

System EKV s řídící jednotkou NetAXS-123 a přístupovým systémem WIN-PAK

Bc. Jaroslav Kobza

Diplomová práce
2019



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Jaroslav Kobza**
Osobní číslo: **A17322**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Forma studia: **kombinovaná**

Téma práce: **Systém EKV s řídicí jednotkou NetAXS-123 a přístupovým systémem WIN-PAK**

Téma anglicky: **A Physical Access System with a NetAXS-123 Controller and the WIN-PAK Programme**

Zásady pro vypracování:

1. Seznamte se s přístupovou řídicí jednotkou NetAXS-123 a s možností správy přes webové rozhraní od společnosti Honeywell.
2. Vytvořte jednoduchý demonstrační panel s jedním elektrickým zámekem a RFID čtečkou.
3. Na demonstračním panelu otestujte naprogramování řadiče NetAXS-123 přes webový prohlížeč.
4. Nastudujte správu přístupového systému s programem WIN-PAK.
5. Pomocí programu WIN-PAK 4 proveďte naprogramování demonstračního panelu s řídicí jednotkou NetAXS-123 a ověřte jeho správnou funkci.
6. Porovnejte jednotku NetAXS-123 s řídicí jednotkou jiného výrobce.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. UHLÁŘ, J. Technická ochrana objektů, II. Díl. Praha: Vydavatelství PA ČR, 2005. ISBN 80-7251-189-0.
2. ČANDÍK, M. Objektová bezpečnost II. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-217-3.
3. NetAXS-123 Jednotka pro řízení přístupu – Uživatelská příručka. Honeywell, 2010. 165 stran.
4. NexAXS123 Příručka k uvedení systému do provozu. Honeywell, 2010. 24 stran.
5. Winpak 4 uživatelský manuál. Honeywell, 2014. 696 stran.
6. Atrium, jednotka kontroly vstupu s webovým rozhraním – instalační manuál. Honeywell. 32 stran.
7. Atrium, jednotka kontroly vstupu s webovým rozhraním – uživatelský manuál. Honeywell. 24 stran.

Vedoucí diplomové práce:

Ing. Stanislav Goňa, Ph.D.

Ústav elektroniky a měření

Datum zadání diplomové práce:

30. listopadu 2018

Termín odevzdání diplomové práce:

17. května 2019

Ve Zlíně dne 14. prosince 2018

doc. Mgr. Milan Adámek, Ph.D.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

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

Ve Zlíně, dne 22.5.2019

.....
podpis diplomanta

ABSTRAKT

Diplomová práce je zaměřena na způsob konfigurace a nastavení řídicí jednotky přístupového systému NetAXS-123 společnosti Honeywell prostřednictvím webového rozhraní a programu WIN-PAK pro správu přístupového systému. Teoretická část se zabývá hardwarovou skladbou řídicích jednotek přístupového systému a možnostmi softwarových nástrojů pro jejich správu. Získané poznatky jsou analyzovány a porovnávány s příslušnými technickými normami. Praktická část se zabývá sestavením demonstračního panelu osazeného řídicí jednotkou přístupového systému NetAXS-123 a uvádí korektní postup jeho konfigurace v návaznosti na připojené vstupní a výstupní periférie. Praktická část si dává za cíl být vodítkem pro studenty, kteří se zabývají problematikou a možnostmi konfigurace přístupového systému NetAXS-123 prostřednictvím programu WIN-PAK pro jeho správu.

Klíčová slova: řídicí jednotka přístupového systému, vstupní místo, entita, komunikační rozhraní, WIN-PAK, konfigurace, vstupní čtecí a snímací zařízení, aktivátor

ABSTRACT

The diploma theses deals with way of configuration and setting of the NetAXS-123 access control unit by Honeywell thru web interface of WIN-PAK access control system. The theoretical part is focused on hardware composition of the access control system units and the possibilities of software tools for their management. Clues are analyzed and compared with the relevant technical standards. The practical part deals with the assembly of the showcase panel equipped with the control unit of the NetAXS-123 access control system and presents the correct procedure of its configuration related to the connection of an input and output peripherals. The aim is to be a guide for students who deal with the issues and various possibilities of configuration the NetAXS-123 access system through WIN-PAK solution.

Keywords: Access control unit, Entry point, Entity, Communication interface, WIN-PAK, Configuration, Input read device, Activator

Tímto bych chtěl poděkovat svému vedoucímu Ing. Stanislavu Goňovi, Ph.D. za jeho vedení, poskytnutý čas a cenné rady při vypracování mé diplomové práce. Současně bych rád poděkoval své manželce za podporu po celou dobu studia.

OBSAH

ÚVOD	7
I TEORETICKÁ ČÁST	9
1 ÚVOD DO PŘÍSTUPOVÝCH SYSTÉMŮ	10
2 IDENTITA UŽIVATELE	12
3 ROZHRANÍ UŽIVATELE	13
3.1 DATOVÝ VÝSTUP.....	13
3.2 BEZKONTAKTNÍ ČTEČKA HID ICLASS SE R10	16
4 ŘÍDÍCÍ JEDNOTKA KONTROLY VSTUPU	19
4.1 ŘÍDÍCÍ JEDNOTKA KONTROLY VSTUPU NETAXS-123	19
4.2 KONFIGURACE ŘÍDÍCÍ JEDNOTKY PŘÍSTUPOVÉHO SYSTÉMU NETAXS-123	22
5 SOFTWARE PRO SPRÁVU PŘÍSTUPOVÉHO SYSTÉMU WIN-PAK	27
6 VÝSTUPNÍ ZAŘÍZENÍ	43
6.1 ELEKTOMAGNETICKÉ ZÁMKY	43
6.2 OSTATNÍ ZÁMKY	44
7 KOMUNIKAČNÍ ROZHRANÍ	45
II PRAKTICKÁ ČÁST	46
8 NÁVRH PŘÍSTUPOVÉHO SYSTÉMU	47
9 DEMONSTRAČNÍ PANEL	48
10 KONFIGURACE NX1P	50
10.1 KONFIGURACE PŘES WEBOVÝ PROHLÍZEČ	50
10.2 KONFIGURACE PROGRAMEM WIN-PAK SE	55
11 POROVNÁNÍ ŘÍDÍCÍCH JEDNOTEK	61
11.1 SITUACE NA TRHU	61
11.2 ŘÍDÍCÍ JEDNOTKA PŘÍSTUPOVÉHO SYSTÉMU A22.....	61
ZÁVĚR	63
SEZNAM POUŽITÉ LITERATURY	64
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	65
SEZNAM OBRÁZKŮ	66
SEZNAM TABULEK	68
SEZNAM PŘÍLOH	69

ÚVOD

Pokud v současné době zadavatel řešení systému elektronické kontroly vstupu (dále EKV) zadá do Internetového vyhledávače heslo „přístupový systém“ zobrazí se mu nepřehledné množství odkazů na výrobce, dodavatele, systémové integrátory a mnoho dalších. Pro zadavatele řešení EKV není jednoduché zorientovat se v nabízených produktech a řešeních jednotlivých subjektů. V současné době se pak nabízí dvojí cesta, kterou si zadavatel řešení EKV může vybrat:

1. Zadat návrh řešení externě. Výhodou je přenesení kompetencí, ale i zodpovědnosti na externího řešitele. Nevýhodou navýšení ceny výsledného řešení.
2. Pokusit se zorientovat v nabídkách jednotlivých dostupných řešitelů a sestavit tabulku pro vícekritériální hodnocení, která bude aplikována na jednotlivá řešení systému EKV.

Pokud se řešitel systému EKV vydá cestou vlastního výběru podle výše uvedeného druhého bodu, pak se postupně dopravuje k jednomu ze základních kritérií, a tím jsou reference požtávaného subjektu. Zadavatel by měl požadovat od subjektu odpovědi na otázky:

1. Jaké jsou jeho zkušenosti s navrhovanou implementací řešení systému EKV?
2. V jakých objektech je řešení systému EKV implementováno?
3. Jaká je zastupitelnost subjektu v případě jeho výpadku? (ochrana investice zadavatele řešení systému EKV).
4. Jakým způsobem a za jakých podmínek subjekt zajišťuje servis implementovaného systému EKV, a zda je tento způsob v souladu s představou provozovatele systému EKV?

V různých pozicích se nachází zadavatelé řešení systému EKV pro bytový dům, kde se odhaduje výše investice v řádech několika málo desítek tisíc korun s minimálním požadavkem na další růst systému EKV, a na zadavatelé řešení systému EKV pro objekt státní správy nebo administrativně – obchodního centra, kde se předpokládá investice řádově ve stovkách tisíců korun s možností dalšího růstu a změn systému EKV v průběhu následných několika let, a to podle vývoje požadavků na funkci příslušné státní instituce nebo změn nájemců v administrativně – obchodním centru. U těchto rozsáhlých systémů musí být od začátku uvažováno, aby byla zachována kontinuita a kompatibilita systému EKV minimálně po celou následující dekádu z důvodu ochrany investice (např. systém EKV pro státní polici ČR).

Diplomová práce si dává za cíl vytvořit laboratorní úlohu s řídicí jednotkou přístupového systému NetAXS-123: popsat konkrétní řešení pro systém EKV tak, aby byl vodítkem pro studenty z pohledu možností implementace, konfigurace a správy systému EKV.

Z pohledu pozice produktu NetAXS-123 na českém trhu, splňuje tento všechny parametry pro to, aby byl implementován do rozsáhlých řešeních, u kterých se předpokládá růst z pohledu počtu řízených vstupů (dveře, vjezdová vrata, vstupní turnikety atp.), ale také z pohledu zvyšování počtu osob (identifikačních médií), ale současně není vyloučena možnost použít řídicí jednotku přístupového systému NetAXS-123 samostatně na řízení jednoho vstupu:

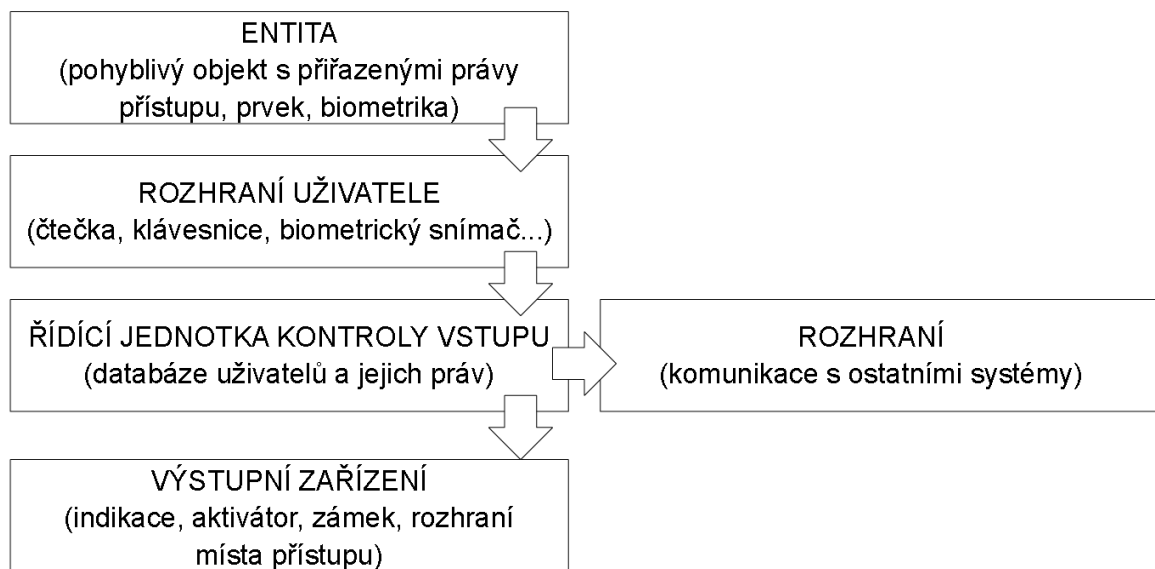
1. Kontinuita – výroba, vývoj a distribuce je zajišťována nadnárodní společností.
2. Robustnost – systém je dále rozšiřitelný s prakticky neomezenou kapacitou dveří a osob.
3. Dosažitelnost – distribuce zajišťuje školení různých subjektů.
4. Funkčnost – zajištěna dostupnost kompatibilních náhradních dílů, pravidelná aktualizace firmware řídicí jednotky kontroly vstupu.

I. TEORETICKÁ ČÁST

1 ÚVOD DO PŘÍSTUPOVÝCH SYSTÉMŮ

Systémy EKV jsou primárně určeny k restrikci osob, tzn. zabránění přístupu nepovolaným osobám do zabezpečených oblastí nebo k zabezpečeným aktivům, jakými mohou být utajované skutečnosti či informace, hmotný i nehmotný majetek atp. Konfigurací a správou systému EKV je určeno „KDO“, „KDY“ a „KAM“ má povolen přístup a jakým způsobem tuto skutečnost prokazuje. Nejedná-li se o autonomní přístupový systém, který plní spíše jen funkci komfortního vstupu pro oprávněné osoby, pak veškeré aktivity přístupového systému se evidují a zaznamenávají, případně se posouvají dále ke zpracování dalším systémům.

Systémy EKV se obecně skládá z několika funkčních částí.

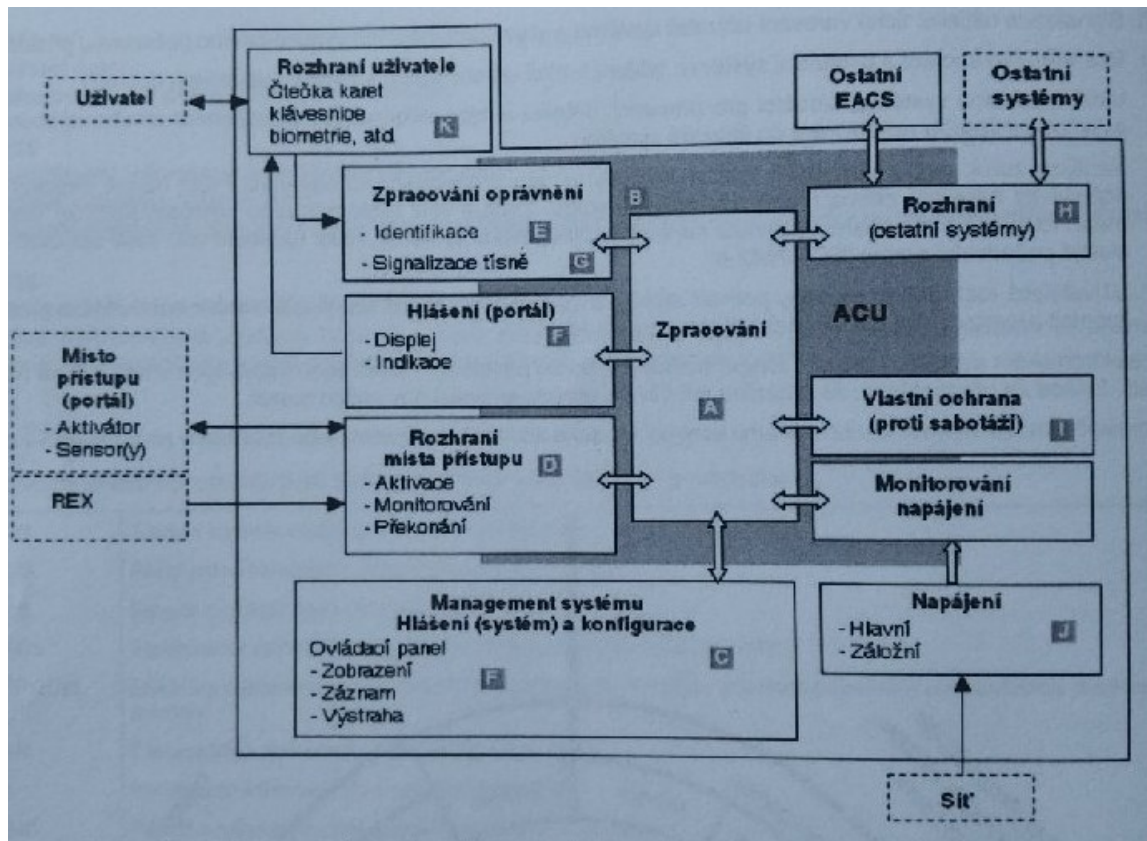


Obr. 1 – Funkční části systému EKV [Zdroj: vlastní]

Ověření totožnosti uživatele (autentizace) probíhá v závislosti na typu identifikačního nosiče informací. Jedná se o:

- vlastnictví předmětu (RFID čip, karta, token ...),
- znalost informace (PIN, heslo ...),
- biometrický údaj (otisk prstu, oční duhovka, 3D snímání obličeje ...).

V závislosti na hodnotě zabezpečených a chráněných aktiv a odhodlání (znalosti/schopnosti) a způsobu útoku pachatelů systém obejít [2], stanovuje norma ČSN EN 60839-11-1 třídu identifikace a klasifikaci přístupu, kde jsou k jednotlivým stupňům uvedeny minimální požadavky na typ identifikace, případně na kombinaci uvedených typů identifikace.



Obr. 2 – Typická architektura elektronického systému kontroly vstupu [2]

Při návrhu řešení zabezpečení referenčního objektu systémem EKV je nutné vhodně zakomponovat požadavky klienta s technickými možnostmi systému EKV. Návrh je nutné zpracovat z globálního pohledu na přístupový systém jako na funkční celek a zároveň je nutné rozpracovat řešení zabezpečení každého jednotlivého vstupu zvlášť. Při návrhu se musí zohlednit technické řešení v kontextu s požadavky na provozní režim objektu, počet uživatelů, četnosti průchodů, komfort správy systému, nouzové otevírání a požární ochranu objektu, funkčnost systému při poruše.

2 IDENTITA UŽIVATELE

Každý přístupový systém pracuje s identitou uživatele, na základě které povoluje nebo naopak zakazuje vstup do zabezpečené oblasti. Kvalita přístupového systému je dána přesností ověření identity uživatele v rozsahu povolené odchylky. Podle základních principů pak dělíme ověřování identity uživatele:

- identifikace heslem (znalost hesla nebo PINu),
- identifikace předmětem (vlastnictví předmětu),
- biometrická identifikace (jedinečná biometrická charakteristika člověka).

S přesností určení identity uživatele souvisí i míra rizika a úroveň zabezpečení. Teno vztah řeší Norma ČSN EN 60839-11-1 v kapitole 6.1. Metodika klasifikace a funkcí – Stanovení úrovně ochrany. Klasifikace systémů kontroly vstupu jsou určeny jedním ze čtyř stupňů, kde stupeň 1 je nejnižší a stupeň 4 nejvyšší.[2]

Tab. 1 – Stupně klasifikace [2]

Stupeň	1	2	3	4
Úroveň rizika	Nizké	Nizké až střední	Střední až vysoké	Vysoké
Aplikace	organizační prostředky, ochrana majetku nízké hodnoty	organizační prostředky, ochrana prostředků nízké až střední hodnoty	méně organizačních prostředků, ochrana komerčních prostředků střední až vysoké hodnoty	zejména ochrana komerčních prostředků velmi vysoké hodnoty nebo kritické infrastruktury
Dovednost/znalosti pachatelů/útočnicků	malá dovednost, malá znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií malé finanční prostředky pro napadení	střední dovednost a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií malé až střední finanční prostředky pro napadení	velká dovednost a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií střední finanční prostředky pro napadení	velmi vysoká dovednost a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií velké finanční prostředky pro napadení
Typické příklady	hotel	obchodní kanceláře, malé firmy	průmysl, administrativní prostory, finanční instituce	Vysoce citlivé prostory (vojenská zařízení, vládní budovy, výzkum a vývoj, kritická infrastruktura

3 ROZHRAŇÍ UŽIVATELE

V současné době jsou nejčastěji v přístupových systémech používány bezkontaktní RFID čtečky. Dalšími možnými prvky rozhraní uživatele mohou být biometrické čtečky, nejčastěji pro snímání otisku prstu, ale i duhovky oka, rozpoznávání tváře, snímání krevního řečiště ruky atp. Rozhraní uživatele má primárně za úkol identifikovat osobu pro následné vyhodnocení, zda je osoba oprávněna vstoupit do zabezpečené oblasti.

