65 obsahuje dvě třístavové LED a bzučák (stavu dveří a režimovou). J-205 obsahuje také dvě LED (stav dveří a programovací) a bzučák. AYC-E65 dovoluje nastavení doby otevření zámku i typu připojeného zámku a funkce zablokování po opakovaném zadání neplatných identifikátorů. J-205 má oproti tomu přesně stanovenou dobu otevření na 2 sekundy a po 3 neplatných zadáních dochází k vyhlášení poplachu. AYC-E65 umožňuje také připojení odchodového tlačítka a může komunikovat

se zařízeními pomocí výstupu Wiegand. J-205 neumožnuje žádné další propojení. AYC-E65 obsahuje relé pro jedny dveře a pomocný kontakt pro sledování stavu dveří. J-205 oproti tomu obsahuje relé jen pro jedny dveře. AYC-E65 má funkci vyhledávání kódů uživatelů v paměti a také funkci pomocného vstupu/výstupu, včetně sledování nedovřených dveří, násilně otevřených dveří, přemostění, sledování stavu dveří, běžného nebo bezpečnostního režimu. J-205 žádnou dodatečnou funkci nemá. Cena AYC-E65 je okolo 6000 Kč [23] naproti tomu cena J-205 je pouze asi 700 Kč [19]. Celkově se dá tedy konstatovat, že AYC-E65 je ve všech směrech lepší, bezpečnější a kvalitnější. Výhodou J-205 je skutečnost, že umožnuje větší délku PINu a hlavně je levnější. Elektronická stavebnice J-205 neumožnuje tolik funkcí a nastavení jako AYC-E65. Je podstatně technologicky zastaralejší a jednoduší, což je dáno tím, že používá starší a méně složité součástky, kterými je možné daný výrobek osadit radioamatéry.

6.2 Srovnání čtečky RFID2 s řídící jednotkou NS2 se dvěma čtečkami

Tab. č. 4. Srovnání čtečky RFID2 s řídící jednotkou NS2 se dvěma čtečkami.

	RFID2	**NS2, HID iCLASS R 10, WIN-PAK**
Klasifikace dle rozsahu a topologie	autonomní	modulární
Napájení	12 Vss	24 Vss, 16,5 Vstř.
Kapacita uživatelů	25	10 000
Paměť událostí	0	100 000
Výstup	1x relé	2x relé
Vstup	1	2
Komunikace s jinými zařízeními	NE	ANO
Frekvence	125 kHz	13,56 MHz
Maximální čtecí dosah	5 cm	7,1 cm
Způsob konfigurace	manuálně	programově
Cena	cca 900 Kč	řádově desítky tisíc Kč

Základním rozdílem mezi elektronickou stavebnicí RFID2 a řídící jednotkou NS2 s dvěma čtečkami HID iCLASS R10 a ovládacím softwarem WIN-PAK je, že RFID2 je autonomní systém, zatím co NS2 s čtečkami a WIN-PAKem je systém modulární. RFID2 je napájen pouze 12V stejnosměrného napětí a NS2 může být napájen stejnosměrným napětím 24V nebo střídavým napětím 16,5V, které zároveň napájí i čtečky a elektronické zámky. Paměť stavebnice RFID2 umožnuje uložit až 25 uživatelů. U NS2 je paměť až 10000 uživatelů

