

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: **Physical access system with controller NetAXS-123 and WIN-PAK program**

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 zámkem 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 bakalářské práce:

Rozsah příloh:

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

Seznam doporučené 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 bakalářské práce: **Ing. Stanislav Goňa, Ph.D.**
Ústav elektroniky a měření

Datum zadání bakalářské práce: **26. července 2019**

Termín odevzdání bakalářské práce: **26. srpna 2019**

Ve Zlíně dne 2. srpna 2019

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
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 16.8.2019

.....
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	27
5 VÝSTUPNÍ ZAŘÍZENÍ	32
6 KOMUNIKAČNÍ ROZHRANÍ	34
II PRAKTICKÁ ČÁST	35
7 NÁVRH PŘÍSTUPOVÉHO SYSTÉMU	36
8 DEMONSTRAČNÍ PANEL	37
9 KONFIGURACE NX1P PŘES WEBOVÝ PROHLÍZEČ	39
9.1 ZÁKLADNÍ KONFIGURACE A NASTAVENÍ.....	39
9.2 SLEDOVÁNÍ STAVŮ SYSTÉMU A PODÁVÁNÍ ZPRÁV	62
10 SOFTWARE PRO SPRÁVU PŘÍSTUPOVÉHO SYSTÉMU WIN-PAK	65
10.1 KONFIGURACE DEMONSTRAČNÍHO PANELU S VYUŽITÍM WIN-PAKU	66
11 POROVNÁNÍ ŘÍDÍCÍCH JEDNOTEK	77
11.1 SITUACE NA TRHU	77
11.2 ŘÍDÍCÍ JEDNOTKA PŘÍSTUPOVÉHO SYSTÉMU A22.....	77
ZÁVĚR	81
SEZNAM POUŽITÉ LITERATURY	82
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	83
SEZNAM OBRÁZKŮ	84
SEZNAM TABULEK	86

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 dopracuje 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:

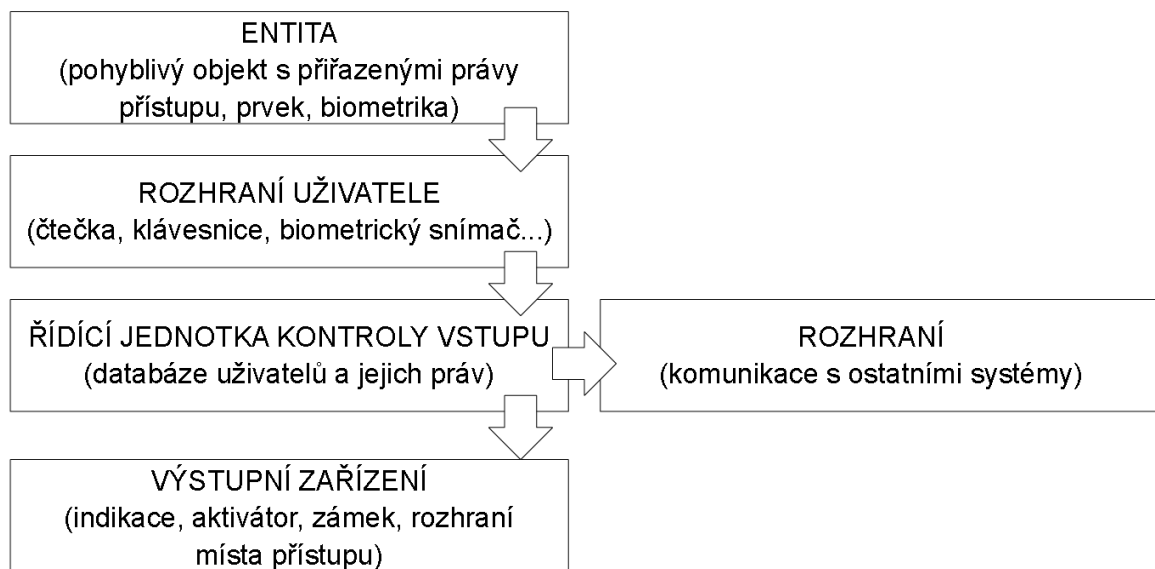
1. Kontinuita – výroba, vývoj a distribuce je zajišťována nadnárodní společností.
2. Robustnost – systém je dále rozšiřitelný s prakticky neomezenou kapacitou dveří a osob.
3. Dosažitelnost – distribuce zajišťuje školení různých subjektů.
4. Funkčnost – zajištěna dostupnost kompatibilních náhradních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

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.