V závislosti na úrovni zabezpečení a s ohledem na typ rozhraní uživatele, může být tato vybavena tamper kontaktem. Jedná se především o autonomní přístupové systémy, kde celá architektura přístupového systému je implementována do jediného zařízení. Tamper kontakty jsou mechanické nebo optické.

Pokud je rozhraní uživatele vybaveno signalizačními vícebarevnými LED, můžeme jejich pomocí signalizovat různé stavy zabezpečené oblasti, pro kterou řídí vstup. Nejčastěji je signalizován stav zastřežení zabezpečené oblasti. Využití signalizačních vícebarevných LED vyžaduje vyšší počet vodičů než je běžné, zpravidla jedna barva vyžaduje jeden vodič navíc.

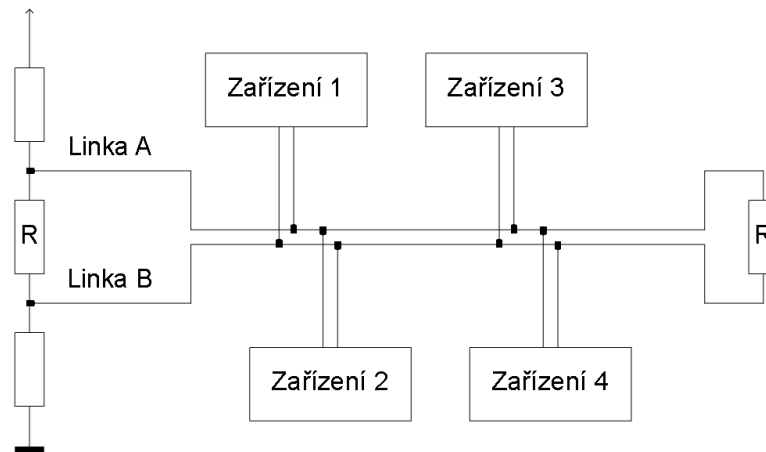
3.1 Datový výstup

Další vlastností, která nás u rozhraní uživatele zajímá je způsob připojení k řídicí jednotce kontroly vstupu, tzv. datový výstup. Rozlišujeme rozhraní uživatele se sběrnice datovým výstupem nebo s datovým výstupem Wiegand.

Sběrnice EIA-485 (RS-485) je realizována zpravidla dvěma vodiči – linka A a linka B. U sběrnice datových zařízení je nutné při návrhu a realizaci dbát na kompatibilitu snímacích a čtecích prvků s řídicí jednotkou kontroly vstupu. Mezi jednotlivými prvky systému probíhá komunikace, která je zpravidla šifrovaná. Šifrování není univerzální, ale každý výrobce používá svůj vlastní způsob šifrování přenášených dat mezi připojenými zařízeními. Kromě vyšší bezpečnosti (velmi obtížné až nemožné kopírování identifikačních médií – RFID karet, přívěsků atp.) je zde zajištěn pro výrobce odbyt jím vyráběných zařízení a systémů. Základní vlastnosti sběrnice EIA-485:

- Délka sběrnice až 1200m díky kroucené dvoulince a diferenciálnímu kódování, přičemž přenosová rychlost může být až 10 Mbit/s. Odbočky k jednotlivým vysílacům/přijímačům by neměly být delší než 5m.

- Počet současně fungujících vysílačů a přijímačů může být až 32 na jednom okruhu sběrnice.
- Pro správnou funkci sběrnice EIA-485 musí být na obou koncích instalovány zakončovací rezistory 120 Ω .



Obr. 3 – Způsob připojení čtyř zařízení na sběrnici EIA-485 [Zdroj: vlastní]

Rozhraní **Wiegand** je univerzální. Jedná se o normovaný datový výstup rozhraní uživatele. Tento standardizovaný datový výstup umožňuje připojit čtecí nebo snímací zařízení libovolného výrobce k řídicí jednotka přístupového systému výrobce třetí strany. Při návrhu přístupového systému pro referenční objekt pak musíme dodržet technologickou jednotnost všech rozhraní uživatele a vyhodnocovacích jednotek. Z pohledu uživatele, ale i projektanta přístupového systému je univerzálnost datového výstupu Wiegand výhodná hned z několika pohledů:

- **Bezpečnost** – volíme technologii, která splňuje požadované bezpečnostní standardy a to mezi přenosem informací mezi identifikačním médiem a čtecím nebo snímacím zařízením.
- **Design** – čtecí nebo snímací zařízení volíme podle jeho rozměrů, nebo podle vzhledu s ohledem na umístění.

Univerzální rozhraní Wiegand vyžaduje minimálně 4 vodiče pro připojení rozhraní uživatele k vyhodnocovací jednotce. Dva vodiče pro napájení 12Vss, a dva vodiče datové, označené jako DATA 0 a DATA 1 (někdy označované také jako WIEGAND 0 a WIEGAND 1). Při zapojení zařízení na kabel UTP Cat.5, ale lépe na kabel F/UTP Cat.5, je vhodné dodržovat barevné zapojení vodičů pro vlastní, ale i budoucí orientaci při pravidelných servisních prohlídkách systému:

Napájení +12V	oranžový vodič.
Napájení 0V	bílý vodič od oranžového.
Data 0	zelený vodič.
Data 1	bílý vodič od zeleného.



Obr. 4 – Rozpletení kabelu UTP Cat.5 [3]

Další vodiče je možné použít na ovládání LED, podle typu zařízení 1 až 2 vodiče pro ovládání zelené a červené LED a 1 vodič pro ovládání bzučáku zařízení. Vzhledem k tomu, že kabel F/UTP Cat.5 má celkem 8 vodičů, je zpravidla dostačující pro připojení jednoho rozhraní uživatele. Vzdálenost zařízení od vyhodnocovací jednotky závisí na doporučení výrobce, ale dnes zpravidla většina výrobců uvádí vzdálenost až 150m. Rozhraní Wiegand umožňuje paralelní připojení více rozhraní uživatele k jednomu portu vyhodnocovací jednotky (například vjezd do areálu, kde jsou RFID čtečky pro osobní a nákladní automobily umístěné na jednom sloupku, protože ovládají jedno společné zařízení). U tohoto způsobu zapojení však musíme uvažovat, že se zvýší úbytek napětí na vedení v důsledku vyššího proudového odběru zapojených rozhraní uživatele a úměrně tomu se zkrátí maximální povolená délka kabelu mezi vyhodnocovací jednotkou a rozhraní uživatele.

Rozhraní Wiegand pracuje s přenosem čísel. Základní a nejrozšířenější jsou formáty s délkou 26 bitů, ale můžeme se setkat s délkami 28, 33, 37, 48, 50 bitů, ale i dalšími.

Základní vlastnosti univerzálního rozhraní Wiegand:

- Rozhraní uživatele lze připojit k libovolné řídicí jednotce přístupového systému.
- Připojení k řídicí jednotce přístupového systému minimálně 4mi vodiči.
- Umožňuje spojovat vstupy/výstupy paralelně.
- Vzdálenost rozhraní uživatele od řídicí jednotky přístupového systému až 150m.

- Rozhraní Wiegand nemá přímou souvislost s použitou snímací technologií (EM, Mifare, DESfire ... atp.).

3.2 Bezkontaktní čtečka HID iCLASS SE R10

Pro laboratorní úlohu byl jako referenční typ rozhraní uživatele zvolena bezkontaktní čtečka iCLASS SE R10.

Popis bezkontaktní čtečky iCLASS SE R10:

Nová řada čteček iCLASS SE přináší vyšší zabezpečení dat uložených v kartě i jejich přenos do čtečky, a to zejména díky velmi robustní autentizaci prostřednictvím modelu SIO (Secure Identity Object), který zajišťuje důvěryhodnou a vysoce bezpečnou komunikaci mezi kartou a čtečkou. Kromě klasických identifikačních prvků jakými jsou standardní bezkontaktní přístupové karty nebo přívěsky iCLASS SE podporuje i identifikaci prostřednictvím mobilních zařízení. Toto řešení nabízí poměrně zajímavý způsob bezpečné distribuce identifikačního prvku do vzdáleného mobilního zařízení. Výrobce nabízí technologii iCLASS SE v několika provedeních bezkontaktních čteček, od klasického úzkého provedení R10, přes provedení v kombinaci s kódovou klávesnicí RK40 až po dlouhodosahové provedení R90.[4]

Tab. 2 – Základní parametry bezkontaktní čtečky iCLASS SE R10 [4]

Typ čtečky	bezkontaktní
Technologie	iCLASS; Mifare; DESFire
Napájecí napětí	5 - 16 Vss
Odběr	45 mA
Max. čtecí dosah	9 cm
LED dioda	6-stavová (volitelně)
Bzučák	ano
Barva krytu	černá
Krytí	IP55
Pracovní teplota	-35 - 65 °C
Relativní vlhkost	5 - 95 %
Rozměry - výška	103 mm

Rozměry - šířka	48 mm
Rozměry - hloubka	23 mm
Kompatibilní karta (příklad)	iClass 2K (varianta SE)
Kompatibilní přívěsek (příklad)	iClass 2K Key (varianta SE)
Kompatibilní nalep. TAG (příklad)	iClass 2K Tag (varianta SE)
Použití v exteriéru	ano
Pracovní frekvence	13,56 MHz
Výstupní formát	Wiegand

Základní vlastnosti:

Vysoké zabezpečení – Bezpečnost na několika úrovních i mimo samotné karty, pro extra vysoké zabezpečení ID dat pomocí SIO (Secure Identity Object) .[4]

Přizpůsobivost – Čtečky mohou spolupracovat s řadou technologií a ID médií, včetně mobilních zařízení (s využitím modelu Seos) .[4]

Flexibilita – Čtečky mohou obsluhovat celou řadu typů aplikací; jsou navíc konfigurovatelné pomocí karet i přímo v instalaci.[4]



Obr. 5 – Bezkontaktní čtečka HID iCLASS SE R10, pohled z čelní a zadní strany

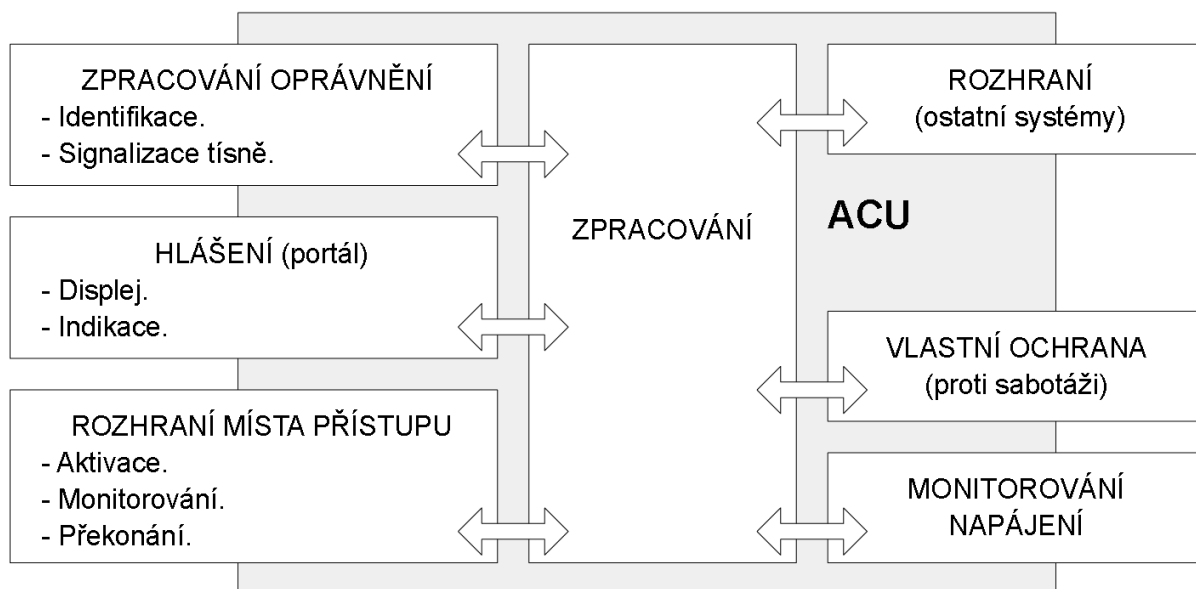
[Zdroj: vlastní]

Bezkontaktní čtečka je zalitá v epoxidu a výrobce u ní udává doživotní záruku. Vzhledem k provedení čtečky je z ní vyveden několika žilový vodič, kterým se připojuje k řídicí jednotce přístupového systému. Barevné označení a význam je uveden v tabulce č.3.

BARVA	VÝZNAM	BARVA	VÝZNAM
žlutá	bzučák	červeno-zelená	GPIO1 (RS232-T/RS485-A)
oranžová	zelená LED	sv.hnědá	GPIO2 (RS232R/RS485-B)
černá	napájení -	fialová	tamper
červená	napájení +	bílá	wiegand data 1
hnědá	červená LED	zelená	wiegand data 0
modrá	funkce HOLD	růžová	GPIO3 (RS485-Z)
		šedá	GPIO4 (RS485-Y)

4 ŘÍDÍCÍ JEDNOTKA KONTROLY VSTUPU

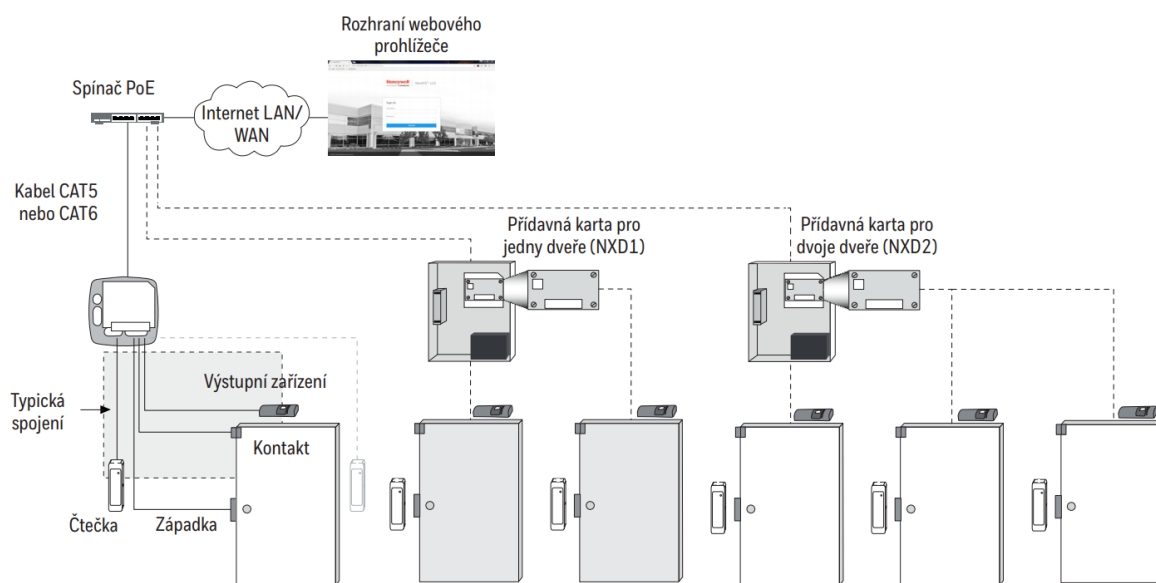
Řídící jednotka kontroly vstupu (ACU – access control unit) je část systému kontroly vstupu, která je propojena se čtečkami, uzamykacími zařízeními a snímači, rozhodující o poskytnutí nebo zamítnutí přístupu vstupním místem.[3]



Obr. 6 – Blokové schéma řídicí jednotky přístupového systému. [3]

4.1 Řídící jednotka kontroly vstupu NetAXS–123

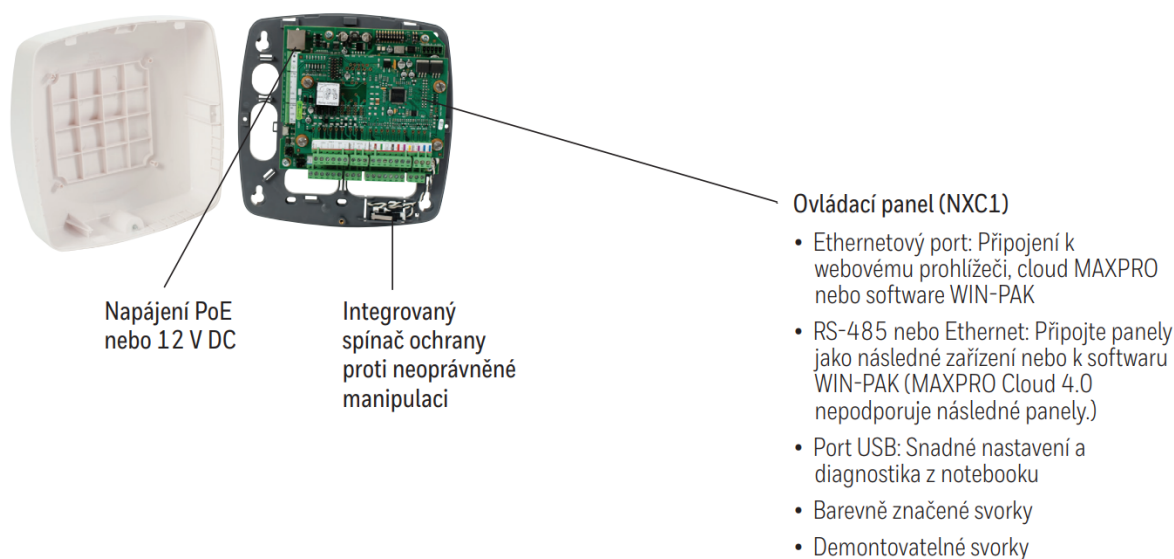
Pro laboratorní úlohu byla zvolena řídicí jednotka přístupového systému NetAXS–123, typové označení provedení NX1P pro řízení jednoho místa přístupu.