s pamětí událostí až 100000 událostí. Dále závisí na použitém ovládacím softwaru. RFID2 má pouze jedno čtecí zařízení a dokáže ovládat jedny dveře. NS2 oproti tomu může připojit dvě čtečky a ovládat dvoje dveře. RFID2 nemá žádné krytí ani žádnou samoochranu a velikostně lze umístit do krabice standartního vypínače nebo rozvaděčové skříně. NS2 také nemá žádné krytí. Lze jej naproti tomu instalovat buď samostatně pomocí krytu ENC10 nebo do rozváděčové skříně. RFID2 neumožnuje žádnou komunikaci s ostatními zařízeními. NS2 umožnuje komunikovat s počítačem prostřednictvím sériového kabelu RS-232 nebo volitelně sběrnicí RS-485 prostřednictvím odpovídajícího komunikačního převodníku, na které může být připojeno až 31panelů. Umožnuje také komunikovat s řídicími jednotkami na větší vzdálenost pomocí sítě typu LAN nebo WAN s rozhraním Ethernet. RFID2 pracuje na frekvenci 125 kHz s čtecí vzdáleností 5 cm naproti tomu použité čtečky HID iCLASS R10 na frekvenci 13,56 MHz na maximální čtecí dosah 7,1 cm. Programování RFID2 je realizováno pomocí tlačítka a signalizace LED a piezoměniče. NS2 je oproti tomu ovládán programem WIN-PAK, který umožňuje uživateli definovat časové zóny, komunikační smyčky, panely, karty, držitele karet a jiné informace a zobrazovat veškeré alarmy a systémové události. Graficky zobrazuje jednotlivá zařízení – dveře, panely, vstupy, výstupy, díky němuž je možno sledovat stav systémového hardwaru a možnost tato zařízení dálkově ovládat. Cena RFID2 se pohybuje okolo 900 Kč [21] zatím co systém NS2 s dvěma HID iCLASS R10 a softwarem WIN-PAK řádově okolo desítky tisíc Kč [32].

6.3 Zhodnocení

Elektronické stavebnice pro použití v systémech kontroly vstupu, jsou oproti profesionálním komponentům systémů kontroly vstupu v současné době technologicky a funkčně zastaralejší. Profesionální komponenty umožnují mnohem více funkcí a jsou lépe chráněny před nedovoleným poškozením a před pokusy o vniknutí do střeženého prostoru. Elektronické stavebnice obsahují minimum funkcí a nejsou převážně vůbec chráněny. To je dáno tím, že se jedná o stavebnici určenou k osazení radioamatéry. Samotná stavebnice musí být konstrukčně jednoduší. Plošné spoje jsou jasněji vedeny a obsahují větší koncovou plochu k připájení větších součástek. Aby ji mohl sestavit i radioamatér, je stavebnice osazena technologicky staršími a jednoduššími součástkami. Stavebnice není vhodná z bezpečnostního hlediska k ovládání zařízení, strojů a přístrojů, které by mohly při špatném sestavení způsobit škody na majetku a zdraví obyvatel. Nespornou výhodou elektronické sta-

vebnice je její cena, která je nesporně nižší než u profesionálních komponentů. To je převážně dámo tím, že se nejedná o finální výrobek, ale o polotovar. Z toho důvodu není elektronická stavebnice nijak certifikována. Využití těchto stavebnic není k zabezpečení velkých podniků, obchodů, továren a perimetrů pozemků. Dají se využít k zabezpečení vnitřních prostor domu (obytné místnosti, sklady apod.), kde jsou konstantní teplotní podmínky. Dále také k výuce ve školách k názorné ukázce funkčnosti a zapojení. Nebo je možno využít v praktických hodinách, kde si žáci odzkoušejí vlastní kompletaci výrobku. Stavebnice mohou být využity i k mnoha jiným činnostem, které si spotřebitel vymyslí, ale vždy je to na jeho vlastní zodpovědnost. Vše tedy spočívá na spotřebiteli, zda zvolí výrobek levný, ale s méně kvalitními funkcemi nebo si za kvalitnější a spolehlivější výrobek připlatí. Já osobně bych tedy doporučil kvalitu. Nepředpokládám totiž nějaké větší technické zlepšení elektronických stavebnic, a to z důvodu, že kompletaci provádějí radioamatéři, kteří za pomoci svého nářadí nemají možnost kompletovat složitější zapojení. Také se nedomnívám, že dojde k většímu masovému prodeji elektronických stavebnic, jelikož se jedná o okrajovou zájmovou prodejní sféru, která má poměrně malý rozsah zákazníků.