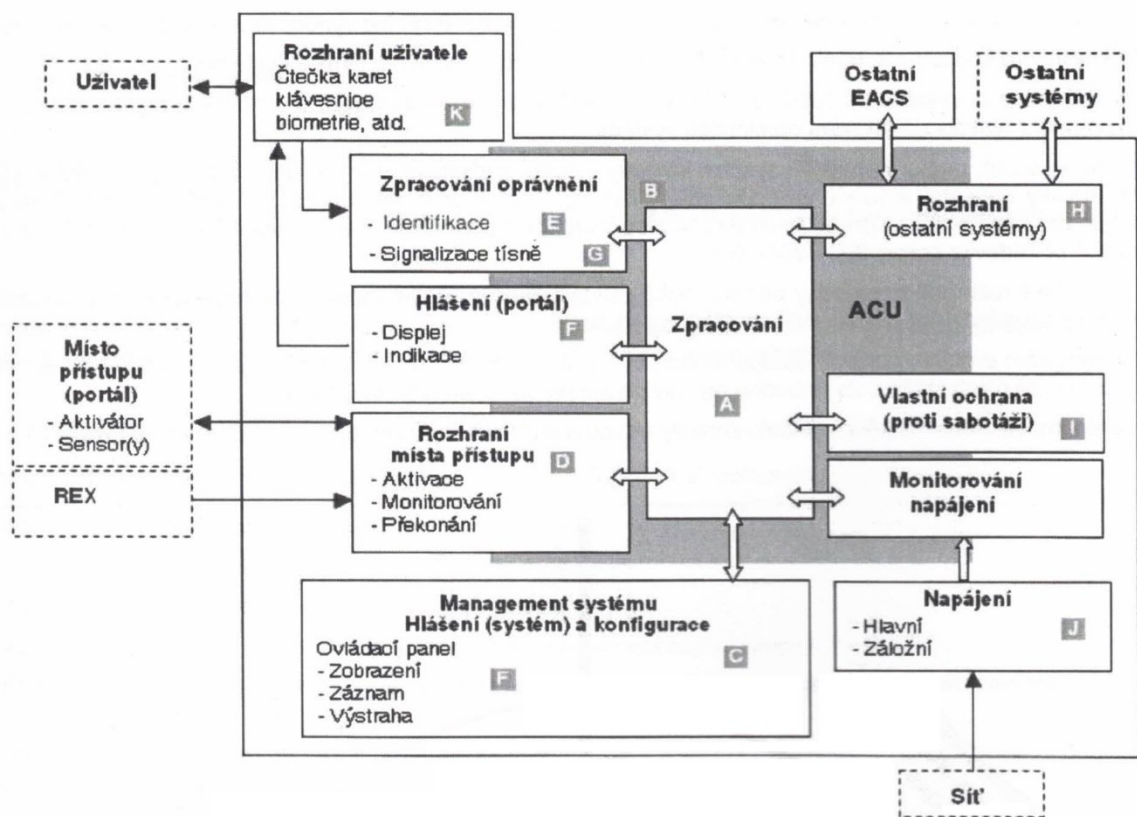


Obr. 1 – Funkční části systému EKV [Zdroj: vlastní]

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.

Jednotlivé funkční bloky architektury elektronického systému pro kontrolu vstupu dle obr.2 jsou rozvedeny dále v samostatných kapitolách.

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	Nízké	Nízké až střední	Střední až vysoké	Vysoké
Aplikace	organizační prostředky, ochrana majetku nízké hodnoty	organizační prostředky, ochrana prostředků nízké až střední hodnoty	méně organizačních prostředků, ochrana komerčních prostředků střední až vysoké hodnoty	zejména ochrana komerčních prostředků velmi vysoké hodnoty nebo kritické infrastruktury
Dovednost/znalosti pachatelů/útočníků	malá dovednost, malá znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií malé finanční prostředky pro napadení	střední dovednost a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií malé až střední finanční prostředky pro napadení	velká dovednost a znalost systémů kontroly vstupu, identifikačních prostředků a IT technologií střední finanční prostředky pro napadení	velmi vysoká dovednosti 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.

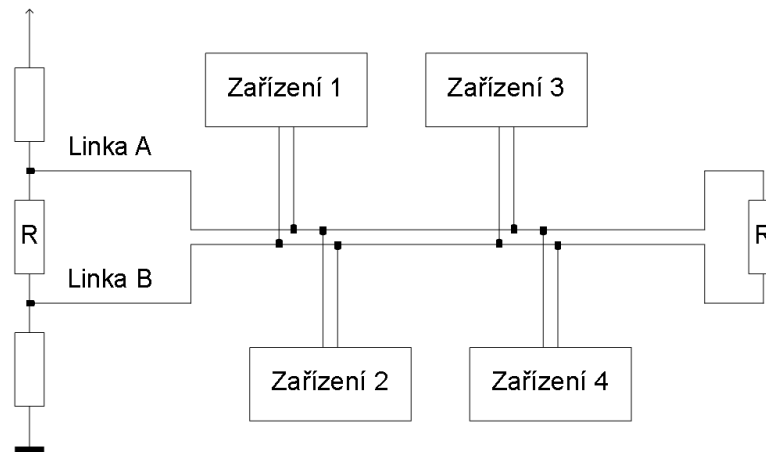
3.1 Datový výstup

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 V _{ss}
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 ni 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.

Tab. 3 – Barevné označení a význam vodičů bezkontaktní čtečky iCLASS SE R10

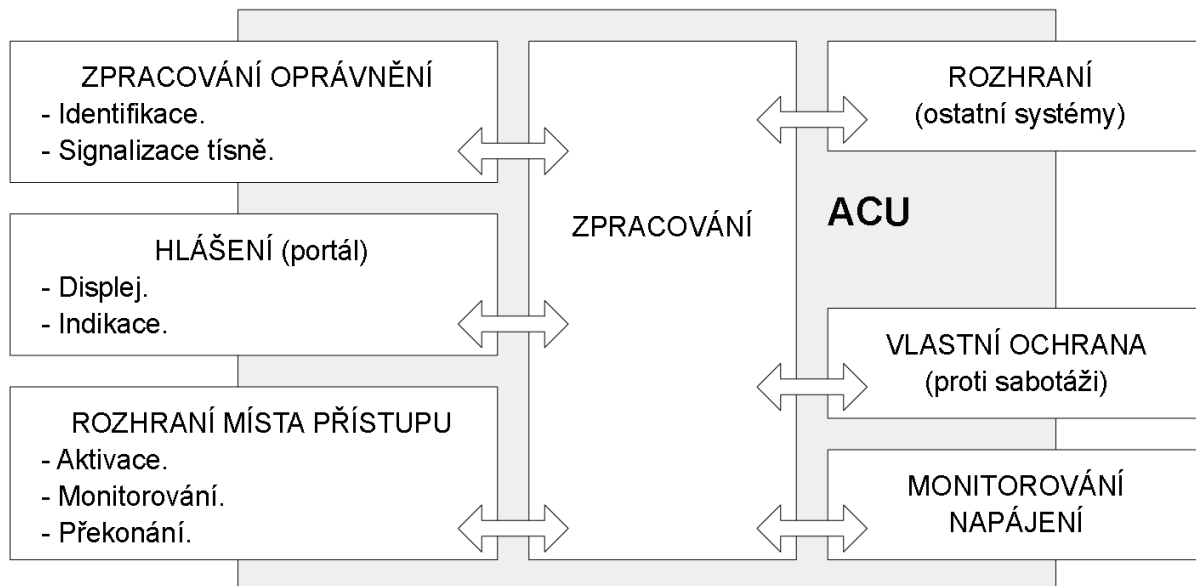
BARVA	VÝZNAM	BARVA	VÝZNAM
žlutá	bzučák	červeno-zelená	GPIO1 (RS232-T/RS485-A)
oranžová	zelená LED	sv.hnědá	GPIO2 (RS232R/RS485-B)
černá	napájení -	fialová	tamper
červená	napájení +	bílá	wiegand data 1
hnědá	červená LED	zelená	wiegand data 0
modrá	funkce HOLD	růžová	GPIO3 (RS485-Z)
		šedá	GPIO4 (RS485-Y)

RFID:

Čtečka iCLASS R10 využívá technologii radiofrekvenční identifikace (RFID), která umožňuje bezdotykovou identifikaci zboží, lidí, zvířat atp. a to i bez přímé viditelnosti. Čtečka komunikuje s tzv. tagy (tranpondéry) pomocí elektromagnetických vln. Tagy jsou malá a levná elektronická zařízení s malou spotřebou, proto jsou napájeny na principu elektromagnetické indukce – pohyb vlastní cívky v elektromagnetickém poli čtečky. Technologie RFID se využívá na různých pracovních frekvencích, typicky od stovek kHz (EM 125kHz) až do jednotky GHz (Mifare/Desfire 13,56MHz). Čtečka bezkontaktních tagů iCLASS R10 SE pracuje na frekvenci 13,56MHz.