Obr. 7 – Přehled přístupového systému s řídicími jednotkami NetAXS-123.[5]

Webová řídicí jednotka NetAXS společnosti Honeywell poskytuje řešení pro instalace jakékoliv velikosti. NetAXS-123 umožňuje uživatelům bezpečně spravovat systém pomocí Internetu, kdekoliv je k dispozici připojení – bez vyhrazeného počítače nebo softwaru. Uživatelsky přívětivý design zjednodušuje instalaci a usnadňuje obsluhu a údržbu.[5]

NetAXS-123 poskytuje všechny výhody tradičního řízení vstupu, například pomáhá zabezpečovat dveře, řídit vstup zaměstnanců a dálkově ovládat různá místa. Umožňuje rovněž vytvářet zprávy, aby byly splněny předpisové požadavky. Díky webovému rozhraní se značně zkracuje doba zácvičení a zaškolení. Nevyžaduje se žádný vyhrazený software – jednoduše se přihlaste a jste připraveni k práci, zabezpečeně – z kanceláře nebo odkudkoliv odjinud. NetAXS-123 je možné spravovat pomocí integrovaného prohlížeče, zabezpečené infrastruktury cloudu MAXPRO, nebo integrované sady zabezpečení WIN-PAK®. Panel NetAXS-123 byl vyvinut tak, aby se snadno instaloval a snadno se přizpůsoboval stávající infrastruktuře IT a metodám při současném snížení nákladů na instalaci a podporu. Jak váš systém poroste, stejně poroste i NetAXS.[5]



Obr. 8 – Řídicí jednotka přístupového systému NetAXS–123 v plastové skříni.[5]

Přístupový systém vybudovaný s řídicími jednotkami přístupového systému NetAXS – 123 je vysoce flexibilní:

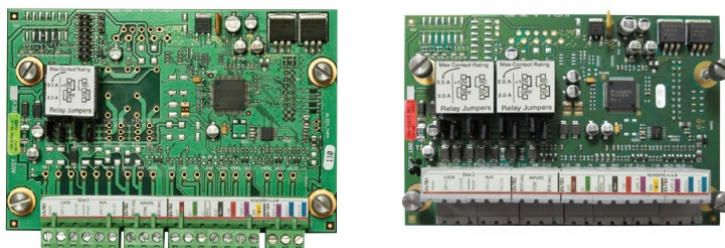
- Možnost integrace, cloudu nebo funkce z hostitelského softwaru z jediného panelu.
- Panel NetAXS-123 je možné nasadit pro mnoho různých činností – od základního řízení vstupu pro jedno místo či několik míst, přes zabezpečení na podnikové úrovni s plně integrovaným přístupem, videem a detekcí průniku.[5]

Je umožněna rychlejší instalace:

- Nativní hardware na bázi IP s napájením Power over Ethernet (PoE) eliminuje nutnost další kabeláže síťového modulu a zjednodušuje celé napájení panelu.
- Montáž vedle dveří pomocí plastové skříně snižuje nutnost vedení kabeláže.
- Součástí dodávky je kovová skříň s napájením 4 A a záložní baterie pro tradiční instalace nebo renovace.[5]

Nižší pořizovací náklady:

- Řídicí jednotku pro jedny dveře je možné rozšířit pro správu 2 nebo 3 dveří s pomocí přídatných karet pro 1 nebo 2 dveře (přídavná karta NXD2 je kompatibilní pouze pro provedení NX1P v kovové skříni).
- Přidáním dodatečných panelů lze správu provádět pomocí integrovaného rozhraní prostřednictvím virtuálního okruhu Ethernet (EVL) nebo RS-485.
- Čtečky na každé straně dveří mohou pracovat bez dodatečného hardwaru. [5]



Obr. 9 – Přídavné karty pro 1 a 2 dveře pro NetAXS-123.[5]

System zvyšuje produktivitu:

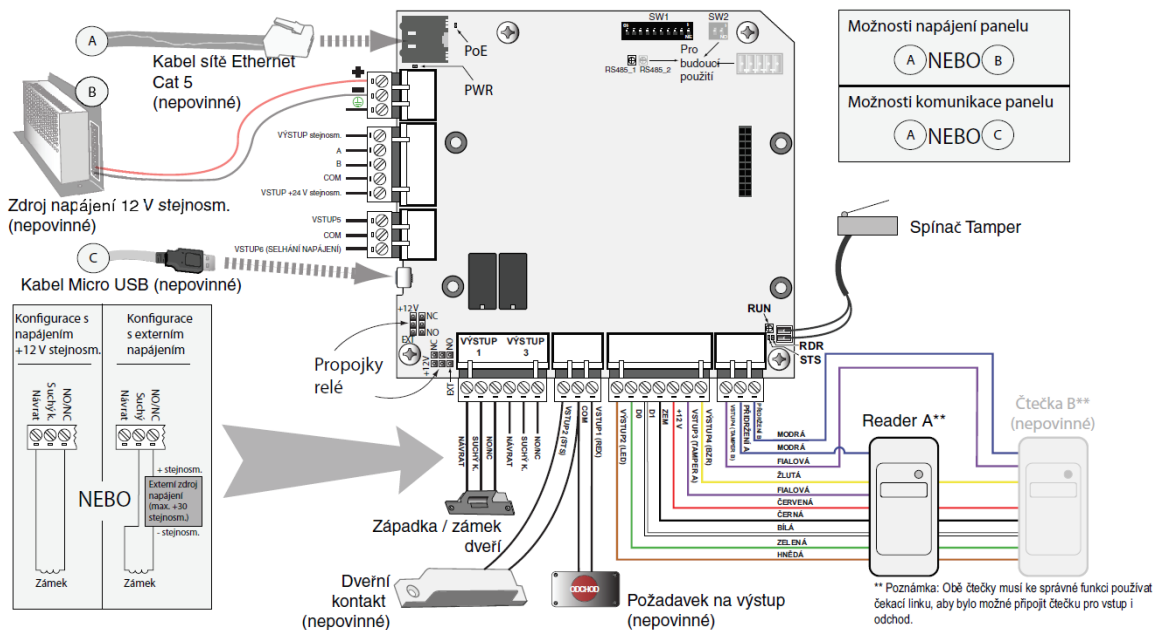
- Novější, rychlejší a intuitivnější uživatelské rozhraní zkracuje dobu strávenou nasažením systému a školením.
- Integrovaný webový prohlížeč má funkce základního řízení vstupu, které jsou jednoduché a snadno použitelné. Přidáním cloudu MAXPRO nebo WIN-PAK lze získat pokročilejší funkce, například integraci videa a detekci průniku, pokročilejší tvorbu zprávy a tvorbu fotografií na identifikační karty.[5]

Zabezpečení řídicí jednotky pro přístupový systém NetAXS je jednak mechanické a jednak je šifrována komunikace mezi zařízeními:

- 256 bitové šifrování AES komunikace mezi panelem a hostiteli (prohlížeč, cloud a WIN-PAK).

- Možnost používání certifikátu zabezpečení zajišťuje zabezpečenou a důvěryhodné připojení k panelu.
- Spínač neoprávněné manipulace s panelem na plastové a kovové skříně.[5]

Schéma připojení uživatelských a systémových rozhraní k desce elektroniky řídicí jednotky přístupového systému NetAXS-123 je následující:



Obr. 10 - Schéma připojení uživatelských a systémových rozhraní.[6]

4.2 Konfigurace řídicí jednotky přístupového systému NetAXS-123

Systém NetAXS-123 lze nakonfigurovat mnoha různými způsoby podle konkrétních potřeb koncového uživatele.

Základní konfiguraci řídicí jednotky přístupového systému NetAXS-123 lze uvést v několika málo bodech:

- Ověření výchozího továrního nastavení spínačů DIP.

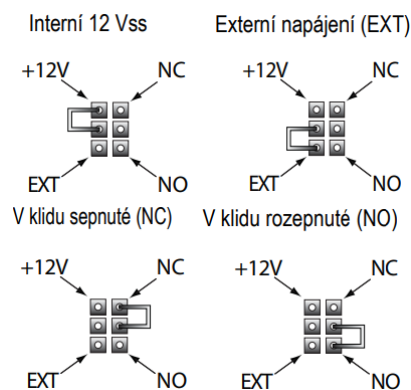


Skutečná orientace spínačů DIP na desce řídicí jednotky je otočena o 180°.

- Ověření způsobu napájení: PoE nebo externí 12Vss.

Při použití napájení PoE zůstává k dispozici celkem 450mA (pro 12Vss) pro napájení externích zařízení. Zálohování napájení z PoE se realizuje napájecím switche ze záložního zdroje UPS.

- Volba komunikačního kanálu: IP/ Ethernet nebo USB.
- Nastavení konfigurace relé pro výstupy. Pro dvě relé se nastavuje typ napájení: 12Vss externí nebo interní, a typ kontaktu: NO nebo NC.



Obr. 11 – Nastavení přepínačů pro konfiguraci relé.

- Pořadí připojení zařízení:
 1. Rozhraní uživatele (vstupní čtecí a snímací zařízení: bezkontaktní čtečky, kódové klávesnice, snímače biometrických prvků ... atp.).
 2. Vstupní zařízení (prvky pro rozhraní místa přístupu, odchodové tlačítko, indikace změny stavu místa přístupu... atp.).
 3. Výstupní zařízení (prvky pro rozhraní místa přístupu, zámek, aktivátor ... atp.).
 4. Rozhraní komunikace (Ethernet nebo micro USB-B)

Před připojením rozhraní USB musí být v počítači nainstalovány příslušné ovladače.

- Připojení k elektrické síti.
 1. Zapnutí externího zálohovaného napájecího zdroje nebo napájení přes PoE.
 2. Ověření napájení řídicí jednotky.
Rozsvítí se kontrolka PoE nebo PWR a po určitou dobu se načítá operační systém. Kontrolka RUN LED bude zpočátku svítit červeně a poté začne blikat zeleně s frekvencí jedenkrát za sekundu.
 3. Ověření funkčnosti panelu a zapojení – kontrolka RUN LED krátce modře blikne při aktivaci libovolného vstupu. Kontrolka RDR LED zeleně blikne po přiložení karty ke čtečce.

- Připojení k webovému serveru.

Existují dvě možnosti připojení – prostřednictvím kabelu micro USB-B nebo prostřednictvím potru Ethernetu.

Výrobce doporučuje připojit řídicí jednotku přístupového systému NetAXS-123 prostřednictvím USB kabelu až v okamžiku, kdy jsou na počítači instalovány všechny příslušné ovladače (dostupné na CD přiložené k řídicí jednotce).

Pro připojení řídicí jednotky přístupového systému NetAXS přes port Ethernetu je důležité znát tovární nastavení IP adresy:

192.168.1.150 s maskou podsítě:255.255.255.0

Do uvedeného rozsahu adres je nutné nastavit počítač, ke kterému bude řídicí jednotka přístupového systému NetAXS-123 připojena, například 192.168.1.10 s maskou podsítě 255.255.255.0.

- Přihlášení do systému.

Podporovány jsou internetové prohlížeče Internet Explorer a Mozilla Firefox. V případě připojení přes USB kabel se zadává IP adresa: <https://192.168.2.150>. Pro komunikaci prostřednictvím sítě Ethernet se zadává IP adresa: <https://192.168.1.150>.

Pro přístup do cílové stránky NetAXS-123 je uživatel vyzván k zadání jména a hesla. Tovární nastavení jména je: „admin“ a hesla: „admin“. Rozhraní pro přihlášení rozlišuje malá a velká písmena.

Přes webový prohlížeč je možné provést kompletní konfiguraci řídicí jednotky přístupového systému NetAXS-123:

- Časové zóny, svátky.
- Formáty karet.
- Dveře (+kontakty/ tlačítka/ výstupy)
- Přístupové úrovně.
- Karty (+ držitelé) a jejich přístupová oprávnění.
- Zobrazování událostí a alarmů.

A ovládání systémových nástrojů:

- Upgrade firmwaru.
- Upload/ download souborů atp.[6]

Tab. 3 - Technické parametry řídicí jednotky NetAXS-123.[5]

	TECHNICKÉ ÚDAJE	NX1P	NX1MPS
KOMUNIKACE	INTEGROVANÉ MOŽNOSTI KOMUNIKACE	Ethernet; RS-485; USB	
	KONEKTIVITA ROZŠÍŘOVACÍCH MODULŮ I/O	Port RS-485 použijte k připojení maximálně 6 následných modulů I/O (4 výstupy a 2 vstupy)	
	SCHOPNOSTI OKRUHU ŘÍDICÍ JEDNOTKY	EVL: 16 panelů NetAXS-123 RS-485: 31 panelů NetAXS-123 nebo NetAXS-4 celkem ^{1,2}	
ČTEČKY / DVEŘE	SCHOPNOSTI DVEŘÍ / ČTEČEK	1 dveře / 2 čtečky (rozšiřitelné na 2 dveře / 4 čtečky)	1 dveře / 2 čtečky (rozšiřitelné na 3 dveře / 6 čteček)
	ROZŠÍŘITELNOST	Rozšiřitelné na 93 dveří / 186 čteček na okruh řídicí jednotky ^{1,2}	
	KOMPATIBILITA ČTEČKY	Podpora standardního protokolu Weigand; bez podpory ABA	
VÝSTUPY	POČET VÝSTUPŮ	2 SPDT (volitelné propojkou NO nebo NC kontaktů) na dveře, dimenzování 3 A při 28 V DC; 2 otevřené výstupy kolektoru (OC), dimenzování 16 mA při 12 V DC; K dispozici je LED čtečky (AUX) a buzčák čtečky (AUX) na dveře	
	ROZŠÍŘITELNOST VÝSTUPU	2 relé, 2 OC rozšiřitelné na 4 relé, 4 OC s NXD1 přídavnou kartou	2 relé, 2 OC rozšiřitelné na 6 relé, 6 OC s NXD2 přídavnou kartou
	RELÉOVÝ NAPÁJECÍ ZDROJ	Volitelné: napájecí zdroj 12 V DC nebo externí napájení 0–28 V DC	
VSTUPY	POČET VSTUPŮ	6 konfigurovatelných čtyřstavových dozorovaných vstupních bodů (Výchozí tovární nastavení: stav, REX, neoprávněná manipulace se čtečkou A, neoprávněná manipulace se čtečkou B, porucha napájení a obecný vstup)	
	ROZŠÍŘITELNOST VSTUPU	5 vstupů rozšiřitelných na 10 s přídavnou kartou NXD1 (rozšiřitelné na celkem 74 vstupů pomocí maximálně 2 reléových vstupních karet NX4IN)	5 vstupů rozšiřitelných na 14 s přídavnou kartou NXD2 (rozšiřitelné na celkem 74 vstupů pomocí maximálně 2 reléových vstupních karet NX4IN)
	PORUCHA NAPÁJENÍ A NEOPRÁVNĚNÁ MANIPULACE S PANELEM	Ano	Ano
NAPÁJECÍ VSTUPY	VSTUP JEDNOTKY	Power over Ethernet (PoE) 802.3af nebo externí napájení 12 V DC	vstup 93–264 V AC, 50/60 Hz poskytuje výstup 12 V DC, 4 A
	ZÁSUVKA NEBO HARDWAROVÝ STRÍDAVÝ VSTUP	—	Ano
	NAPÁJECÍ VSTUP ŘÍDICÍ DESKY	Power over Ethernet (PoE) nebo napájení 12 V DC	12 V DC z dodaného napájecího zdroje
NAPÁJECÍ VÝSTUPY	NAPÁJENÍ ZÁMKŮ / ZÁPADEK / ČTEČEK / VSTUPNÍCH ZAŘÍZENÍ	450 mA, 12 V DC k dispozici pro západky, čtečky a vstupní zařízení pomocí PoE (Pokud se vyžaduje vyšší proud, externí napájení 12 V DC)	1,15 A na dveře pro zámky / západky, čtečky a vstupní zařízení (3,5 A při celkem 12 V DC)
	SYSTÉM ZÁLOŽNÍ BATERIE	Není součástí dodávky	Baterie 12 V DC, 7 Ah
SKŘÍŇ	MATERIÁL	Nárazuvzdorný plast	Kov
	FYZICKÝ ROZMĚR SKŘÍŇE	197 v x 197 š x 70 h (mm) 7,75" v x 7,75" š x 2,75" h	354 v x 303 š x 120 h (mm) 13,9" v x 11,9" š x 4,7" h
	PŘÍSTUPOVÉ / VYLAMOvací OTVORY KABELÁŽE	7	19
INSTALACE	ODNÍMATELNÉ SVORKOVNICE S BAREVNÝM OZNAČENÍM	Ano	
	GRAFICKÉ KARTY/ŠTÍTKY KABELÁŽE	Ano	
	UPEVNŮVACÍ SPOJOVACÍ MATERIÁL	Ano	
SYSTÉMOVÉ INFORMACE	HODINY REÁLNÉHO ČASU	Globální podpora zeměpisných časových pásem; podpora letního času	
	SYNCHRONIZACE HODIN	Ano: prostřednictvím síťového serveru NTP	
	PROCESOR	Freescale Coldfire 32 bitový	
	SYSTÉMOVÝ STŘEDNÍ ČAS MEZI PORUCHAMI	250 000 hodin	
	TEPLOTNÍ ODOLNOST	Provozní: 0°C až 49°C; Skladovací: -55°C až 85°C	
	CERTIFIKACE A SCHVÁLENÍ	Splňuje požadavky CE a FCC; UL 294	

LEDs	STAVOVÁ KONTROLKA LEDs	12 kontrolkek LED celkem (napájení 12 V, PoE, nadproud, Ethernet, RS-485, čtečky, stav dveří, chod, stav relé)
HOSTITEL	SOFTWAREVÁ KOMPATIBILITA ¹	MAXPRO Cloud, WIN-PAK XE/SE/PE/CS
	NETAXS-123 JAKO PANEL BRÁNY	Podporované následné panely zahrnují NetAXS-123 a NetAXS-4 ^{2,3}
	NETAXS-4 JAKO PANEL BRÁNY	Podporované následné panely zahrnují pouze NetAXS-4 ^{2,3}
	POUŽITÍ KONVERTORU PC13	Podporované následné panely zahrnují NetAXS-123, NetAXS-4, řadu N-1000 a NS2
	POUŽITÍ KONVERTORU N-485-PCI-2	Není kompatibilní
ŘÍZENÍ DVEŘÍ	REŽIMY ŘÍZENÍ DVEŘÍ	Pouze karta, karta a PIN, karta nebo PIN, pouze PIN, uzamčení, deaktivace, supervizor, doprovod, karta s omezeným použitím, expirace k datu, pravidlo první karty, pravidlo dne sněžení, přepnutí časového pásma, ochrana před předáváním karty, nátlak ⁴
	BLOKOVACÍ ZÁMKY PRO AKCE ZÁKAZNÍKA	Ano
	OCHRANA PŘED PŘEDÁVÁNÍM KARTY	Místní a globální schopnosti; implementace hardwaru a softwaru
KARTY A DATABÁZE	KAPACITA KARTY A VYROVNÁVACÍ PAMĚTI UDÁLOSTÍ	kapacita 10 000 karet; kapacita 25 000 událostí;
	VERZE FIRMWARU	Integrovaná paměť Flash pro aktualizaci firmwaru a rozšíření funkcí
	K DISPOZICI OFFLINE ZÁLOHA DATABÁZE	Databáze karty a konfigurační databáze
	SCHOPNOSTI EXPORTU	Databáze karty, alarmy a události (formát CSV) ⁴
	POČET FORMÁTŮ KARET	lze podporovat 128 jedinečných formátů karet ⁴
	KÓDY LOKALITY	8
	MAXIMÁLNÍ VELIKOST FORMÁTU KARET	75 bitové (maximální počet karta = 64 bitů) ^{4,5}
	ČASOVÁ PÁSMA	127 ⁴
	ÚROVNĚ PŘÍSTUPU	128
	SVÁTKY	255 ⁴
ZPRÁVY A ANALÝZY	INTEGROVANÉ ZÁKLADNÍ ZPRÁVY	Ano
	IMPORT/EXPORT DATABÁZE KARET	Ano
	EXPORT ALARMU/UDÁLOSTI	Ano
WEB	PODPORA PROHLÍZEČŮ	Google Chrome
GLOBÁLNÍ	PODPORA JAZYKŮ	angličtina, francouzština, němčina, holandská, italština, španělština, čeština, zjednodušená čínština, arabština

5 SOFTWARE PRO SPRÁVU PŘÍSTUPOVÉHO SYSTÉMU WIN-PAK

V současné době se aplikace pro správu přístupového systému nabízí v několika verzích:

- WPX4 (WIN-PAK XE)
 - Jen EKV pro jednotky NetAXS-123, NetAXS-4 a NS2.
 - Všechny funkce jako „velký“ WIN-PAK, pro 1 operátora.
- WPS4 (WIN-PAK SE, 1-uživatelský)
 - Bez účtů, v 1 okamžiku přihlášený jen 1 operátor.
 - Podpora základních funkcí CCTV (integrace).
 - Podpora ústředny PZTS Galaxy jen s licenčním rozšířením (verze WPS4G).
- WPS4U5A (WIN-PAK SE, 5-uživatelský)
 - Bez účtu, v jednom okamžiku přihlášených až 5 operátorů.
 - Kompletní podpora integračních funkcí CCTV,
 - Podpora ústředny PZTS Galaxy s licenčním rozšířením (verze WPS4U5GA).
- WPP4 (WIN-PAK PE, neomezený počet uživatelů)
 - Podpora dělení karet a držitelů do účtů.
 - Kompletní podpora integračních funkcí CCTV a ústředny PZTS Galaxy.[6]



Obr. 12 – Verze a návaznosti WIN-PAK.[6]

Konfigurace WIN-PAK SE/PE

1. Účty (jen ve WPP4/WIN-PAK PE).