ZÁVĚR

Tato bakalářská práce má čtenářům poskytnou ukázku složení současných systémů kontroly vstupu a různé druhy jejich komponentů, které se nacházejí na trhu. V této práci se zabývám srovnáním profesionálních komponentů systémů kontroly vstupu s jinými komponenty, které nejsou přímo sestaveny a nejsou speciálně určeny do systémů kontroly vstupu. V mém případě jsem za tyto výrobky považoval tzv. elektronické stavebnice. Elektronické stavebnice jsou určeny k tomu, aby je zákazník nejprve zkompletoval podle přiloženého návodu, a až potom mohl využívat jejich předem určených funkcí. Na trhu se nachází mnoho stavebnic, které mají využití v mnoha oblastech lidské činnosti. Můžeme se setkat se stavebnicemi, které umožňují například dálkové ovládání, měření a regulování. Dále lze také sestavit různé druhy zabezpečovací techniky a audio techniky, napájecích zdrojů, zábavní techniky apod. Výrobou těchto stavebnic se zabývají specializované firmy. Mnoho stavebnic je možné si zakoupit a sestavit podle návodů, zveřejněnými radioamatéry na internetu.

V teoretické části mé bakalářské práce jsem se zabýval základním popisem systémů kontroly vstupu. Popisuji systémy kontroly vstupu, kde se vyskytují a k čemu slouží. Popisuji základní úkoly a funkce, které musí systém kontroly vstupu splňovat. Popisuji také kombinace s ostatními poplachovými systémy. Dále je zde popsána základní struktura systémů kontroly vstupu a popis identifikačních prvků, snímacích zařízení, řídících jednotek, centrálních jednotek, blokovacích zařízení. Na závěr jsem v teoretické části uvedl a popsal normy, které se zabývají systémem kontroly vstupu.

V praktické části mé bakalářské práce jsem popsal způsob kompletace dvou elektronických stavebnic, které jsem si pro účel této práce pořídil. Jednalo se o kódovou klávesnici a čtečku bezkontaktní identifikace. Po zkompletování jsem výrobky odzkoušel a postup zapsal. Z profesionálních výrobků jsem použil autonomní klávesnici se zabudovanou čtečkou bezkontaktních karet a modulární systém kontroly vstupu od firmy Honeywell NS2 se dvěma bezkontaktními čtečkami ovládané programem WIN-PAK. Tyto výrobky jsem zprovoznil a následně popsal jejich otestování. Nakonec jsem veškeré výrobky porovnal a zhodnotil základní rozdíly mezi profesionálními systémy kontroly vstupu a elektronickými stavebnicemi.

Přínosem mé bakalářské práce je popis základních výhod a nevýhod elektronických stavebnic. Tyto stavebnice si jistě najdou mezi radioamatéry své uplatnění i v budoucnosti.

SEZNAM POUŽITÉ LITERATURY

[1] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9.

[2] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2011. ISBN 978-808-7500-057.

[3] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management III: [teorie a praxe ochrany majetku a fyzické bezpečnosti]. 1. vyd. Zlín: VeRBuM, 2013. ISBN 978-808-7500-354.

[4] UHLÁŘ, Jan. Technická ochrana objektů [online]. Vyd. 1. Praha: Vydavatelství Policejní akademie České Republiky, 2006, 246 s. [cit. 2015-04-12]. ISBN 80-725-1235-8.

[5] FOJTÍK, Daniel. Systémy kontroly vstupu pro kombinované a integrované systémy. Zlín, 2010. Dostupné z: http://hdl.handle.net/10563/11825. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

[6] 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.