4 ŘÍDÍCÍ JEDNOTKA KONTROLY VSTUPU

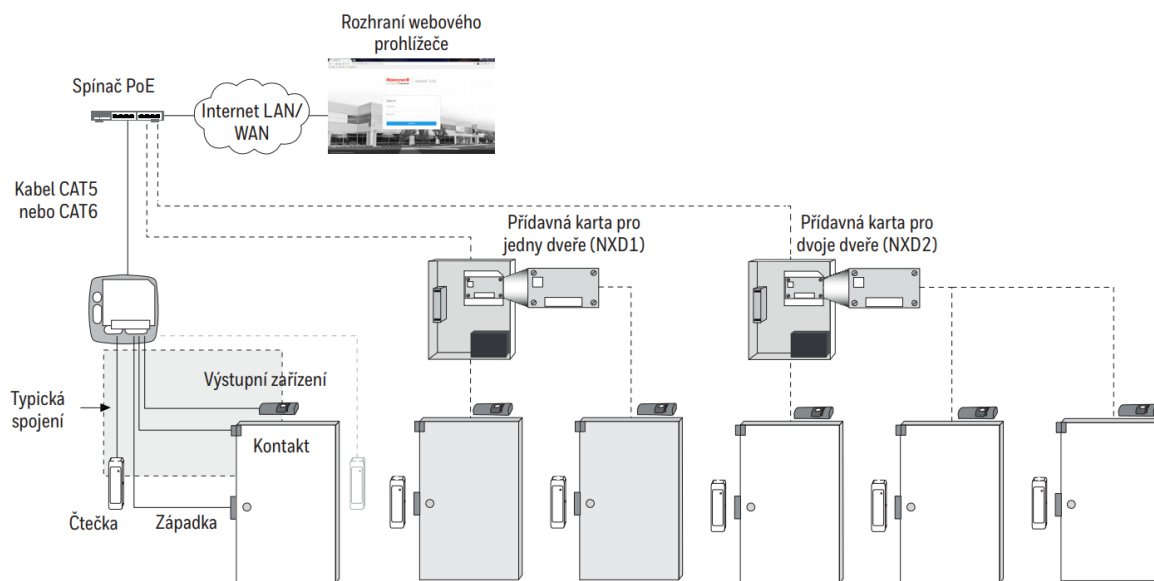
Řídící jednotka kontroly vstupu (ACU – access control unit) je část systému kontroly vstupu, která je propojena se čtečkami, uzamykacími zařízeními a snímači, rozhodující o poskytnutí nebo zamítnutí přístupu vstupním místem.[3]



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.

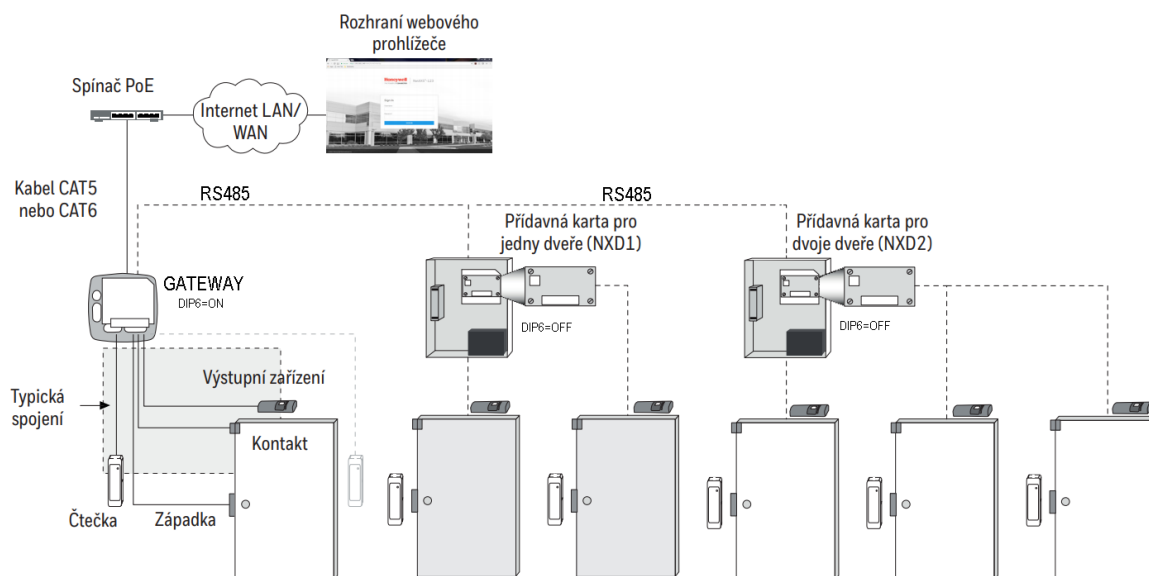


Obr. 7 – Přehled přístupového systému s řídicími jednotkami NetAXS-123.[5]

Architektura přístupového systému s řídicími jednotkami NetAXS-123

Každá řídicí jednotka přístupového systému je vybavena webserverem a konektorem RJ45 pro připojení do sítě LAN (obr. 7). U této architektury propojení řídicích jednotek NetAXS-123 musí mít všechny jednotky nastaven DIP přepínač na pozici 6 v hodnotě ON a u všech řídicích jednotek je nastavena IP adresa.

Pokud je řešen rozsáhlý přístupový systém, u kterého je dosahováno mezních hodnot celkové teoretické kapacity počtu řízených dveří, musí se v architektuře propojení jednotlivých řídicích jednotek přistoupit i k druhému („tradičnímu“) propojení řídicích jednotek, a tou je sběrnice RS485. Řídicí jednotky jsou vybaveny svorkovnicí RS485 (obr. 8). Jedna řídicí jednotka je připojena do sítě LAN, tzv. GATEWAY a ostatní řídicí jednotky jsou připojené k této nadřazené prostřednictvím sběrnice RS485. Přístup k nim je zajištěn přes nadřazenou řídicí jednotku NetAXS-123 a jednoznačné určení řídicích jednotek NetAXS-123 na sběrnici RS485 je realizováno adresací od 1 do 31 na pozicích S1 až S5 DIP přepínače. U adresných systémů s možností rozvětvené architektury bývá pravidlem, že adresa 0 se nepoužívá, resp. využívá ji systém na své vnitřní komunikační potřeby, v tomto případě je adresa 0 u každé jednotky vyhrazena na převodník RS232/RS485.