- Dělí karty, držitele karet do logických skupin.
- Každý operátor má práva jen k vybraným účtům.
- Musí existovat alespoň jeden účet pro práci s kartami.

[menu] **Účet > Editovat**

Údaje závislé na účtu:

- | | |
|--------------------------|------------------------------|
| - karty | [jen v 1 účtu] |
| - držitelé karet | [jen v 1 účtu] |
| - časové zóny | [v libovolné kombinaci účtů] |
| - přístupové úrovně | [v libovolné kombinaci účtů] |
| - poznámková pole | [jen v 1 účtu] |
| - návrh průkazu (potisk) | [jen v 1 účtu] |

2. Časová nastavení

- Nejčastěji – Časové zóny.
- Event. Grupy svátků.
- Event. Grupy pro letní čas.

[menu] **Konfigurace > Časová nastavení**

Časová zóna musí být definována alespoň jedna pod jeden účet.

Grupy svátků jsou vhodné, uvažuje-li uživatel se zvláštními přístupovými režimy pro vybrané dny.[6]

3. HW zařízení

- Veškeré chování jednotek se určuje pomocí Mapy zařízení.
- Struktura zadávání musí odpovídat skutečnému zapojení:
 - typicky Komunikační server > Převodník > Jednotky[6]

[menu] **Konfigurace > Zařízení > Mapa zařízení**

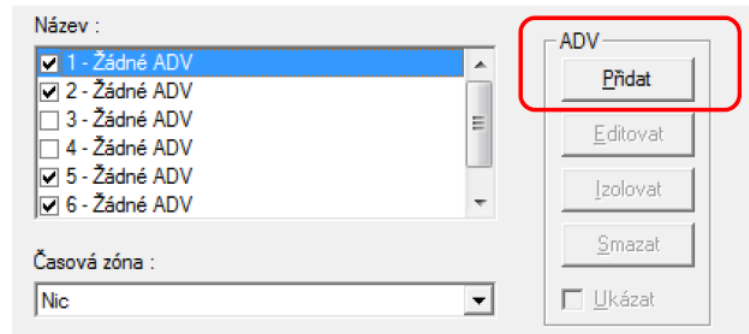
U definice jednotky je nutné vždy přiřadit alespoň jednu časovou zónu, protože jinak by nebylo možné čtečky jednotky nastavit v přístupových úrovních.

4. HW zařízení – ADV

- Každé samostatné zařízení musí mít přiřazeno ADV (Abstract DeVice) – abstraktní zařízení.

Jedná se o: panel, převodník, čtečku, vstup, výstup, server atd.[6]

Pokud je u zařízení dostupná ikona ADV > Přidat, pak stačí potvrdit volbu Přidat a volbu potvrdit kliknutím na OK:



Obr. 13 – Přiřazení ADV zařízení.[6]

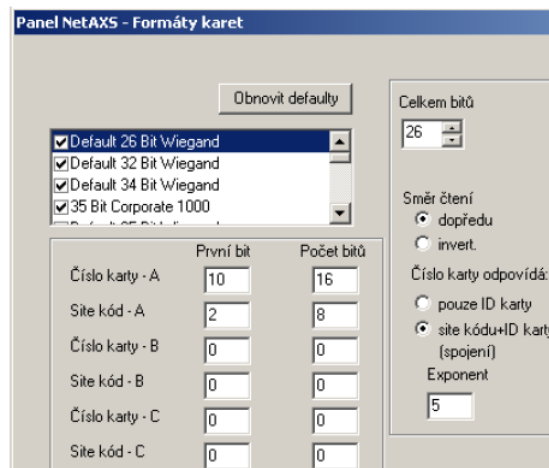
- ADV = „zástupce“ prvku pro jeho monitoring ve WIN-PAKu.
 - ADV určuje, jak se bude prvek ve WIN PAKu zobrazovat / jevit.
 - Definuje jméno, pod kterým se bude prvek zobrazovat.
 - Neurčuje chování dotyčného hardwarového prvku.
 - Přiřazuje prioritu událostem, které může prvek generovat.
 - 1 nejvyšší priorita.
 - 49 poslední priorita zobrazovaná v alarm monitoru.
 - 79 poslední priorita zobrazovaná v monitoru událostí.
 - 99 nejnižší priorita (jen zápis do dB).
 - 0 událost se nebude ve WP vůbec zobrazovat ani ukládat do dB.
 - Chování lze filtrovat přes časovou zónu.
 - Lze nechat přehrát zvukový soubor při události.
 - Lze spustit tzv. soubor příkazů při události (příkaz do HW).
 - Lze odeslat mail při události.[6]
- Chování prvku se přenáší přes tzv. akční grupu na další prvky stejného typu.
 - Všechny ADV se stejnou akční grupu budou sdílet stejné nastavení.
 - Změna jednoho parametru u jednoho ADV se přes akční grupu promítne do všech ostatních ADV s touto grupou.

- Lze vytvářet vlastní (nové) akční grupy pro uživatelsky definované skupiny ADV.
 - Libovolné ADV může mít přiřazenu akční grupu „Uživatelská“; pak chování definováno jen pro tento jeden prvek.
 - V ADV lze definovat tzv. výchozí mapu.
 - Mapa, která se bude po kliknutí z alarm monitoru automaticky otevírat.
- [6]

5. Nastavení formátu karet.

- Pro NetAXS-123

lze definovat i vlastní formát spojením SC a ID karty (exponent), například pro Wiegand 26b: exponent = 5.



Obr. 14 – Nastavení formátu karet pro NetAXS-123.[6]

6. Umístění ADV do map sledovaných oblastí.

- Nepovinné, jen pro sledování pohybu osob v libovolných oblastech.
- Každá oblast určena vstupní čtečkou / vstupními čtečkami.
- Lze vytvářet i vnořené oblasti (objekt > 1.p. > pravé křídlo ...).
- Oblasti nemusejí odpovídat fyzickému uspořádání.
- Nepoužité oblasti automaticky v oblasti „Exit:čtení“.[6]

[menu] **Konfigurace > Definice > Sledování oblastí**

7. Umístění ADV do map podlaží.

- Nepovinné, pro grafický monitoring dění v systému.
- „Pevný“ mapový podklad ve vektorech wmf, emf.
- Na něm ikony ADV vybraných prvků.

- Libovolná velikost ikon, natočení, definice barevných stavů, blikání ...
- Možné i odkazy na další mapy podlaží.[6]

Správa uživatelů ve WIN-PAK SE/PE

1. Definice přístupových úrovní.

- Určují kam se osoby (karty) s určitou úrovní oprávnění dostanou a kdy.
- Seznam povolených čteček; na každé povolená časová zóna.
- Čtečky lze povolovat i skupinově přes složku
- Přístupové úrovně vždy přiřazeny pod libovolnou kombinaci účtů, přístupové úrovně lze „sdílet“ napříč více účty.
- Funkce kopírování přístupových úrovní usnadní vytváření podobných oprávnění.
- Funkce izolování přístupových úrovní umožní rychle zjistit, kdo má jakou přístupovou úroveň přidělenou a hromadně kartám přidělit jinou přístupovou úroveň (a volnou pak event. smazat).[6]

[menu] **Karty > Přístupové úrovně**

2. Definice karet.

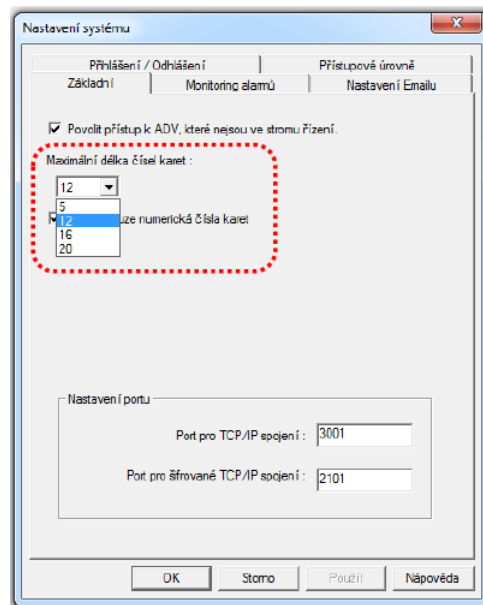
Nově jsou u NetAXS zavedeny pole pro omezený počet použití karty a dočasná platnost karty. Dále je u karty možné nastavit typ: Standard/Supervisor/VIP:

- Supervisor = otevírá i dveře v režimu Supervisor („zamknuto“ pro karty typu Standard); sám sobě může autorizovat přístup v režimu Eskort.
- VIP = otevírá i dveře v režimu Supervisor („zamknuto“ pro karty typu Standard); prochází standardně i dveřmi v režimu Eskort.
- Určení Číslo karty je povinné.
- Stav karty aktivní/ neaktivní/ ztracená/ odcizená je povinný.
- Určení Přístupové úrovně je povinné.
- Přiřazení Držiteli karty je nepovinné.
- Zadání PINu je nepovinné.
- Datum expirace je nepovinné.
- Akční grupa karty (zvláštní chování vybrané karty) je nepovinná.
- Přiřazení Průkazu pro potisk karty (líc / rub) je nepovinné.

[menu] **Karty > Karty**

- Určení maximální délky čísla karty – 5/ 12/ 16.[6]

[menu] **Systém > Nastavení systému**



Obr. 15 – Určení maximální délky čísla karty.[6]

3. Definice držitelů karet.

- Jméno, Příjmení jsou povinné.
- Volitelná poznámková pole (rozdělená na libov.záložkách) jsou nepovinné.
 - Definice poznámk.polí přes Konfigurace > Držitelé karet > Položky pro pole poznámek a> Záložky pro držitele karet.
 - Až 40 poznámkových polí , lze zadávat masky (filtry) polí.
- Přiřazení Karet nepovinné
 - Každá osoba může mít neomezený počet karet.
 - Přidání = zadání nové (zatím neexistující) karty s nastavením parametrů.
 - Připojení = navázání záznamu již existující karty k osobě.
- Biometrické parametry karty nepovinné
 - Fotografie (lze až 99 fotografií k držiteli).
 - Fotografie lze importovat ze souboru (+ořez, komprese) nebo zachycovat „živě“ z kamery.
 - Naskenovaný podpis držitele.[6]

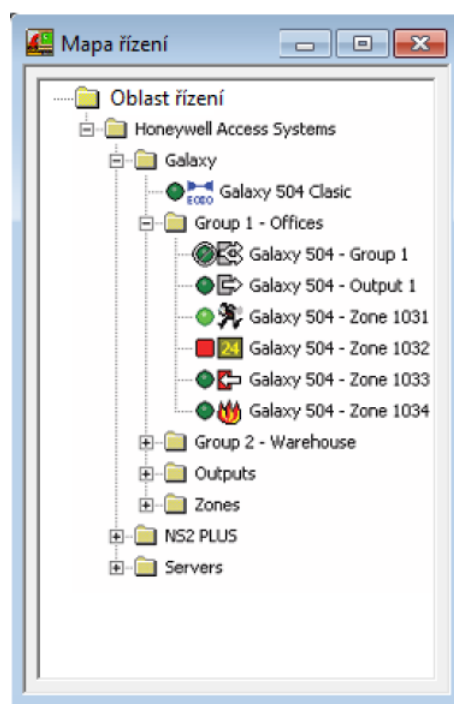
[menu] **Karty > Držitelé karet**

Monitoring ve WIN-PAK SE/PE

1. Přehledový monitoring – Mapa řízení.

- Zobrazuje ikony prvků (ADV) ve složkách definovaných Oblastmi řízení.
 - Zelené kolečko = klidový stav.
 - Červený čtvereček = alarmový stav.
 - Žlutý trojúhelník = tamper (sabotáž).
 - Přeškrtnutí = přemostěno.
 - Otazník = neznámý stav.
 - Světlý odstín = nepotvrzená změna.
 - Tmavý odstín = žádná změna od smazání.
- Umožňuje i ovládání prvků.
 - Pravé tlač. myši = dostupné operace.
 - Inicializace panelů.[6]

[menu] **Ovládání > Mapa řízení**



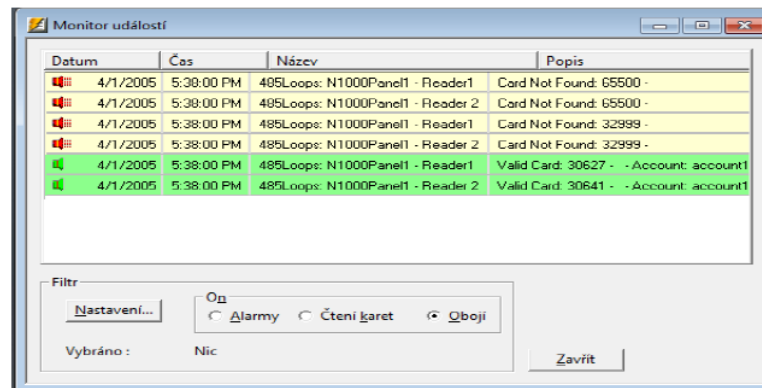
Obr. 16 – Přehledový monitoring ve WIN-PAKu.[6]

2. Textový monitoring – Monitor událostí.

- Detailní přehled o čase / místě / původci apod. události.
 - Jen chronologické řazení událostí.
 - Zobrazení událostí s prioritou < 80.
 - Zavření okna = smazání přehledu.

- Možné filtrování zařízení ADV.[6]

[menu] **Ovládání > Události**

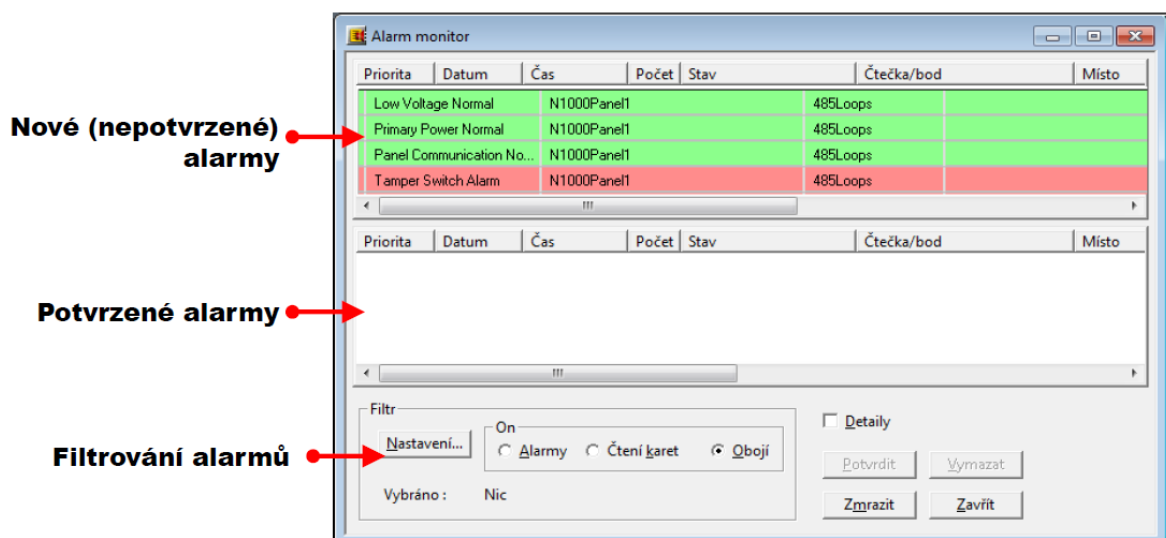


Obr. 17 – Textový monitoring ve WIN-PAKu.[6]

3. Textový monitoring – Alarm monitoring.

- Detailní přehled o čase / místě / původci apod. události
 - +Razení událostí dle priorit.
 - Zobrazení událostí s prioritou < 50.
 - Potvrzování/ mazání alarmů/ připojování poznámek.
 - Zavření okna = přehled zůstává.
 - Možné filtrování zařízení ADV.
 - Detaily = info o změnách stavu prvku v čase.[6]

[menu] **Ovládání > Alarmy**



Nové (nepotvrzené) alarmy

Potvrzené alarmy

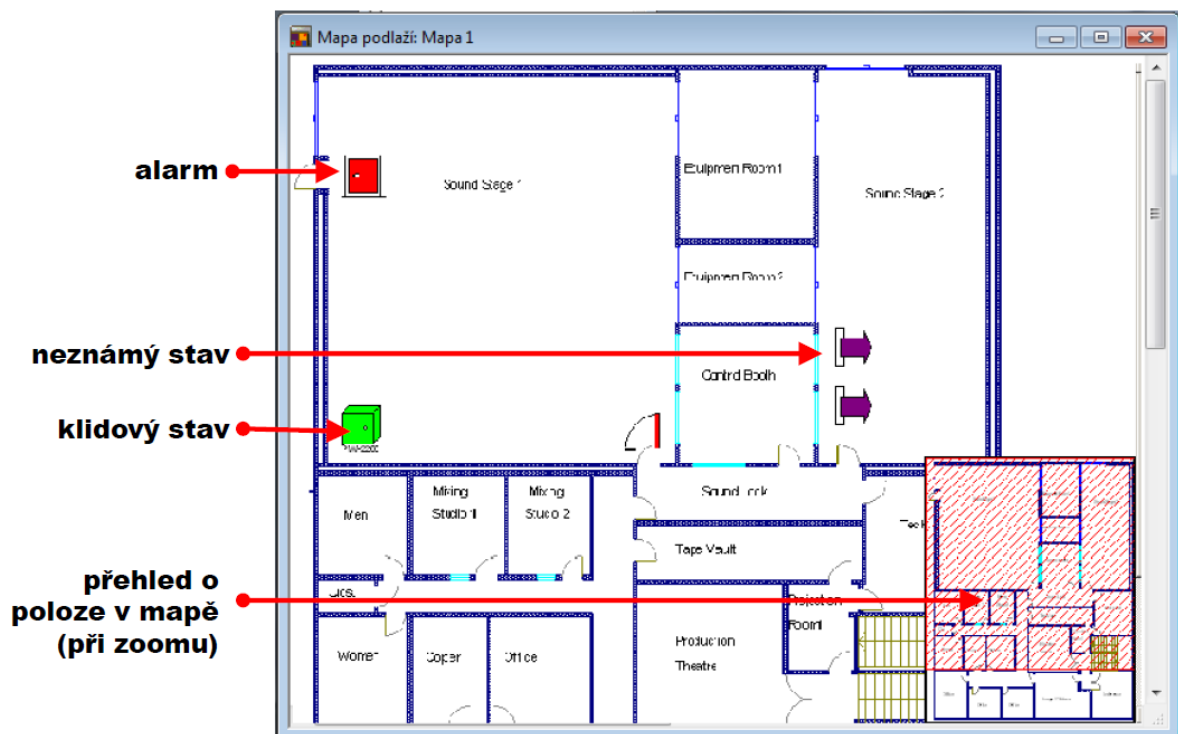
Filtrování alarmů

Obr. 18 – Alarm monitoring ve WIN-PAKu.[6]