[7] VALOUCH, Jan. Projektování bezpečnostních systémů [online]. První. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012 [cit. 2015-04-12]. ISBN 978-80-7454-230-5. Dostupné z: http://www.utb.cz/

[8] LAUCKÝ, Vladimír a Rudolf DRGA. Specialní technologie komerční bezpečnosti [online]. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012 [cit. 2015-02-03]. ISBN 978-80-7454-146-9. Dostupné z: http://www.utb.cz/

[9] ČSN EN 50133-1. Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky. 1. vyd. Praha: Český normalizační institut, 2001. 28 s. Třídící znak 334593

[10] ČSN EN 50133-2-1 Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 2-1: Všeobecné požadavky na komponenty. 1. vyd. Praha: Český normalizační institut, 2001. 12 s. Třídící znak 334593

[11] ČSN EN 50133-7 Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace. 1. vyd. Praha: Český normalizační institut, 2000. Třídící znak 334593

[12] 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.

[13] www.sovte.cz dostupný z http://www.sovte.cz/cipove-karty.php

[14] www. open- close.cz dostupný z http://www.open-close.cz/identifikacni_media.html

[15] www.qdocházka.cz dostupný z http://www.qdochazka.cz/biometricky-snimac.html

[16] www.světsiti.cz dostupný z http://www.svetsiti.cz/clanek.asp?cid=Cipove-karty-a-USB-tokeny-aneb-bezpecnejsi-autentizace-a-sifrovani-2-metody-autentizace-482003

[17] ČSN CLC/TS 50398. Poplachové systémy – Kombinované a integrované systémy – všeobecné požadavky. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. Třídící znak 33 4597.

[18] Jabel [online]. [cit. 2015-05-08]. Dostupné z: http://sklep.jabel.com.pl/produkt/129/12/Zestawy_do_montazu/Elektronika_domowa/J-205_Code_lock.html

[19] J-205 [online]. In: . [cit. 2015-05-27]. Dostupné z: http://sklep.jabel.com.pl/produkt/129/12/Zestawy_do_montazu/Elektronika_domowa/J-205_Code_lock.html

[20] Pájení [online]. [cit. 2015-05-08]. Dostupné z: http://cs.wikipedia.org/wiki/P%C3%A1jen%C3%AD

[21] Flajzar: RFID identifikační systém pro 25 uživatelů [online]. [cit. 2015-05-27]. Dostupné z: http://www.flajzar.cz/elektronicke-stavebnice/rfid-identifikacni-system-pro-25-uzivatelu.htm

[22] Flajzar: RFID identifikační systém pro 25 uživatelů. 516-Aktuální návod - RFID s PIC obj.č.453 [online]. 2005 [cit. 2015-05-27]. Dostupné z: http://www.flajzar.cz/elektronicke-stavebnice/rfid-identifikacni-system-pro-25-uzivatelu.htm

[23] ADI Global Distribution: Konvertibilní kontrolér s bezkont. čtečkou EM a piezo klávesnicí 2x6 tlačítek. AYC-E65 - Instalační a uživatelský manuál_CZ_p [online]. [cit. 2015-

05-27]. Dostupné z: https://www.adiglobal.cz/iiWWW/cz/produkty130.nsf/web_category_list1_cenik_asc/288DE5E7F126D728C12575EE00336AA5

[24] ADI Global Distribution: Inteligentní napájecí zdroj s výst.relé pro konvertibilní kontroléry řady AYC [online]. [cit. 2015-05-27]. Dostupné z: https://www.adiglobal.cz/iiWWW/cz/produkty130.nsf/w/003BBDE86F641AB5C12575EE00336AAF?OpenDocument

[25] 1000805_NS2 - Instalační manuál_CZ_www (1) [online]. 2009, 24 s. [cit. 2015-05-21].

[26] Adi Global. WIN-PAK PRO - Manuál 2. Praha.