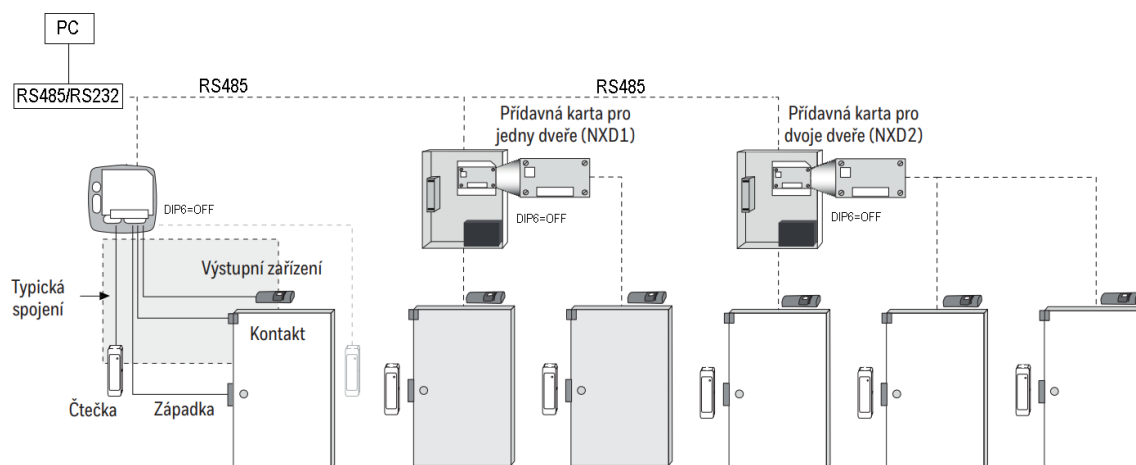


Obr. 8 – Architektura přístupového systému, kombinace IP a RS485.[5]

V praxi je velmi vhodné využívat oba způsoby propojení řídicích jednotek přístupového systému s ohledem na vlastnosti obou systémů z hlediska dosahovaných délek (RS485 až 1200m bez opakovacích sběrnice, LAN až 100m, resp. 90m – pravidla pro budování LAN sítí) a přenosových rychlostí.

Někteří výrobci přístupových systémů nabízí dvě provedení řídicích jednotek – jednu pro připojení k LAN a druhou pro připojení prostřednictvím sběrnice RS485. V okamžiku, kdy řídicí jednotka s připojením k Ethernetu je cenově až 3x výše než s připojením ke sběrnice RS485, pak vhodnou kombinací obou typů těchto řídicích jednotek je možné dosáhnout i poměrně výrazné finanční úspory.

Za historickou architekturu přístupového systému lze v současné době pokládat propojení řídicích jednotek NetAXS-123 výlučně prostřednictvím sběrnice RS485 (obr. 9). Vzhledem ke skutečnosti, že je řídicí jednotka vybavena síťovou kartou pro připojení do sítě LAN, pak je tohoto využito minimálně vždy u jedné se zapojených řídicích jednotek pro konfiguraci a monitorování přístupového systému v reálném čase. S nástupem internetu a jeho dostupností se začaly pro vzdálenou správu a monitorování používat převodníky RS485/Ethernet namísto převodníků RS485/RS232, které vyžadovaly lokální pracoviště v místě instalace. V současných verzích přístupových jednotek NetAXS-123 jsou převodníky RS485/Ethernet integrovány do desky elektroniky NetAXS-123 – síťová karta LAN.



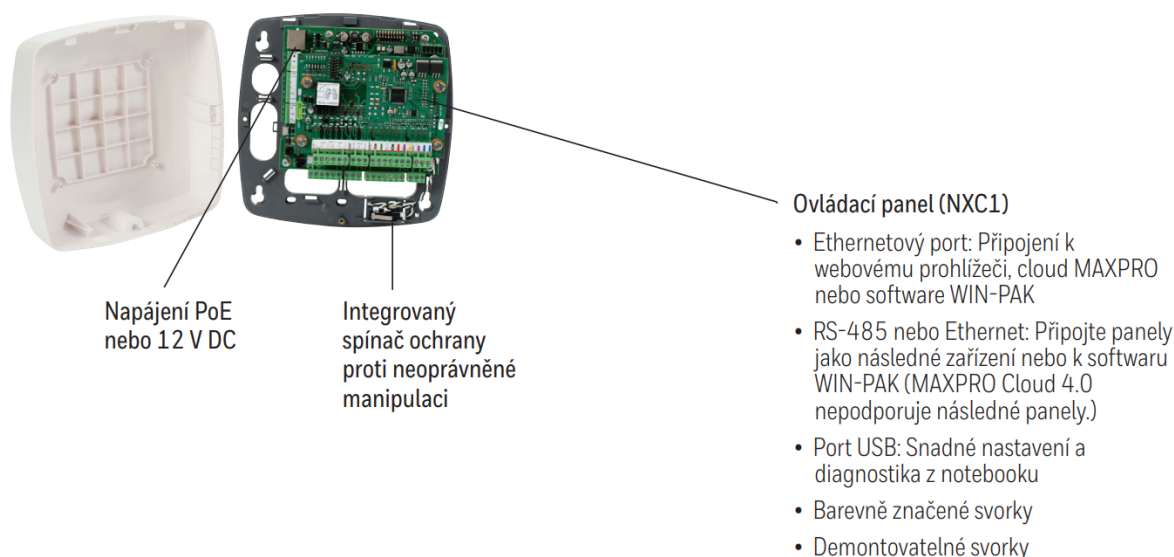
Obr. 9 – Architektura přístupového systému, sběrnice RS485.[5]

Vlastnosti řídicí jednotky NetAXS-123

Webová řídicí jednotka NetAXS společnosti Honeywell poskytuje řešení pro instalace jakéhokoliv rozsahu. 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] V určitém okamžiku růstu systému začíná být správa systému prostřednictvím webového prohlížeče velmi náročná pro správce systému, může se stát nepřehlednou a tento stav může generovat chyby při správě systému. V tomto okamžiku je vhodné přejít na správu takto rozsáhlého systému pomocí programu WIN-PAK.