4. Grafický monitoring – Mapy podlaží.

- Přehled o stavu prvků a místě vzniku alarmu
 - Možnost otevření přes Výchozí mapu z Alarm monitoru.
 - Barvy a stavy jako u Mapy řízení.
 - Navíc: blikání = alarmový stav.
 - Dveře ikona signalizuje stav dveří (otevřeno/ zavřeno).
 - Monitoring a ovládání prvků (přes pravé tlačítko myši).
 - Zoomování, rychlý přehled o poloze v celkové mapě.
 - Linky pro otevírání návazných map.[6]

[menu] **Ovládání > Mapa**



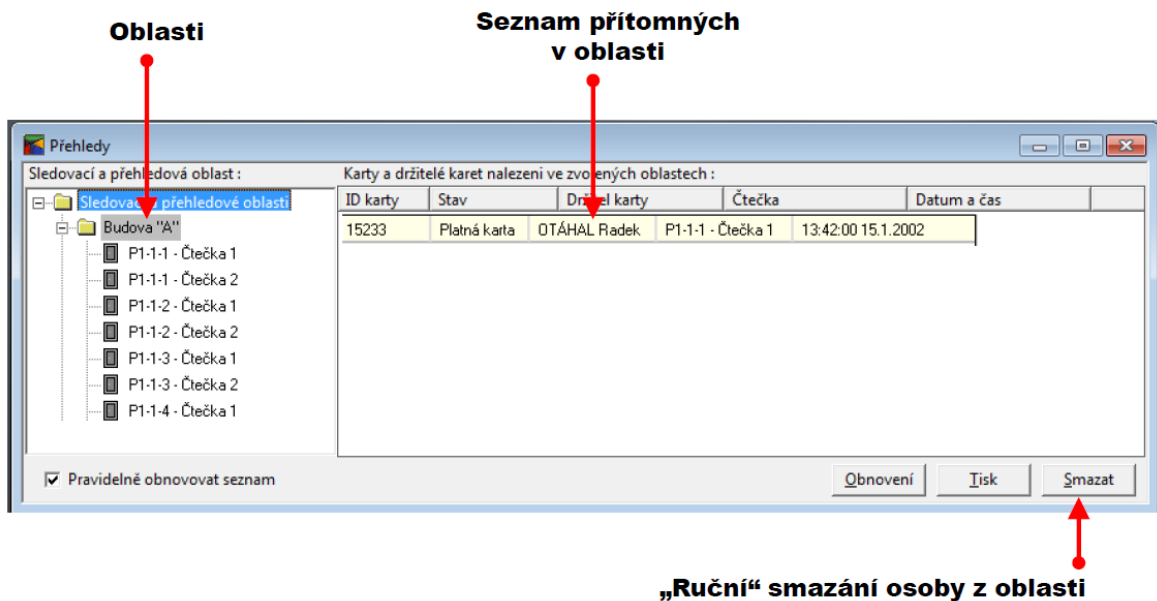
Obr. 19 – Grafický monitoring ve WIN-PAKu.[6]

5. Monitoring pohybu osob – Přehledy a sledování.

- Přehled o aktuální poloze osob podle posledního čtení karty.
 - Automatická aktualizace.
 - Součty osob v oblastech.
 - Jmenný seznam přítomných v oblasti.
 - Sdružený přehled v nadoblastech.
 - Funkce shromažďovací čtečky při evakuaci, shromažďovací.
 - čtečka maže přítomnost v předchozích oblastech.

- U WIN PAKu 4.1 — „jednotlačítkový“ report o osobách v objektu.[6]

[menu] **Ovládání > Sledování a přehledy**



Obr. 20 – Monitoring pohybu osob ve WIN-PAKU.[6]

6. Zobrazování fotografií při průchodech.

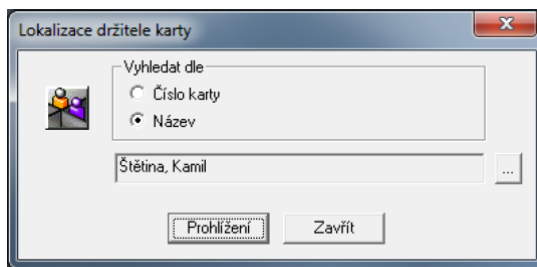
- Vizuální verifikace oprávněných držitelů karet.
 - Výběr čteček, z nichž se mají fotky zobrazovat.
 - Nastavení priority čtení (např. zobrazení jen zájmových osob).
 - Možnost zobrazování textových poznámek.[6]

[menu] **Ovládání > Automatické zobrazení karty**

7. „Textová“ lokalizace osoby.

- Vyhledání místa přítomnosti osoby.
 - Podle posledního načtení karty.
 - Vyhledávání podle čísla karty nebo jména osoby.
 - Vypsání oblastí, v níž je osoba přítomna.[6]

[menu] **Ovládání > Lokalizace držitele karty**



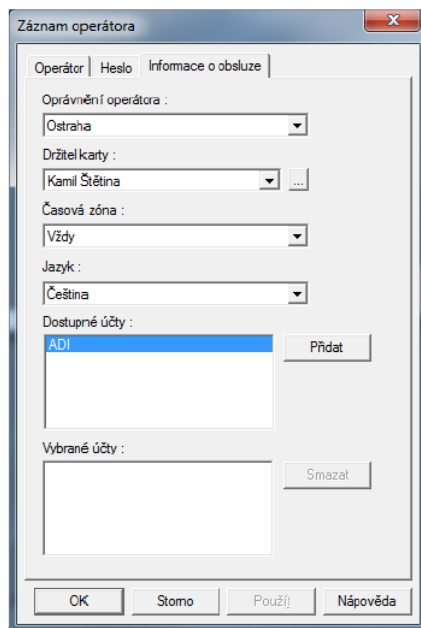
Obr. 21 – Lokalizace držitele karty ve WIN-PAKu.[6]

Obsluha ve WIN-PAK SE/PE

1. Operátoři, oprávnění obsluhy.

- Operátoři
 - Jméno, heslo.
 - Nastavení jazyka uživatelského rozhraní (nastaven při přihlášení).
 - Přihlašování operátorů lze omezovat časem.
 - Přístup jen k vybraným účtům (a tím i jen k určeným kartám a držitelům).
 - Práva ve WIN PAKu definována profilem
 - operátora (Oprávnění operátora).[6]

[menu] Ovládání > Lokalizace držitele karty

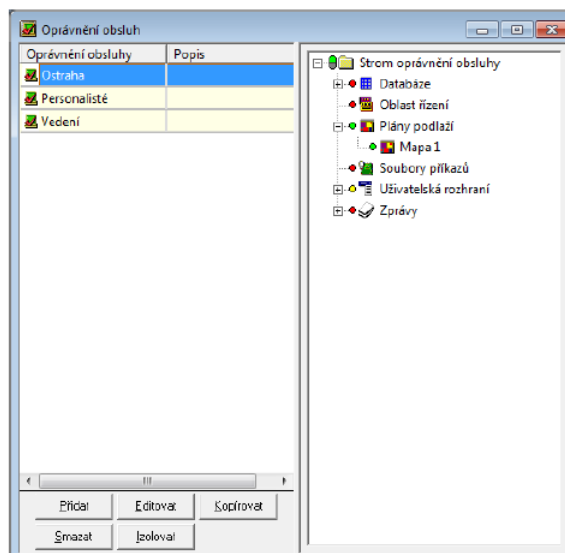


Obr. 22 – Záznam operátora ve WIN-PAKu.[6]

- Možnost přihlašování operátora doménovým profilem.
 - Využití Active Directory.

- Nelze pak definovat „standardní“ operátory.
- UAC potlačení UAC dialogu při spuštění klienta.
 - System Manager , Service Manager a Backup & Restore stále chráněny.
- Oprávnění obsluhy.
 - Definice co kdo může provádět v rámci WIN-PAKu.
 - Určení práv k tabulkám databáze (nic/ prohlížení/ editace/ mazání).
 - Určení práv k zařízením (nic/ prohlížení/ ovládat).
 - Určení práv k ovládacím prvkům programu (alarmy, události, mapy...).
 - Jeden profil oprávnění může sdílet více operátorů.[6]

[menu] **Ovládání > Lokalizace držitele karty**



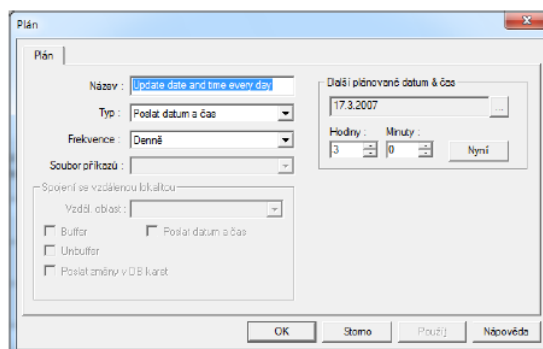
Obr. 23 – Oprávnění obsluhy ve WIN-PAKu.[6]

Speciální funkce ve WIN-PAK SE/PE

1. Automatické akce – Plány.
 - Definice akcí, které se mají automaticky spouštět.
 - Nutný nadefinovaný server plánů ve WIN PAKu.
 - Typy plánů / realizované úlohy.
 - Aktualizace data&času na jednotkách.
 - (De)aktivace karet.
 - (De)aktivace spec.příst.úrovní.

- Generování zprávy ze šablony.
- Report o četnosti použití karet.
- Zálohování dB (jen pro MS SQL Express).[6]

[menu] **Konfigurace > Časová nastavení > Plány**



Obr. 24 – Plán ve WIN-PAKu.[6]

- WIN-PAK 4.x.
 - Automatické smazání historie starší než xx dnů.
 - xx – nastavitelné od 1 do 999.
 - Plán „Purge History“.[6]
- 2. Podpůrné nástroje – Potisk karet.
 - Vytvoření šablony pro potisk karet.
 - „Pevné“ položky, proměnné položky.
 - Vazba na údaje z databáze (jméno, č. karty...).
 - Možný jiný návrh pro líc, jiný pro rub karty.
 - Potisk karet
 - jednotlivý i hromadný potisk.[6]

[menu] **Konfigurace > Průkaz > Návrh průkazu**

3. Podpůrné nástroje – Obchůzky.
 - Kontrola obchůzkové činnosti strážných s využitím prvků EKV.
 - Automaticky (plány) i ručně spouštěné obchůzky.
 - Sekvencované i nesekvencované obchůzky.
 - Hlídní brzkého/ pozdního příchodu , vynechání kontrolního bodu.
 - Využití (alarmových) vstupů na jednotkách a/nebo čteček.[6]

[menu] **Konfigurace > Obchůzka**

Systémová nastavení ve WIN-PAK SE/PE

1. Nastavení systému.

- Obecné nastavení práce s kartami.
- Pravidla pro zobrazování a obsluhu alarmů.
- Definice emailových adres pro automatické mailování.
- Určení typu přístupových úrovní (konkrétní/ vícenásobné).
- Definice TCP portů pro komunikaci s jednotkami.
- Pravidla pro přihlašování/ odhlašování.[6]

[menu] **Systém > Nastavení systému**

2. Nastavení pracovní stanice.

- Nastavení počtu zobrazovaných záznamů v tabulkách.
 - Důvod „ztráty“ (nezobrazení) karet / osob při velkém počtu záznamů.
- Nastavení tapety hlavního okna WIN PAKu , zvuků/ adresářů.
- Nastavení pravidel pro potvrzení mazání.
- Nastavení pravidla pro odpojování klientů při nečinnosti.
- Nastavení ukládání pozice oken/ obnovování oken.[6]

[menu] **Systém > Nastavení pracovní stanice**

Servisní nástroje ve WIN-PAK SE/PE

1. Údržba databáze.

- Odstranění smazaných záznamů.
 - Fyzické smazání záznamů, které byly doposud jen označeny jako smazané.
- Smazání historie.
 - Odstranění údajů z tabulky Historie do určitého data.
 - Spuštěno vždy ručně.
 - Doporučeno provádět jednou za čas, aby dB nebyla příliš velká.[6]

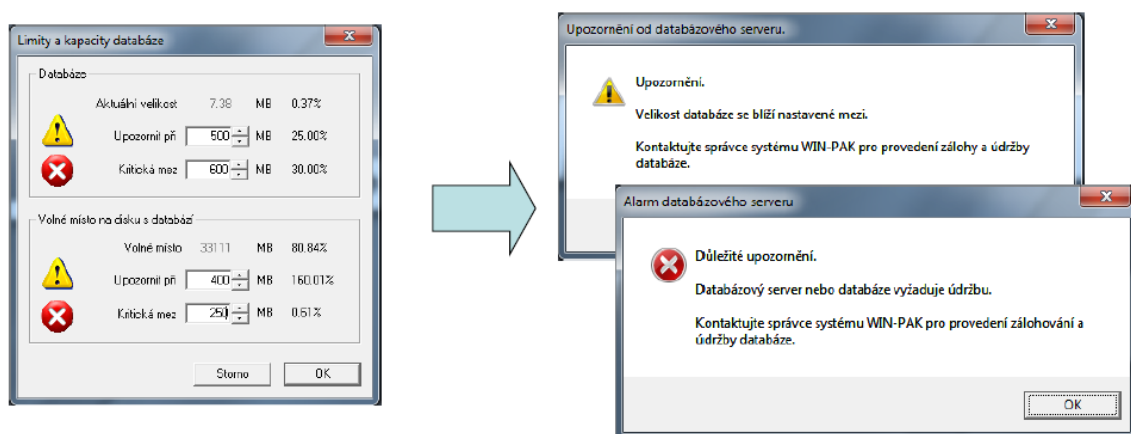
[menu] **Soubor > Údržba databáze**

2. Kapacita a limity databáze.

- Automatické hlídání velikosti databáze.
 - Mez pro upozornění, kritická mez.

- Automatické hlídání volného místa na HDD.
 - Mez pro upozornění, kritická mez.

Při spuštění WIN PAKu (kterýkoliv klient) zobrazeno varování.[6]



Obr. 25 – Hlídání velikosti databáze ve WIN-PAKu.[6]

[menu] **Soubor > Kapacita a limity databáze**

3. Import dat.

- Externí utilita pro rychlý import osobních dat do databáze.
 - Parametry držitelů karet (včetně poznámkových polí), parametry karet.
 - Import fotografií.
 - Vše v jednom souboru.
 - Import z .xls nebo .csv souboru.
 - Libovolné pořadí sloupců.[6]

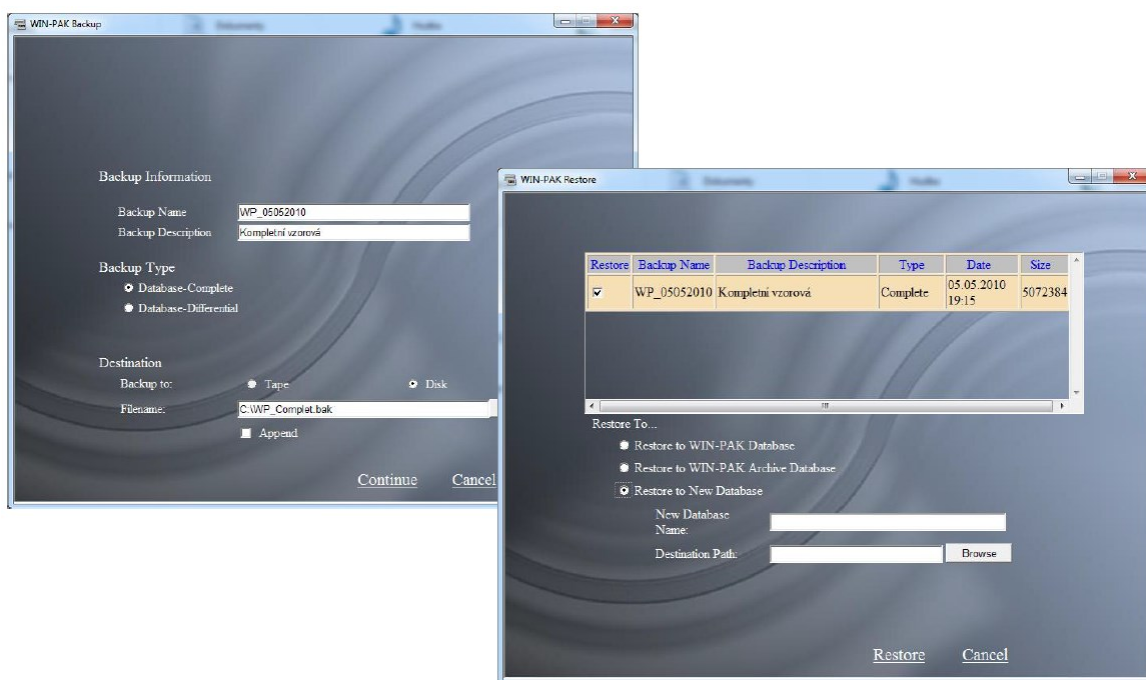
WIN-PAK Import Utility

4. Zálohování/ obnova dat.

- Externí utilita pro snadné zálohování/ obnovu dat ze zálohy.
- Zálohování (Backup & Schedule).
 - Nastavení typu zálohy (kompletní/ rozdílová).
 - Nastavení přepisování souboru/ připojování do stejného souboru.
 - Definice četnosti spuštění.
 - Plán zálohy uložen v SQL/ MSDE jako tzv. job.
 - Není dostupné, pokud je MS SQL 2008 Express (potom automaticky zálohování přes plány).[6]
- Obnova dat ze zálohy (Restore).