[27] Adi Global Distribution: Bezkontant.čtečka (podpora SIO) iCLASS/Mifare/DESFire, úzká [online]. [cit. 2015-05-27]. Dostupné z: http://www.adiglobal.cz/iiWWW/cz/produkty130.nsf/web_category_panel1_cenik_asc/04640338FF2A0052C1257A0E001DE8B1

[28] Katalogový list N-485-PCI Jazyk: Český Verze: 10/2002 .. N-485-PCI-2 [online]. 2002 [cit. 2015-05-27]. Dostupné z: https://www.adiglobal.cz/iiWWW/docs.nsf/../N-485%20-%20KL_CZ.pdf

[29] NStarIntroduction [online]. In: . [cit. 2015-05-27]. Dostupné z: https://www.honeywellaccess.com/documents/NStarIntroduction.pdf

[30] Bezkontaktní identifikace RFID 2 FLAJZAR KF453 [online]. [cit. 2015-05-27]. Dostupné z: http://www.gme.cz/bezkontaktni-identifikace-rfid-2-flajzar-kf453-p763-384

[31] Česká republika. Zákon č. 22/1997 Sb. o technických požadavcích na výrobky a o změně a doplnění některých zákonů. In Sbírka zákonů. 2007, 6. s. 128-136

[32] Honeywell NS2+ Control Panel [online]. [cit. 2015-05-30]. Dostupné z: http://www.security.honeywell.com/me/products/access/cp/117781.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

#	Mřížka
%	Procenta
°C	Stupeň Celsia
µF	Mikrofarad
A	Ampér
ADV	Abstrakt zařízení
C1-17	Kondenzátor
CCTV	Uzavřený televizní okruh (Closed Circuit Television).
CE	Označení shody produktu s požadavky předpisů EU
cm	Centimetr
ČSN	Česká technická norma.
D1-3	Dioda
DNA	Deoxyribonukleová kyselina (deoxyribonucleic acid).
EAN	Mezinárodní číslo obchodní položky (European Article Number).
EM	Elektromagnetická
EN	Evropská norma.
EPROM	Erasable Programmable Read-Only Memory
EPS	Elektronická požární signalizace.
EZS	Elektronický zabezpečovací systém.
ID	Identifikace informace (Identification information).
IP	Značení odolnosti elektrického zařízení proti vniknutí cizího tělesa či kapaliny (ingress protection)
IR	Infračervené záření (Infrared).
J1,2	Zkratovací kolíky

kBd	KiloBaud
Kč	Koruna česká
kHz	Kilohertz
kΩ	Kiloohm
L1	Deska cívky
L2	Deska tištěných spojů
LAN	Místní síť (Local Area Network)
LED	Dioda emitující světlo (Light-Emitting Diode)
mA	Miliampér
mH	Milihenry
MHz	Megahertz
mm	Milimetr
nF	Nanofarad
OP	Optočlen
PC	Osobní počítač (Personal Computer).
pF	Pikofarad
PIC	Jednočipové mikropočítače
PIN	Osobní identifikační číslo (Personal Identification Number).
PVC	Polyvinylchlorid.
Q1	Rezonátor, Piezoměnič
R/O	Nepřepisovatelné (read/only)
R/W	Přepisovatelné (read/write)
R1-7	Rezistor
Re1,2	Relé
RFID	Identifikace na rádiové frekvenci (Radio Frequency Identification).

S1-12 (TL1)	Tlačítka
Sb.	Sbírka
SIO	(Secure Identity Object)
SMD	Povrchová montáž zařízení (Surface Mount Device)
spol. s.r.o.	Společnost s ručením omezeným
SW	Programové vybavení (Software).
T1-3	Tranzistor
Tlum1,2	Tlumivka
Tzv.	Tak zvané
US1-3 (IO1-3)	Označení řídících členů
V	Volt
Vss	Volt stejnosměrného napětí
Vstř.	Volt střídavého napětí
WAN	Globální síť(Wide Area Network)
X1	Krystalická součástka
Ω	Ohm

SEZNAM OBRÁZKŮ

SEZNAM TABULEK