Obr. 10 – Řídící 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]

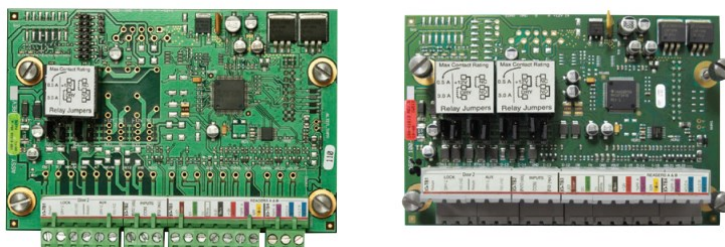
Je umožněna rychlejší instalace:

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

Systém 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 skříni.[5]

Schéma připojení uživatelských a systémových rozhraní k desce elektroniky řídicí jednotky přístupového systému NetAXS-123 je patrné z obr. 12.

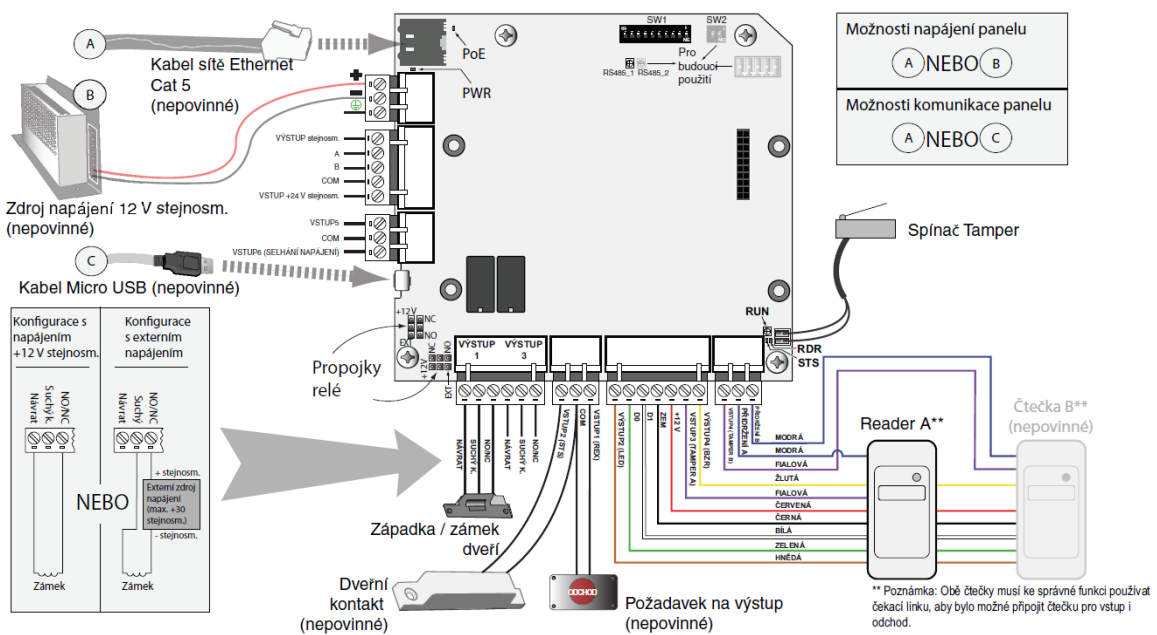
Popis desky elektroniky řídicí jednotky přístupového systému NetAXS-123

Komunikační rozhraní

LAN

Na pravé straně desky elektroniky řídicí jednotky přístupového systému NetAXS-123 nahoře je umístěna zásuvka RJ45 pro připojení LAN. Připojení k LAN umožňuje napájet řídicí jednotku prostřednictvím PoE (POWER over ETHERNET). Tento způsob distribuce napájení jednotlivých řídicích jednotek je poměrně přívětivý k instalaci, projektant nebo řešitel však musí vyřešit dva úkoly spojené s tímto způsobem napájení:

1. Zálohování přístupového systému, zálohuje se přívod 230V/5Hz k PoE injektorům, a to buď klasickými bateriovými UPS nebo se k PoE injektorům vede zálohovaný přívod z diesel agregátů.



Obr. 12 - Schéma připojení uživatelských a systémových rozhraní.[6]

2. Externí napájení zámků, k řídicím jednotkám lze zpravidla připojit různé aktivátory (zámky) prostřednictvím NO/NC kontaktu. Aktivátory ve většině případů jsou elektromagnetické zámky, které pracují na principu elektromagnetu. Mají různý proudový odběr (řádově od 170mA do 2A a více). S touto skutečností je nutné uvažovat při návrhu zálohovaného

napájení aktivátorů. Využití napájení přes PoE je možné, ale výrobce uvádí maximální celkové proudové zatížení 450mA pro všechna připojená zařízení – čtečky, vstupně/výstupní zařízení, zámky ... atp. Tato problematika pak úzce souvisí se způsobem deblokace aktivátorů na únikových cestách systémem Elektrické požární signalizace (EPS).

Závěr: Pro instalace přístupového systému typu bytový dům do 3 dveří je možné využít napájení prostřednictvím PoE a zálohování řešit UPS zdrojem. Pro bezpečnostní instalace přístupového systému do soukromého i veřejného sektoru je vhodné řešit napájení systému třemi nezávislými napájecími okruhy – jeden dimenzován pro řídicí jednotky přístupového systému, včetně čteček, druhý dimenzován pro zámky na únikových cestách s napojením na nouzové ovládání ze systému EPS, a třetí dimenzován pro všechny ostatní aktivátory (elektromagnetické zámky).

RS485

Vpravo, druhý slot po konektorem RJ45, na desce elektroniky je šroubovací svorkovnice pro připojení sběrnice RS485. Sběrnice je určena pro propojení až 30 dalších řídicích jednotek přístupového systému NetAXS-123 (nebo NetAXS-4). Označení svorkovnice sběrnice RS485 je A, B, COM. Součástí portu jsou dvě svorky, na kterých je vyvedeno pomocné napájení 12Vss a 24Vss určené pro napájení nízkoodběrových vstupně/výstupních zařízení.

USB

Deska elektroniky je vybavena na pravé straně slotem pro micro USB, který slouží pro připojení panelu k počítači. Spojení slouží ke konfiguraci jednotky NetAXS-123.

Externí napájení

Port umístěn pod zásuvkou RJ45 má označení svorek:

1. + napájení 12Vss,
2. – napájení 0V,
3. uzemnění.

Důležité: I když je třetí svorka označena symbolem uzemnění, deska elektroniky přístupového systému není v žádném případě vybavena svorkami pro připojení napájení přímo z rozvodné sítě 230V/50Hz!