- Výběr zálohy k obnově.
- Určení databáze, která se má přepsat (pracovní/ archivní/ nová).
- Před obnovou vždy nutno zastavit všechny služby (servery) WIN PAKu.
- Změna plánu (periody) zálohování (Modify Schedule).[6]

WIN-PAK Backup and Restore Utility



Obr. 26 – Zálohování a obnova dat ve WIN-PAKu.[6]

6 VÝSTUPNÍ ZAŘÍZENÍ

Výstupním zařízením je zpravidla myšlen aktivátor, elektricky ovládaný zámkový mechanismus, který slouží k bezpečnostnímu zajištění místa přístupu. Současně v návaznosti na bezpečnost nebo integraci slaboproudých bezpečnostních systémů, může přiložení identifikačního média k zařízení rozhraní uživatele vyvolat i jinou odezvu přístupového systému, například zastřežit zabezpečenou oblast nebo nastavit příslušnou otočnou kameru do definované přednastavené pozice a vytvořit snímek nebo zaslat informační zprávu o změně stavu místa přístupu.

Při návrhu správného bezpečnostního výstupního zařízení typu elektrický nebo elektromagnetický nebo magnetický zámek je nutné v první řadě vycházet z norem, které řeší požární bezpečnost staveb a únikové cesty (ČSN 73 0802, ČSN 73 0804, ČSN 73 0810 a další). Pokud se na zabezpečované dveře nevztahuje žádné omezení z hlediska požárně bezpečnostního řešení (PBR) objektu, pak je lze zabezpečit libovolným vhodným bezpečnostním elektricky ovládaným zámkem a ovládat jej systémem EKV. Typ zámku je nutné volit s ohledem na uvažovaný počet denních průchodů.

6.1 Elektromagnetické zámky

Elektromagnetické zámky zajišťují základní elektrické ovládání zabezpečených dveří. Způsob zajištění spočívá v přidržení, resp. uvolnění střelky zámku. Instalují se do zárubně. Pro jejich správnou funkci nesmí být dveře uzamčené. V základním provedení se připojují do systému EKV dvěma vodiči, do nichž je systémem EKV při autorizaci žádosti o průchod přivedeno napájení a elektromagnetický zámek na definovanou dobu uvolní průchod dveřmi. Zámky mohou být vybaveny mikrospínačem pro signalizaci stavu dveří: otevřeno/ zavřeno do systému EKV, ovšem tento způsob sledování stavu dveří je možné jednoduchým způsobem obejít. Určité celooceľové provedení zámků splňuje požadavky pro instalaci do požárních dveří.



Obr. 27 – Elektromagnetický zámek DORCAS.[Zdroj: vlastní]

6.2 Ostatní zámky

Na trhu je v současné době k dispozici velké množství různých elektricky ovládaných zámků, od elektromechanických samo-zamykacích s kováním klika – klika, přes elektromotorické zámky s kováním klika – koule, až po přídržné magnety, kde může být kování typu klika – klika nebo v kombinaci s elektromagnetickým zámkem kování koule – koule.



Obr. 28 – Elektromechanický zámek EL460 (vlevo) a přídržný magnet V3SR (vpravo).[Zdroj: vlastní]

7 KOMUNIKAČNÍ ROZHŘANÍ

Jedná se o rozhraní, prostřednictvím kterého komunikuje řídicí jednotka přístupového systému s řídicím počítačem nebo serverem. V současné době je běžným standardem propojení lokálních řídicích jednotek prostřednictvím LAN a globální propojení prostřednictvím Internetu. Zpravidla se takto propojují i řídicí jednotky přístupového systému, které jsou vybavené pro komunikaci přes sběrnici RS-232 nebo RS-485 (EIA-485), kde se tato sběrnice pomocí LAN převodníků přizpůsobuje komunikaci pomocí protokolu TCP/IP. Přejít na komunikaci prostřednictvím LAN je způsoben, že většina současných počítačů a počítačových serverů je vybavena rozhraním pro připojení k LAN, resp. ethernetu.



Obr. 29 – Převodník RS-485 na Ethernet VESP211-485.[Zdroj: vlastní]

II. PRAKTICKÁ ČÁST

8 NÁVRH PŘÍSTUPOVÉHO SYSTÉMU

Při návrhu a realizaci přístupového systému vychází řešitel z aktuálního požadavku zadavatele na zvýšení bezpečnosti v daném objektu nebo souboru objektů. Návrh by měl vycházet především z bezpečnostního auditu a dále z požadavků a představ uživatele na provoz a řízení pohybu osob v objektu.

Důležitými vstupními veličinami pro správný, funkční a bezpečný systém EKV jsou:

- Počet zabezpečených vstupních (případně i výstupních) míst.
- Počet entit, které se budou pohybovat v zabezpečených prostorách (například: zaměstnanci a návštěvy).
- Míra akceptovatelného bezpečnostního rizika (bezpečnostní opatření snižují míru rizika, nikdy však míra rizika nebude nulová).

Návrh konkrétního HW a SW vybavení pak musí akceptovat výše uvedené body. Současně je vhodné, aby byl systém EKV koncipován s rezervou minimálně 20% co do počtu zabezpečených vstupních míst tak počtu osob, které budou systém používat. Z parametrů systému EKV jsou zásadní:

- Kapacita navrhovaného systému EKV (počet vstupních míst, počet osob).
- Počet přístupových a časových zón (musí odpovídat kapacitě systému).
- Spolehlivost systému EKV.
- Kompatibilita produktů v časové ose
- Dostupnost a zastupitelnost služeb spojených s provozem EKV.

9 DEMONSTRAČNÍ PANEL

Pro ilustraci možností, které nabízí on-line přístupový systém výrobce Honeywell, byl vytvořen demonstrační panel s řídicí jednotkou NetAXS-123 v provedení NX1P pro řízení jednoho vstupního místa. Demonstrační panel byl sestaven a zapojen dle obrázku 30.



Obr. 30 – Demonstrační panel s řadičem NetAXS-123 typ NX1P.[Zdroj: vlastní]

Specifikace komponent

Pro sestavení a zapojení byly použity komponenty.

- Řídicí jednotka přístupového systému – NetAXS-123, typ NX1P.
- Vstupní čtecí zařízení – bezkontaktní čtečka iCLASS SE R10.
- Snímač stavu vstupního místa – magnetický kontakt MAS303.
- Aktivátor – elektrický zámek s válcovou západkou ELC12D3V (odběr 1,2A).
- Napájecí zdroj pro zámek – CIRCO LED 12VDC 0 – 15W.
- Signalizace výstupu AUX – LED žlutá.
- Odchodové tlačítko – mini kolíbkový spínač.

- Aktivní prvek komunikačního rozhraní – Switch TPE-50S, 5 portů 10/100Mbps, (4x PoE, 1x bez PoE), kapacita 1Gbps, 31W, kov
- Identifikační médium – bezkontaktní karta Mifare 13,56MHz, 5ks

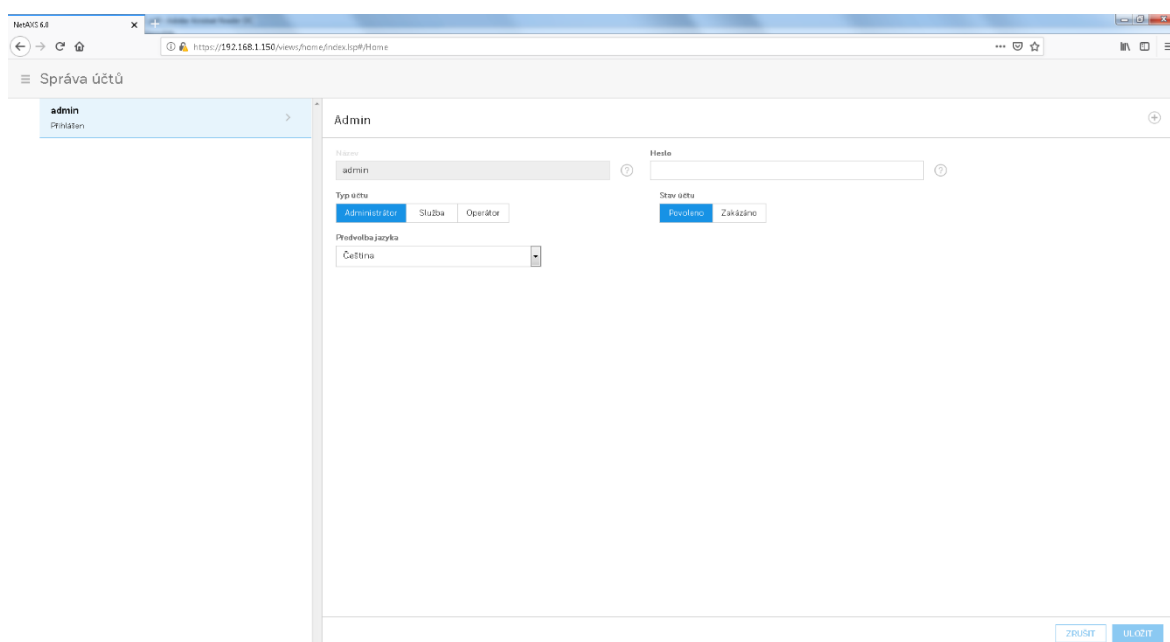
Komponenty jsou zapojené k řídicí jednotce přístupového systému NetAXS-123 dle doporučení výrobce, viz popis v teoretické části diplomové práce. Řídicí jednotka přístupového systému NX1P je nastavena pro jedno vstupní místo řízené jednostranně, druhá strana je řízena odchodovým tlačítkem. Propojky pro způsob ovládání elektrického zámku jsou nastavené pro externí napájecí zdroj a typ kontaktu NO (v klidu uzamčeno). Typ zámku je zvolen s ohledem na dobrou demonstrační vizualizaci aktivace – válcová západka se ze tří čtvrtin zasune do těla zámku a tento pohyb je doprovázen silným akustickým signálem, současně opětovné uvedení zámku do klidové pozice je velmi dobře slyšitelné.

10 KONFIGURACE NX1P

10.1 Konfigurace přes webový prohlížeč

Jedná se o způsob konfigurace, kterou řídicí jednotka přístupového systému umožňuje. Zařízení NX1P je s aktuálním firmware NetAXS 6.0.

Webserver řídicí jednotky NX1P umožňuje nastavit několik jazyků. Defaultním nastavením je angličtina, v nabídce Account (Správa účtů) v záložce Admin je možné jazyk změnit. Jazyková sada obsahuje češtinu.



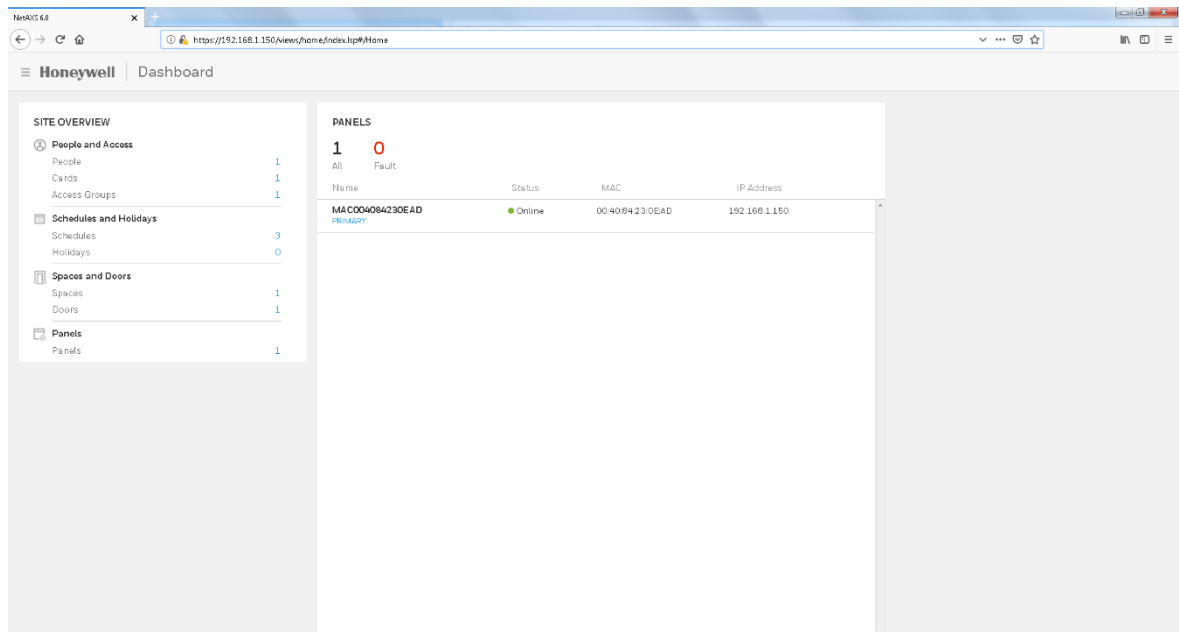
Obr. 31 – Správa účtu, změna jazyka přes webový prohlížeč. [Zdroj: vlastní]

Po nastavení příslušných IP adres a přihlášení se k webserveru zařízení se zobrazí úvodní stránka.

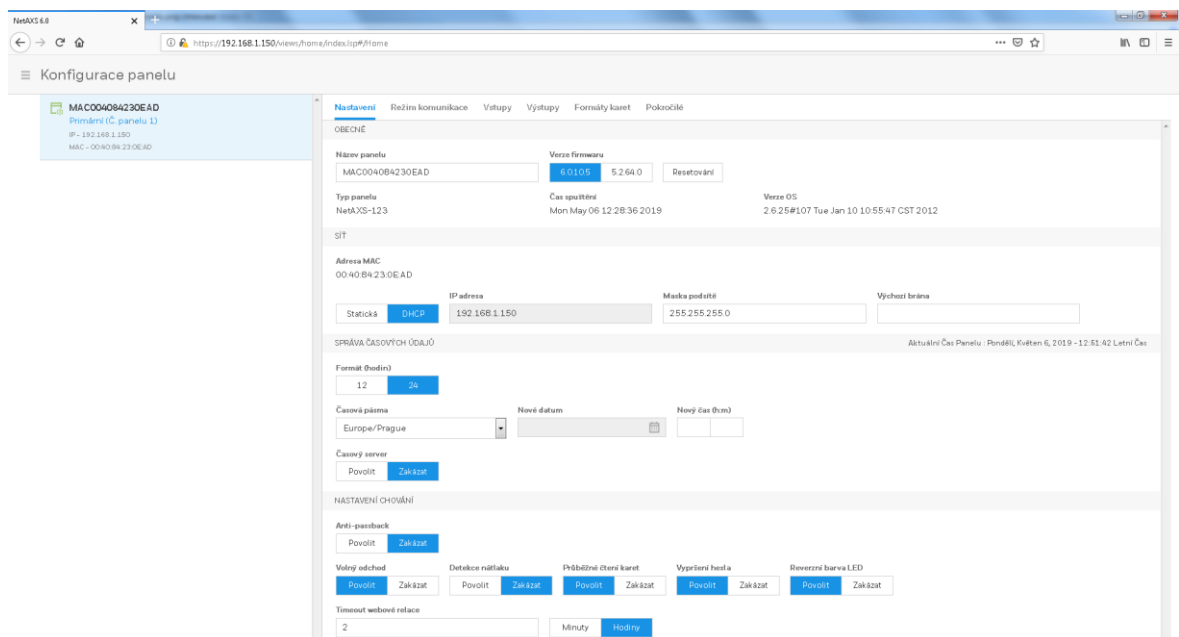
Jako první byl nastaven způsob komunikace řídicí jednotky přístupového systému NX1P s počítačem.

Ve druhém kroku je nutné nastavit čas, resp. nastavení hodin v řídicí jednotce NX1P na místní čas.

Tip: Každá změna v příslušné obrazovce musí být uložena. K tomu slouží volba „Uložit“ na obrazovce vpravo dole. Pokud není volba viditelná, použijte pro posun kurzoru v aktuálním okně klávesu tabelátoru, dokud se kurzor nenastaví na volbu pro uložení změn.



Obr. 32 – Úvodní stránka konfigurace NX1P přes webový prohlížeč. [Zdroj: vlastní]



Obr. 33 – Konfigurace řídicí jednotky, nastavení komunikace a času. [Zdroj: vlastní]

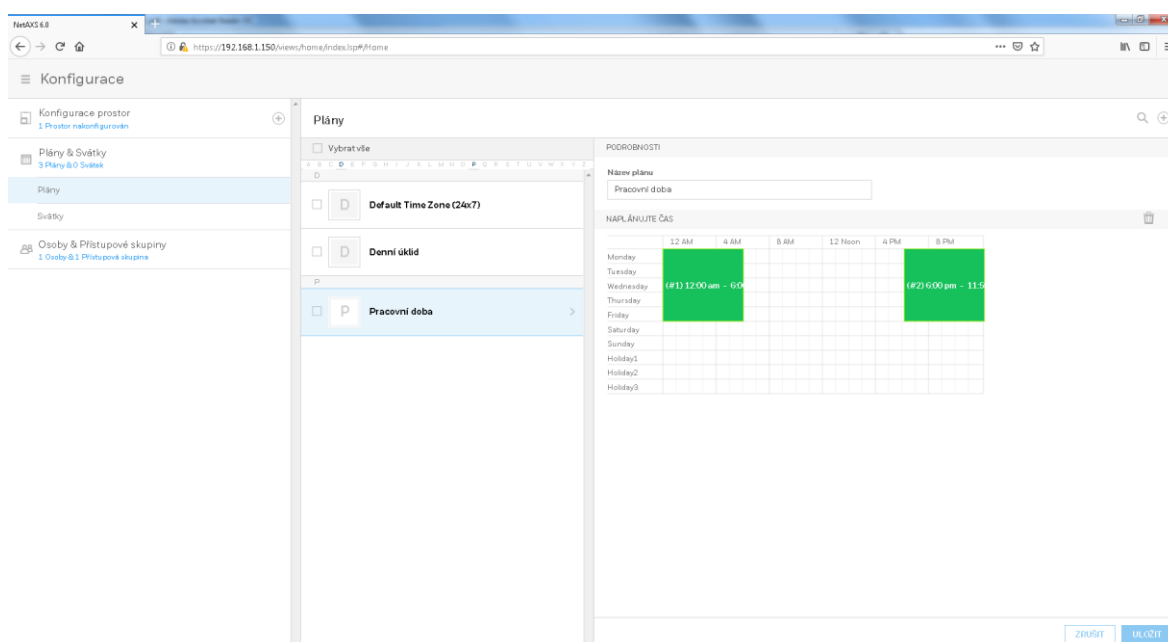
Pro otestování demonstračního panelu je zvoleno jednoduché zadání pro jednostranné řízení jednoho vstupního místa.

Zadání: Nastavte řídicí jednotku přístupového systému NX1P s příslušnými perifériemi pro jednostranné řízení hlavního vstupu do „FIRMY“. Firma má celkem 5 zaměstnanců:

- „BOSS“ – majitel firmy, práva pro přístup bez omezení.

- Pracovník 1 – zaměstnanec, práva pro přístup v pracovní dny v době od 8:00 do 17:00 hodin.
- Externista 1 – externí pracovník, práva pro přístup kdykoliv v době od 6:00 do 19:00 hodin.
- Úklid 1 – pracovník pro úklid, práva pro přístup v pracovní dny od 16:00 do 23:59 hodin.
- Vedoucí skladu – zaměstnanec se stejnými přístupovými právy jako Externista 1.