Signalizace stavu napájení

Přístupový systém patří do rodiny bezpečnostních slaboproudých systémů. Selhání napájení systémů je považováno za bezpečnostní incident. Výrobce na toto myslel a desku elektroniky přístupového systémů NetAXS-123 vybavil dvěma systémovými vstupy (VSTUP5 a VSTUP6), na které se přivede společné minus (COM) v případě výpadku přívodu 230V/50Hz a výpadku napájení systémů ze záložního akumulátoru. Signalizační svorky jsou na desce elektroniky umístěné na třetím portu pod zásuvkou RJ45.

Nastavení relé výstupu

V parvo dole jsou umístěné propojky pro nastavení dvou výstupních relé. Propojkami nastavujeme, zda budeme používat vnitřních nebo externích 12V a zda dvě výstupní svorky relé budou typu “v klidu rozepnuto” (NO) nebo “v klidu sepnuto” (NC).

Pokud bude nastavena propojka pro využití vnitřního zdroje napájení, pak na výstupních svorkách se bude spínat 12Vss pro nastavení typu NO nebo se bude napájení 12Vss odepínat pro nastavení typu NC.

Pokud bude nastavena propojka pro zapojení externího napájecího zdroje, pak výstupní svorky relé budou mít vlastnost suchého kontaktu, podle nastavené druhé propojky pak typu NO nebo NC.

Poznámka: Při konfiguraci je výstup relé pro zámek označen jako VÝSTUP 1 a pomocné programovatelné relé jako VÝSTUP 3.

Snímací zařízení a vstupně/výstupní zařízení

Spodní řada svorkovnic slouží k připojení snímače stavu dveří (zpravidla magnetický kontakt signalizující stav dveří: otevřeno/zavřeno), vstup pro připojení odchodového tlačítka, které umožňuje neautorizované elektrické uvolnění aktivátoru (elektromagnetického zámku) ze strany chráněného prostoru, autorizační čtecí/snímací zařízení s rozhraním WIEGAND (čtečka bezkontaktních karet, biometrická čtečka, kódová klávesnice ... atp.). Pokud je zařízení vybaveno HOLD vodičem (řízení čtení zařízení), pak je možné, aby řídicí jednotka NetAXS-123 ovládala dveře z obou stran (oboustranné řízení přístupu, viz obr.10).

Tamper spínač

V levém spodním rohu je umístěn konektor pro připojení tamper kontaktu, který signalizuje sejmutí vrchního krytu elektroniky nebo otevření dvířek instalační skříně (dle typu umístění řídicí jednotky NetAXS-123).

4.2 Konfigurace řídicí jednotky přístupového systému NetAXS-123

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

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

- Ověření výchozího továrního nastavení spínačů DIP.

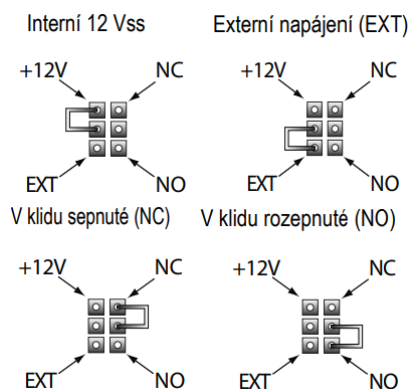


Skutečná orientace spínačů DIP na desce řídicí jednotky je otočena o 180°.

- 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 switchem 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. 13 – 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, od verze webserveru 6.0 je doporučen prohlížeč Google CHROME. 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. To-
vární 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. 4 - 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 bzučák 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 dozoraných 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 vstupní karet NX4IN)	5 vstupů rozšiřitelných na 14 s přídavnou kartou NXD2 (rozšiřitelné na celkem 74 vstupů pomocí maximálně 2 reléových vstupní 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
	ZÁŠUVKA 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 západky / 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	
	UPEVŇOVACÍ 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 PÁSMATA	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 PROHLÍŽEČŮ	Google Chrome
GLOBÁLNÍ	PODPORA JAZYKŮ	angličtina, francouzština, němčina, holandština, italština, španělština, čeština, zjednodušená čínština, arabština

5 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.

Elektromagnetické zámky

Elektromagnetické zámky zajišťují základní elektrické ovládání zabezpečených dveří. Způsob zajištění spočívá v přidržení, resp. uvolnění střelky zámků. 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 celocelové provedení zámků splňuje požadavky pro instalaci do požárních dveří.



Obr. 14 – Elektromagnetický zámek DORCAS.[Zdroj: vlastní]

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

6 KOMUNIKAČNÍ ROZHRAŇÍ

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

II. PRAKTICKÁ ČÁST

7 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:

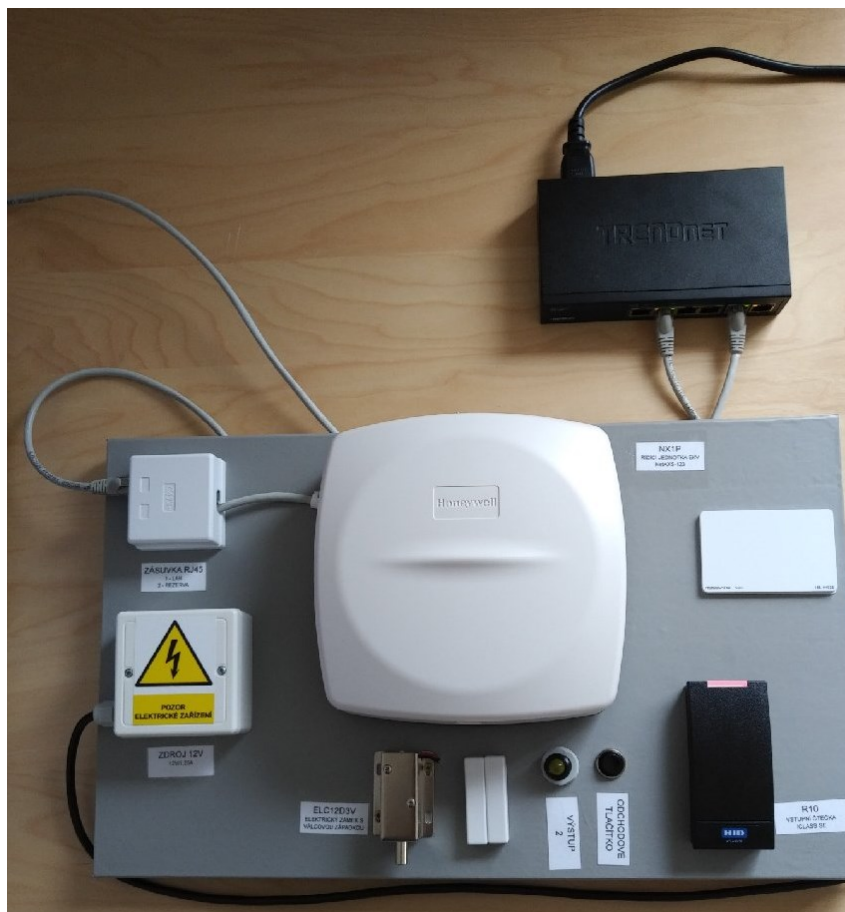
- Počet zabezpečených vstupních (případně i výstupních) míst.
- Počet entit, které se budou pohybovat v zabezpečených prostorách (například: zaměstnanci a návštěvy).
- Míra akceptovatelného bezpečnostního rizika (bezpečnostní opatření snižují míru rizika, nikdy však míra rizika nebude nulová).

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.

8 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. 17 – Demonstrační panel s řadičem NetAXS-123 typ NX1P.[Zdroj: vlastní]

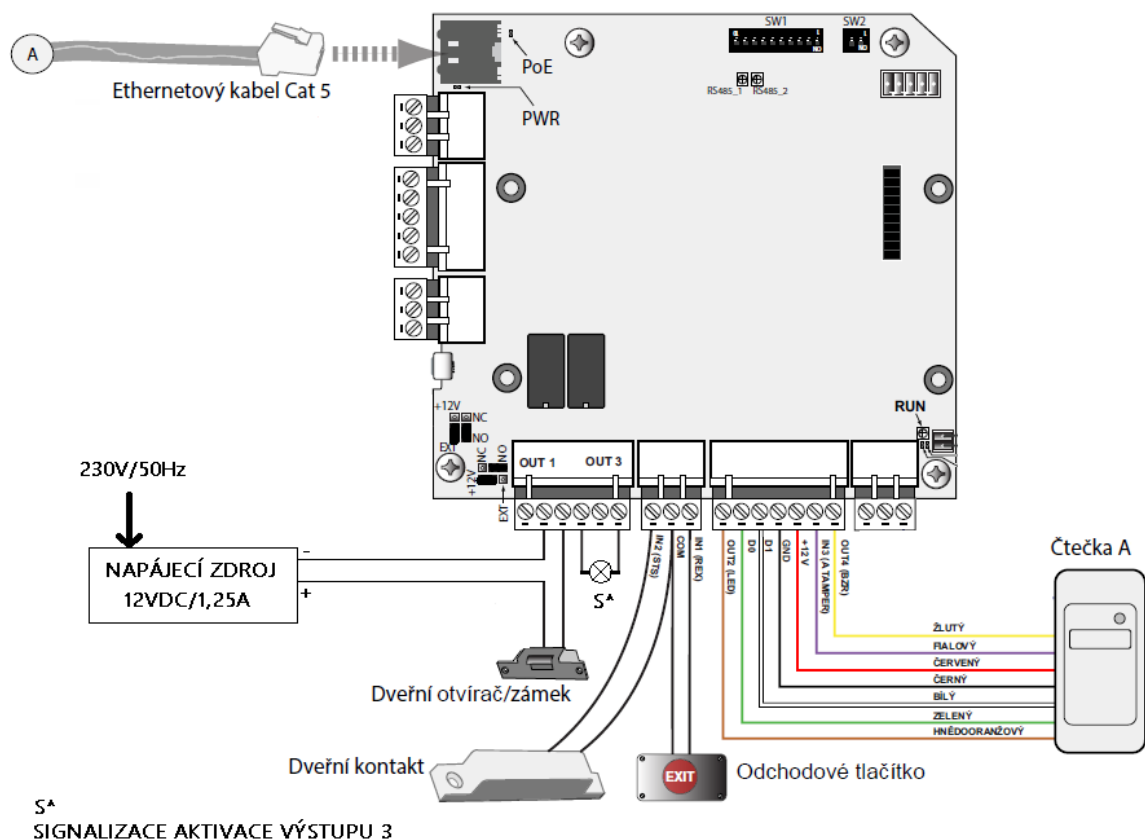
Specifikace komponent

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 (obr.33), 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 (odběr zámku je 1,2A) a typ kontaktu NO (v klidu rozepnuto). 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. Druhé relé se spíná na základě přiložené bezkontaktní karty, u které je nastaveno povolení ovládat VÝSTUP 3. Pro VÝSTUP 3 jsou propojky nastavené jako 12V (využití vnitřního zdroje panelu) a typ kontaktu NO (v klidu rozepnuto). Pro napájení řídicí jednotky je použita technologie PoE.



Obr. 18 – Zapojení demonstračního panel s řídicím NetAXS-123 typ NX1P.[6]

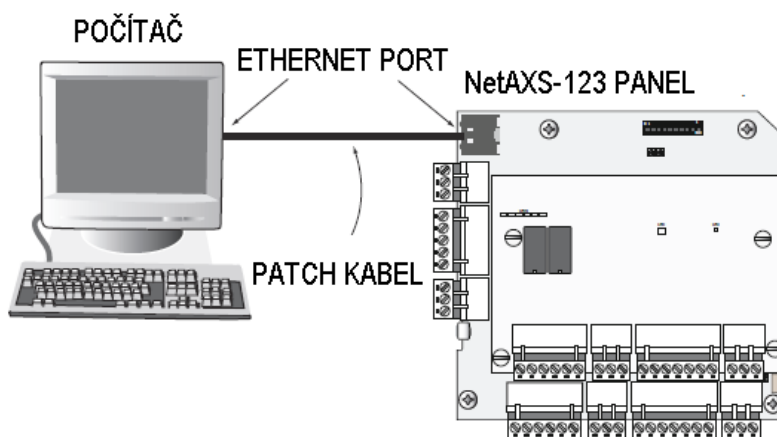
9 KONFIGURACE NX1P PŘES WEBOVÝ PROHLÍŽEČ

9.1 Základní konfigurace a nastavení

Jedná se o způsob konfigurace, kterou řídicí jednotka přístupového systému umožňuje. Zařízení NX1P je s aktuálním firmware NetAXS 6.0.10.20. Výrobce doporučuje pro konfiguraci řídicí jednotky použít webový prohlížeč Google CHROME.