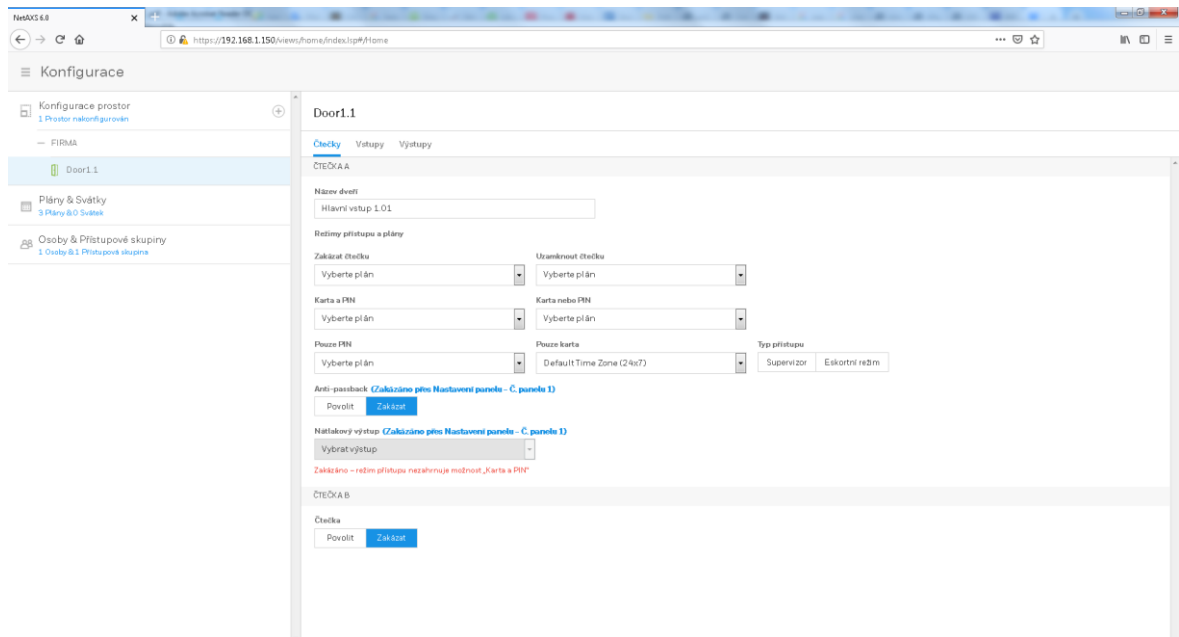
V tomto kroce je možné přistoupit k přidání časových zón, resp. „plánů“ jak je znázorněno na obrázku 34. Defaultně je nastavena systémová časová zóna Default Time Zone (24x7).



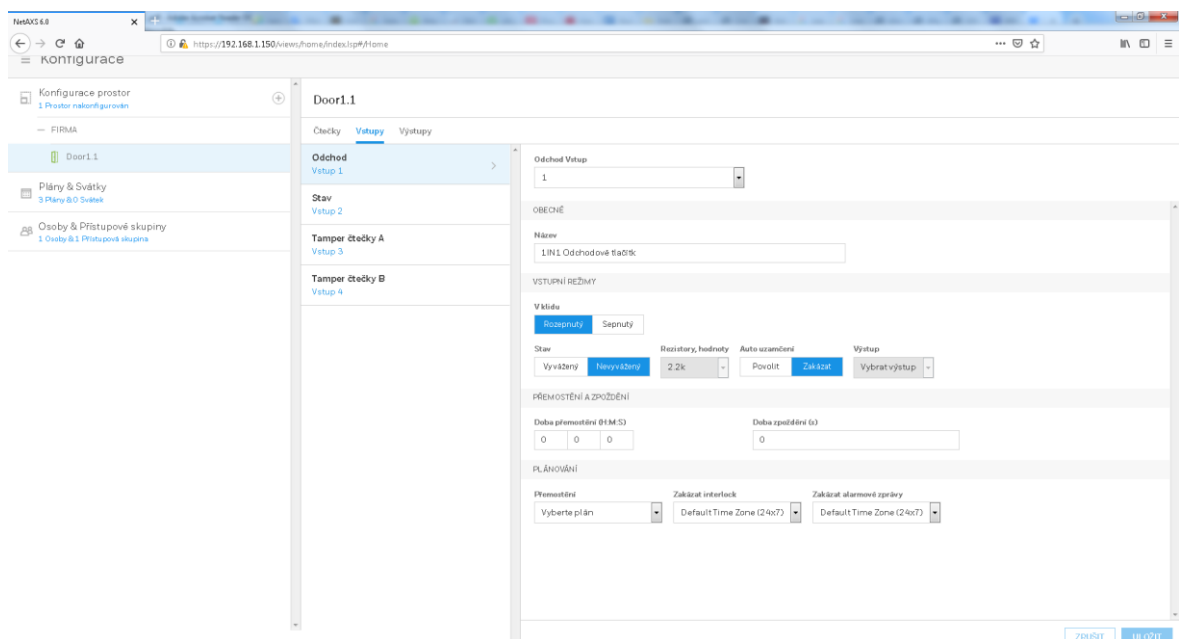
Obr. 34 – Konfigurace řídicí jednotky, nastavení časových zón.[Zdroj: vlastní]

Nyní je možné přistoupit k definici dveří. U dveří nastavujeme jméno. Pro demonstrační panel bylo zvoleno jméno Hlavní vstup a adresně uvedená jeho pozice. Uvedení adresné pozice usnadňuje orientaci při konfiguraci a správě rozsáhlých přístupových systémů. Současně se zde popisují vstupy a výstupy řídicí jednotky NX1P.

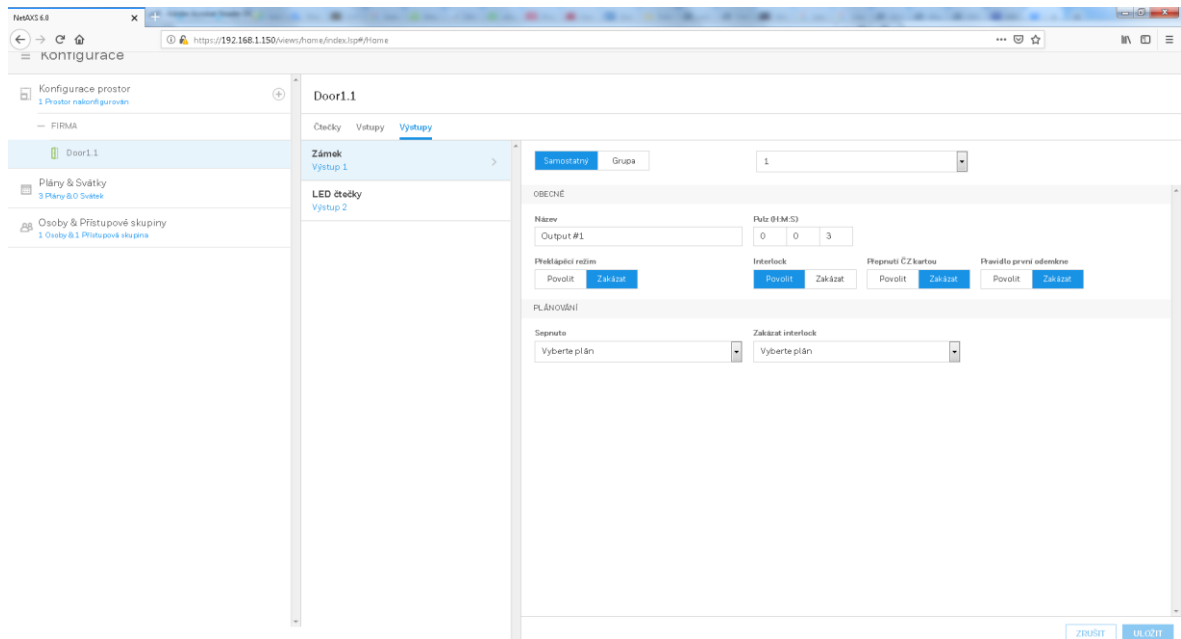
Pro rozsáhlé přístupové systémy je vhodné pracovat i s grafickou formou rozmístění jednotlivých vstupních míst, případně podrobným blokovým schématem.



Obr. 35 – Konfigurace řídicí jednotky, definice dveří.[Zdroj: vlastní]

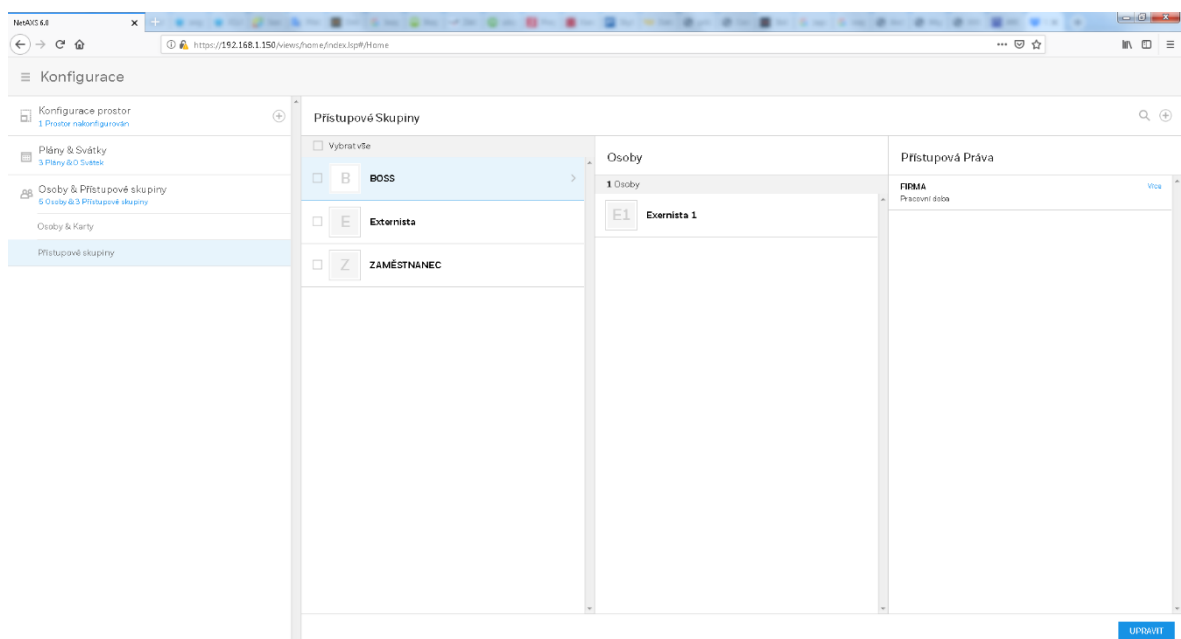


Obr. 36 – Konfigurace řídicí jednotky, definice vstupů.[Zdroj: vlastní zpracování]



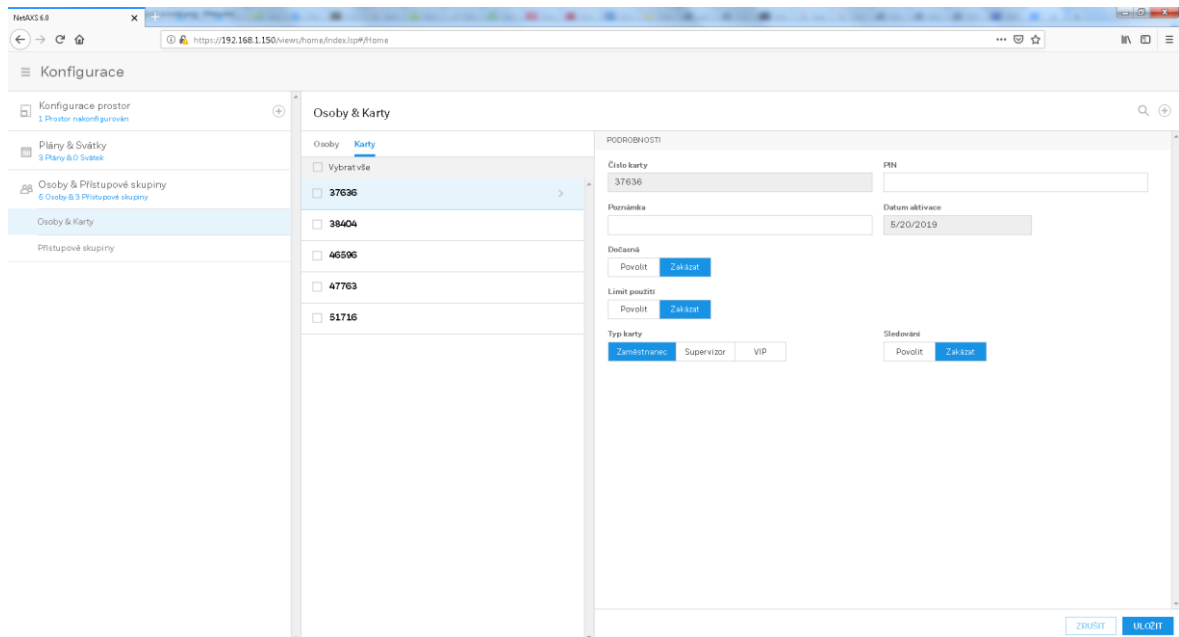
Obr. 37 – Konfigurace řídicí jednotky, definice výstupů.[Zdroj: vlastní]

Nyní můžeme přistoupit k tvorbě přístupových úrovní, kde určujeme kteří držitelé karet mají přístup a kdy jej mají.

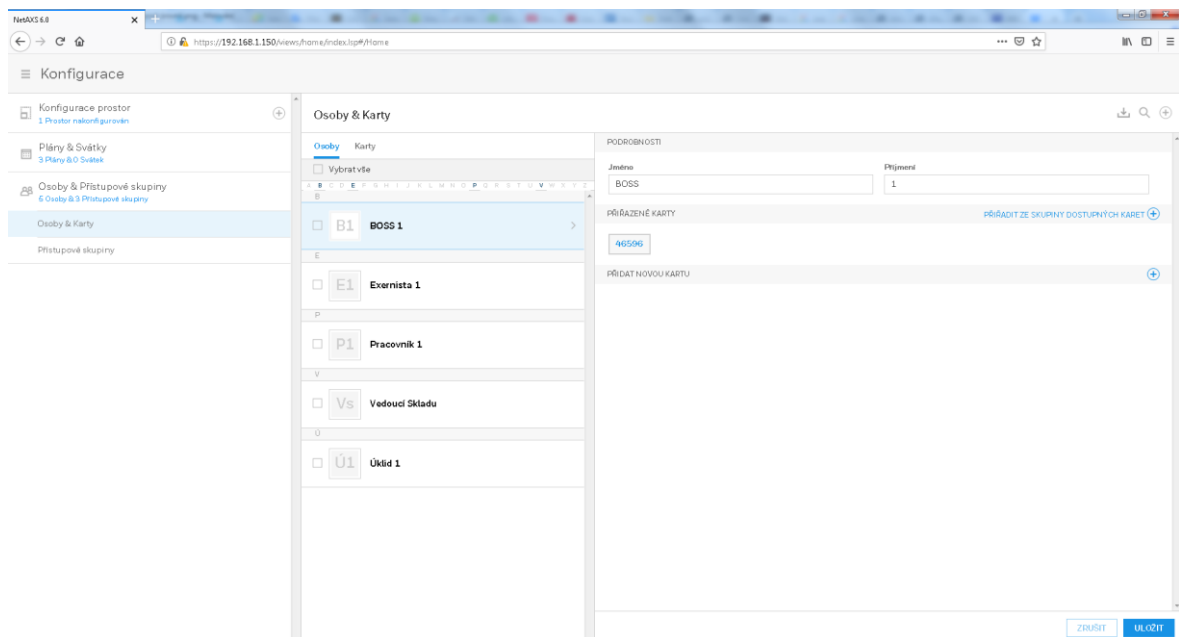


Obr. 38 – Konfigurace řídicí jednotky, přístupové skupiny.[Zdroj: vlastní]

V posledním kroku konfigurace demonstračního panelu je nutné přidat karty a přiřadit je osobám.



Obr. 39 – Konfigurace řídicí jednotky, zadávání karet.[Zdroj: vlastní]



Obr. 40 – Konfigurace řídicí jednotky, zadávání osob.[Zdroj: vlastní]

V tomto okamžiku je základní konfigurace řídicí jednotky hotova a je možné ověřit funkčnost definovaných karet.

10.2 Konfigurace programem WIN-PAK SE

Pro konfiguraci demonstračního panelu s řídicí jednotkou NX1P je použit program WIN-PAK SE (Demo). Demo verze je plnohodnotný program WIN-PAK SE, ale jsou v něm omezené některé základní vlastnosti – lze přiřadit maximálně 10 uživatelů a historie událostí je

maximálně na 100 záznamů. Pro testovací účely je i přes toto omezení program plně vyhovující.

Při prvním spuštění je přihlášení do systému jen pomocí jména admin bez hesla, ovšem po připojení je uživatel vyzván, aby si heslo vytvořil. Podmínkou vytvoření platného hesla je použití malých a velkých alfanumerických znaků, číslic a speciálních znaků. Minimální délka hesla je 8 znaků. Za těchto podmínek je uživatel nucen vytvořit silné heslo, pokud vynechá jednu z uvedených skupin povolených znaků, systém mu nepovolí pokračovat v konfiguraci.

Po spuštění programu WIN-PAK se na obrazovce objeví průvodce nastavením, který v osmi krocích provede základní konfiguraci systému.

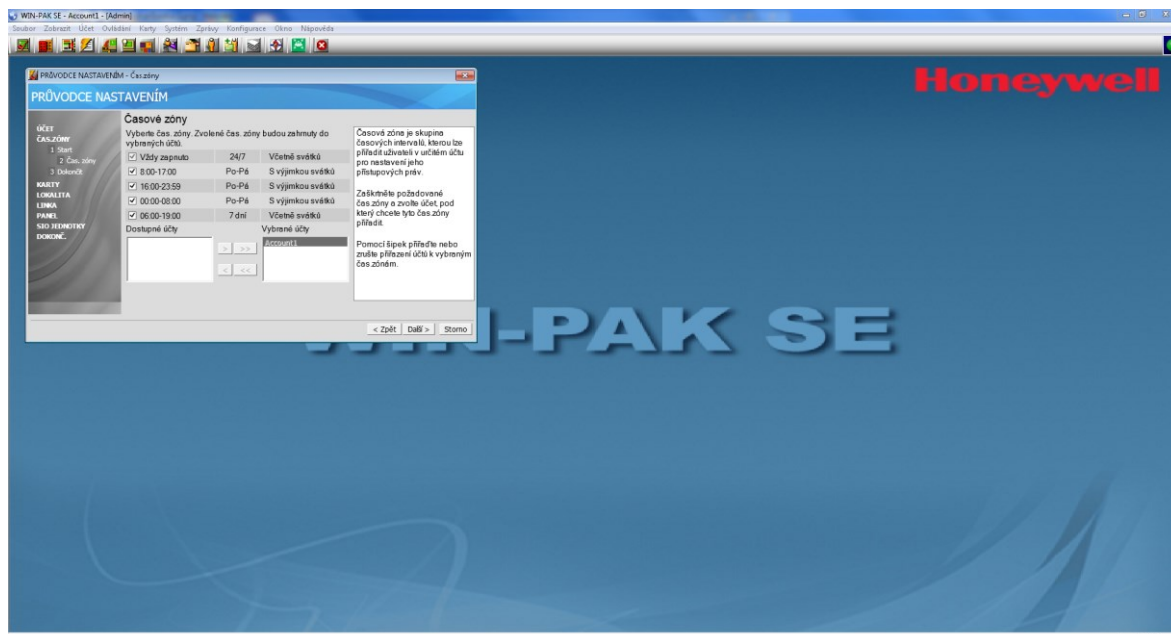


Obr. 41 – Průvodce nastavením WIN-PAK.[Zdroj: vlastní]



Obr. 42 – Konfigurace řídicí jednotky, vytvoření účtu.[Zdroj: vlastní]

Ve druhém kroku je uživatel vyzván k vytvoření časových zón. Posloupnost konfiguračních kroků je stejná jako u konfigurace prostřednictvím webového prohlížeče.



Obr. 43 – Konfigurace řídicí jednotky, časové zóny.[Zdroj: vlastní]

Následuje vytvoření virtuální oblasti (lokality), která slouží pro logické spojení řídicích jednotek přístupového systému a přidělování přístupových práv.



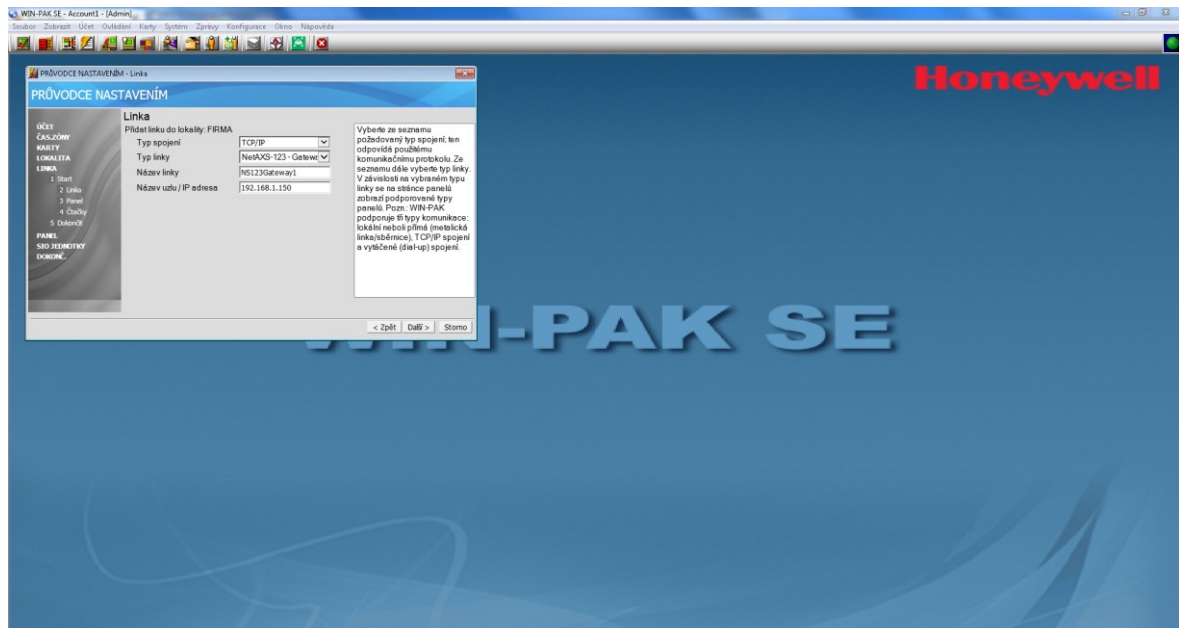
Obr. 44 – Konfigurace řídicí jednotky, virtuální přístupová oblast.[Zdroj: vlastní]

Ve čtvrtém kroku průvodce definuje uživatel linku. Je vhodné, aby každé IP připojení mělo svou vlastní virtuální oblast. Linka odpovídá převodníku pro komunikaci mezi řídicí jednotkou přístupového systému a počítačem. Pokud je jedna řídicí jednotka přístupového systému konfigurována jako Gateway a k ní jsou prostřednictvím sběrnice RS-485 připojené další řídicí jednotky přístupového systému, pak celý tento soubor zařízení je jednou linkou.



Obr. 45 – Konfigurace řídicí jednotky, vytvoření linky.[Zdroj: vlastní]

V pátém kroku se nastavují parametry komunikační linky.



Obr. 46 – Konfigurace řídicí jednotky, nastavení parametrů komunikační linky.[Zdroj: vlastní]

Následuje konfigurační obrazovka, ve které se definují vstupní čtečky, zda je vstupní místo řízeno jednostranně nebo oboustranně. Ke každé vstupní čtečce se přiřazuje časová zóna a čas pro aktivaci zámku.



Obr. 47 – Konfigurace řídicí jednotky, definice vstupních čteček.[Zdroj: vlastní]

V předposledním kroce dojde k vyzvání uživatele, aby rozhodl, zda je konfigurace konečná, a pokud ano, aby průvodce ukončil.



Obr. 48 – Konfigurace řídicí jednotky, přidání zařízení nebo ukončení průvodce.[Zdroj: vlastní]

Jakmile uživatel potvrdí, že konfigurace je úplná a hotova, přejde průvodce na poslední obrazovku, kterou je rekapitulace zadaných zařízení a nastavení dílčích parametrů.



Obr. 49 – Rekapitulace nastavení přístupového systému.[Zdroj: vlastní]

Volbou dokončit přechází program do grafického prostředí pro správu přístupového systému. Nyní je možné přistoupit k zadání karet a přístupových oprávnění prostřednictvím nabídky [menu] a následně vytvořit osoby a jim přiřadit příslušná oprávnění prostřednictvím přidělené karty nebo více karet.

11 POROVNÁNÍ ŘÍDÍCÍCH JEDNOTEK

11.1 Situace na trhu

Jak již bylo zmíněno v úvodu, je v současné době na trhu více než tisíc výrobců přístupových systémů. Z pohledu působnosti a vlivu je můžeme rozdělit na lokální a globální. Lokální výrobci mají výhodu dobré znalosti místního trhu, požadavků zákazníků a jsou schopni svůj hardware i software přizpůsobit konkrétnímu zákazníkovi. Poměrně velkým rizikem však pro zákazníka je, že jeho investice do budovaného a provozovaného bezpečnostního řešení řízení pohybu entit (osoby, automobily, mobilní samočinné pracovní stroje atp.) skončí zmařena, pokud lokální výrobce ukončí svou činnost nebo změní svou obchodní strategii. Naproti tomu u velkých nadnárodních korporací jakými jsou Honeywell, Siemens, ASSA ABLOY aj., je záruka kontinuity bezpečnostního řešení v dlouhodobém časovém horizontu, často až desítky let, ale za cenu unifikovaného produktu, kde se musí uživatel přizpůsobit vlastnostem implementovaného řešení.

V Příloze 1 je uvedena přehledová Tab., která srovnává jednotlivé řídicí jednotky a softwarových programů pro správu a monitoring přístupových systémů.

11.2 Řídicí jednotka přístupového systému A22

Řídicí jednotka přístupového systému A22 je z produkce francouzského výrobce bezpečnostních systémů CDVI. U této řídicí jednotky a softwarové programové nadstavby je patrný progresivní vývoj za posledních pět let. Před pěti lety byl koncept přístupového systému postaven na jedné hlavní IP řídicí jednotce (MASTER), a ostatní řídicí jednotky (SLAVE) byly připojené k této prostřednictvím sběrnice RS-485. Celková kapacita systému byla 10 dveří řízených jednostranně a 2.000 karet. V současné době je původní model rozšířen díky vývoji softwarového programového vybavení, který umožňuje připojit až 50 IP řídicích jednotek, ke kterým mohou být připojeny další až 4 řídicí jednotky prostřednictvím sběrnice RS-485. Navíc výrobce zajistil, že nové řídicí jednotky mohou doplnit starší stávající instalace přístupových systémů. Nutnou podmínkou je aktualizace firmware ve starších řídicích jednotkách.

Ze srovnání technických i softwarových parametrů obou řídicích jednotek, jak je uvedeno v Příloze 1, vychází lépe řídicí jednotka NetAXS-123. Ale současně se obě řídicí jednotky liší v jenom zásadním pohledu – správa přístupového systému. Správa řídicí jednotky při-

stupového systému NetAXS-123 je velmi sofistikovaná, jak prostřednictvím webového prohlížeče, tak programovou nadstavbou WIN-PAK. Naopak přístup ke správě systému u řídicí jednotky přístupového systému A22 s programovou nadstavbou ATRIUM je velmi intuitivní a navíc umožňuje současný přístup webovým prohlížečem ze smartphonu, tabletu nebo počítače nebo z počítače s instalovaným softwarovým vybavením pro správu přístupového systému.

Z výše uvedeného vyplývá, že existují instalace, kde se lépe osvědčí implementace přístupového systému s řídicími jednotkami NetAXS-123, a v jiných instalacích bude vhodnější použít řídicí jednotky A22.

ZÁVĚR

V diplomové práci jsou uvedeny obecné postupy pro návrh bezpečnostního řešení přístupových systémů. V diplomové práci jsou uvedeny postupy pro konfiguraci řídicí jednotky přístupového systému NetAXS-123, typ NX1P pro jedno vstupní místo řízené jednostranně nebo oboustranně. Jsou zde uvedeny parametry, které se při konfiguraci zadávají. Význam jednotlivých parametrů je vysvětlen. V praktické části diplomové práce je uvedena ukázka demonstračního panelu s jednou řídicí jednotkou NX1P, jednou RFID čtečkou a demonstračními perifériemi typu elektrický zámek, optická signalizace druhého výstupu řídicí jednotky, odchodovým tlačítkem pro ovládání zámku a magnetickým kontaktem pro simulaci otevření dveří. Pro názornost jsou v praktické části uvedené konkrétní obrazovky jak z průběhu konfigurace prostřednictvím webového prohlížeče, tak z programu WIN-PAK.

Ze všech uvedených konfiguračních možností zvolené řídicí jednotky přístupového systému NetAXS-123 společně s programovým vybavením WIN-PAK vyplývá, že se jedná o velmi robustní nástroj pro řízení pohybu entit v objektu z pohledu bezpečnosti a z hlediska možnosti nastavení automatických procesů a zasílání informačních zpráv při narušení bezpečnosti nebo bezpečnostním incidentu je zřejmé, že dohled nad prostorem, který je zabezpečen přístupovým systémem je udržitelný s minimálními požadavky na počet členů ostrahy. Hardwarová topologie systému i softwarová hierarchie operátorů ukazuje, že systém splňuje nejpřísnější požadavky na bezpečnost a současně nemá žádná omezení, aby nemohl být implementován jako bezpečnostní řešení do rozsáhlých objektů. Architektura systému Klient – Server umožňuje spravovat systém z několika míst současně, a monitoring realizovat jedním dohledovým centrem. Systém je vhodným řešením pro společnosti, které uvažují sjednotit přístupový systém na všech svých pobočkách, detašovaných pracovištích atp. Z počtu linek definovaných v softwarovém vybavení WIN-PAK je zřejmé, že počet poboček spravovaných jedním serverem je prakticky neomezený.

SEZNAM POUŽITÉ LITERATURY

- [1] UHLÁŘ, J. *Technická ochrana objektů, II. Díl*. Praha: Vydavatelství PA ČR, 2005. ISBN 80-7251-189-0.
- [2] ČSN EN 60839-11-1. *Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty*. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 33 4593.
- [3] Ing.VOTRUBA, Z. *Kroucená dvoulinka*. Článek na Internetu. Dostupné z <http://internet.ha.cz>.
- [4] *Katalogový list k produktové řadě bezkontaktních čteček iCLASS SE s vysokým stupněm zabezpečení*. Dostupné z <https://www.adiglobal.cz>.
- [5] HSF1-NA123 R6-01-CZ(1118)DS-E © 2018 Honeywell International Inc., dostupné z <https://www.adiglobal.cz>.
- [6] *Příručka k uvedení systému NetAXS-123 do provozu*. Dokument 800-06188, verze B. Dostupné z <https://www.adiglobal.cz>.
- [7] *NetAXS-123 Access Control Unit User's Guide* © 2018 Honeywell International Inc., 128 stran, Document 800-05168V5 – A – 02/2018 Dostupné z <https://mywebtech.honeywell.com>
- [8] ČANDÍK, M. *Objektová bezpečnost II*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-217-3.
- [9] *NetAXS-123 Jednotka pro řízení přístupu - Uživatelská příručka*. Honeywell, 2010. 165 stran.
- [10] *NexAXS-123 Příručka k uvedení systému do provozu*. Honeywell, 2010. 24 stran.
- [11] *Winpak 4 uživatelský manuál*. Honeywell, 2014. 696 stran.
- [12] *Atrium, jednotka kontroly vstupu s webovým rozhraním - instalační manuál*. Honeywell. 32 stran.
- [13] *Atrium, jednotka kontroly vstupu s webovým rozhraním - uživatelský manuál*. Honeywell. 24 stran.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACU	Řídící jednotka přístupového systému.
cm	Centimetr.
ČR	Česká republika.
ČSN	České technické normy.
DIP	Vícenásobný přepínač zapájený do desky plošných spojů.
EKV	Elektronická kontrola vstupu.
EN	Evropské normy.
EVL	Ethernetová virtuální linka.
IP	Stupeň krytí.
LAN	Místní síť.
LED	Elektroluminiscenční dioda.
mA	Miliampér.
MHz	Megahertz
mm	Milimetr.
NC	V klidu sepnuto.
NO	V klidu rozepnuto.
PIN	Osobní identifikační číslo.
PoE	Napájení přes internet.
RFID	Identifikace pomocí rádiové frekvence.
UPS	Zdroj nepřerušovaného napájení.
USB	Universální sériová sběrnice.
Vss	Stejnoseměrné napětí.
WAN	Světová síť.

SEZNAM OBRÁZKŮ

Obr. 1 – Funkční části systému EKV [Zdroj: vlastní]	10
Obr. 2 – Typická architektura elektronického systému kontroly vstupu [2]	11
Obr. 3 – Způsob připojení čtyř zařízení na sběrnici EIA-485 [Zdroj: vlastní]	14
Obr. 4 – Rozpletení kabelu UTP Cat.5 [3]	15
Obr. 5 – Bezkontaktní čtečka HID iCLASS SE R10, pohled z čelní a zadní strany [Zdroj: vlastní].....	17
Obr. 6 – Blokové schéma řídicí jednotky přístupového systému. [3].....	19
Obr. 7 – Přehled přístupového systému s řídicími jednotkami NetAXS-123.[5].....	19
Obr. 8 – Řídicí jednotka přístupového systému NetAXS–123 v plastové skříni.[5]..	20
Obr. 9 – Přídavné karty pro 1 a 2 dveře pro NetAXS-123.[5].....	21
Obr. 10 - Schéma připojení uživatelských a systémových rozhraní.[6]	22
Obr. 11 – Nastavení přepínačů pro konfiguraci relé.....	23
Obr. 12 – Verze a návaznosti WIN-PAK.[6].....	27
Obr. 13 – Přiřazení ADV zařízení.[6].....	29
Obr. 14 – Nastavení formátu karet pro NetAXS-123.[6]	30
Obr. 15 – Určení maximální délky čísla karty.[6]	32
Obr. 16 – Přehledový monitoring ve WIN-PAKu.[6]	33
Obr. 17 – Textový monitoring ve WIN-PAKu.[6]	34
Obr. 18 – Alarm monitoring ve WIN-PAKu.[6]	34
Obr. 19 – Grafický monitoring ve WIN-PAKu.[6]	35
Obr. 20 – Monitoring pohybu osob ve WIN-PAKu.[6].....	36
Obr. 21 – Lokalizace držitele karty ve WIN-PAKu.[6].....	37
Obr. 22 – Záznam operátora ve WIN-PAKu.[6]	37
Obr. 23 – Oprávnění obsluhy ve WIN-PAKu.[6].....	38
Obr. 24 – Plán ve WIN-PAKu.[6]	39
Obr. 25 – Hlídaní velikosti databáze ve WIN-PAKu.[6].....	41
Obr. 26 – Zálohování a obnova dat ve WIN-PAKu.[6].....	42
Obr. 27 – Elektromagnetický zámek DORCAS.[Zdroj: vlastní].....	43
Obr. 28 – Elektromechanický zámek EL460 (vlevo) a přídržný magnet V3SR (vpravo).[Zdroj: vlastní].....	44
Obr. 29 – Převodník RS-485 na Ethernet VESP211-485.[Zdroj: vlastní].....	45
Obr. 30 – Demonstrační panel s řadičem NetAXS-123 typ NX1P.[Zdroj: vlastní] ...	48

Obr. 31 – Správa účtu, změna jazyka přes webový prohlížeč.[Zdroj: vlastní].....	50
Obr. 32 – Úvodní stránka konfigurace NX1P přes webový prohlížeč.[Zdroj: vlastní]	51
Obr. 33 – Konfigurace řídicí jednotky, nastavení komunikace a času.[Zdroj: vlastní]	51
Obr. 34 – Konfigurace řídicí jednotky, nastavení časových zón.[Zdroj: vlastní].....	52
Obr. 35 – Konfigurace řídicí jednotky, definice dveří.[Zdroj: vlastní]	53
Obr. 36 – Konfigurace řídicí jednotky, definice vstupů.[Zdroj: vlastní zpracování] ...	53
Obr. 37 – Konfigurace řídicí jednotky, definice výstupů.[Zdroj: vlastní]	54
Obr. 38 – Konfigurace řídicí jednotky, přístupové skupiny.[Zdroj: vlastní]	54
Obr. 39 – Konfigurace řídicí jednotky, zadávání karet.[Zdroj: vlastní]	55
Obr. 40 – Konfigurace řídicí jednotky, zadávání osob.[Zdroj: vlastní].....	55
Obr. 41 – Průvodce nastavením WIN-PAK.[Zdroj: vlastní]	56
Obr. 42 – Konfigurace řídicí jednotky, vytvoření účtu.[Zdroj: vlastní]	57
Obr. 43 – Konfigurace řídicí jednotky, časové zóny.[Zdroj: vlastní].....	57
Obr. 44 – Konfigurace řídicí jednotky, virtuální přístupová oblast.[Zdroj: vlastní] ..	58
Obr. 45 – Konfigurace řídicí jednotky, vytvoření linky.[Zdroj: vlastní]	58
Obr. 46 – Konfigurace řídicí jednotky, nastavení parametrů komunikační linky.[Zdroj: vlastní]	59
Obr. 47 – Konfigurace řídicí jednotky, definice vstupních čteček.[Zdroj: vlastní]....	59
Obr. 48 – Konfigurace řídicí jednotky, přidání zařízení nebo ukončení průvodce.[Zdroj: vlastní].....	60
Obr. 49 – Rekapitulace nastavení přístupového systému.[Zdroj: vlastní].....	60

SEZNAM TABULEK

Tab. 1 – Stupně klasifikace [2]	12
Tab. 2 – Základní parametry bezkontaktní čtečky iCLASS SE R10 [4]	16
Tab. 3 - Technické parametry řídicí jednotky NetAXS-123.[5].....	25

SEZNAM PŘÍLOH

Příloha P I Srovnání technických a softwarových parametrů vybraných řídicích jednotek přístupového systému.	70
--	----

**PŘÍLOHA P I: SROVNÁNÍ TECHNICKÝCH A SOFTWAREVÝCH
PARAMETRŮ VYBRANÝCH ŘÍDÍCÍCH JEDNOTEK
PŘÍSTUPOVÉHO SYSTÉMU**