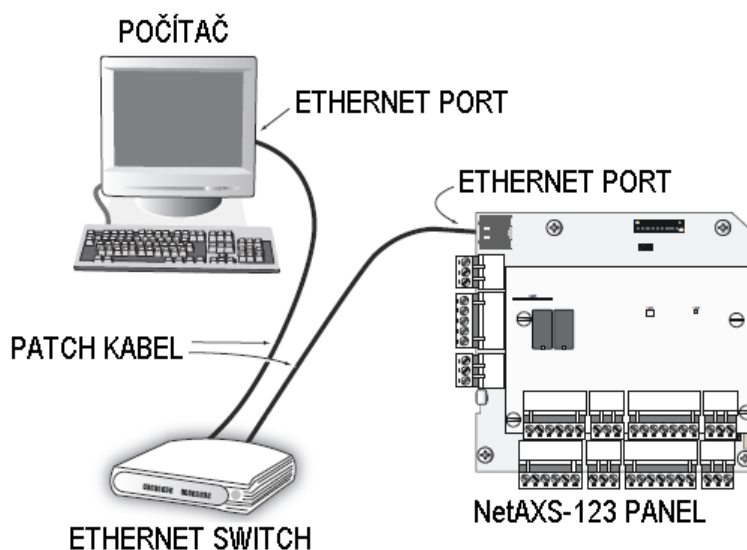
Pro konfiguraci webserveru řídicí jednotky musíme řídicí jednotku připojit k počítači. Toto lze realizovat dvěma způsoby:

- Přímé propojení počítače a řídicí jednotky – nekřížený patch kabel.



Obr. 19 – Přímé propojení počítače a panelu NetAXS-123.[7]

Zapojení přes LAN přepínač (switch).



Obr. 20 – Propojení počítače a panelu NetAXS-123 přes LAN přepínač.[7]

V následném kroku musíme nastavit v počítači IP adresu dle rozsahu IP adresy v řídicí jednotce NetAXS-123. V „Centru síťových připojení a sdílení“ vstoupíme do vlastností místní sítě (web server řídicí jednotky musí být připojen k počítači jedním ze dvou uvedených způsobů). Ve vlastnostech Internet Protocol Version 4 (TCP/IPv4) nastavíme IP adresu:

192.168.1.10

maska podsítě: 255.255.255.0

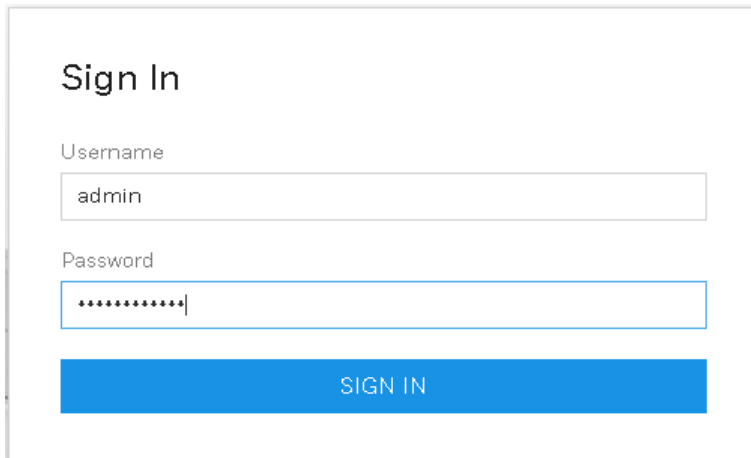
brána 192.168.1.1.

po uložení nastavení je možné na řádku internetového prohlížeče zadat IP adresu řídicí jednotky:

https://192.168.1.150

Pokud se Vám zobrazí zpráva, že připojení není bezpečné, zvolte možnost Upřesnit a zvolte volbu Pokračovat (nezabezpečně).

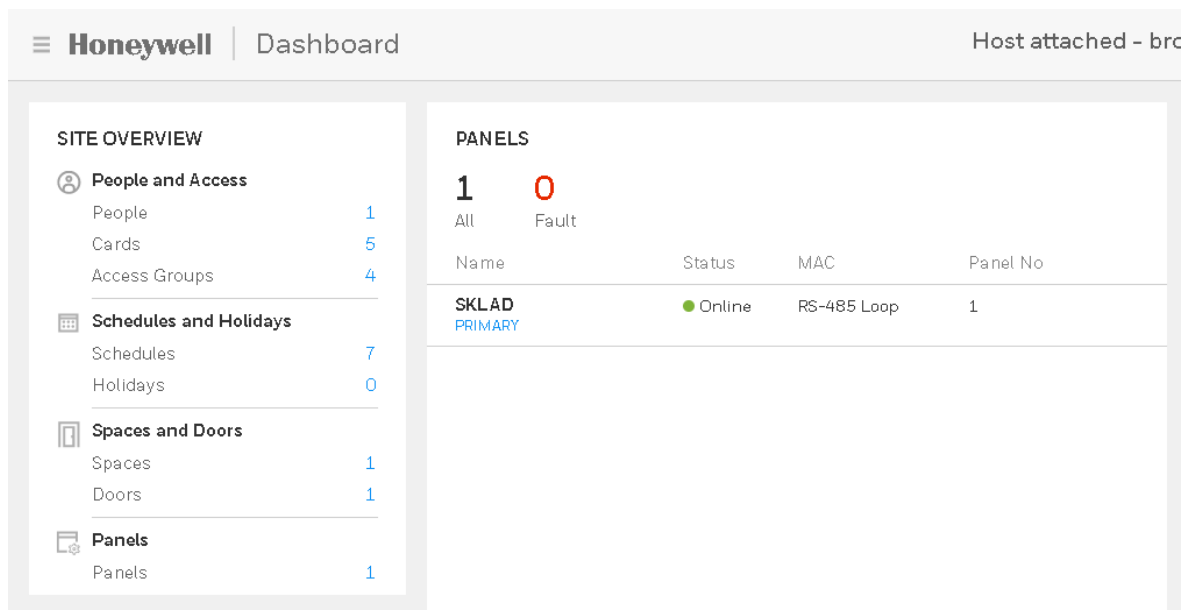
Zobrazí se přihlašovací okno. Do pole Uživatelské jméno zadejte admin a do pole Heslo zadejte admin. Obě pole rozlišují malá a velká písmena.



The image shows a web-based sign-in interface. At the top, the text 'Sign In' is displayed. Below it, there are two input fields. The first is labeled 'Username' and contains the text 'admin'. The second is labeled 'Password' and contains a series of dots, indicating a masked password. Below these fields is a prominent blue button with the text 'SIGN IN' in white capital letters.

Obr. 21 – Přihlašovací okno pro konfiguraci web serveru.[7]

Pět neplatných pokusů o přihlášení zablokuje možnost přihlásit se k webserveru na 30 minut. Při prvním přihlášení je uživatel vyzván ke změně hesla. Po úspěšném přihlášení se zobrazí základní obrazovka webserveru – Dashboard.

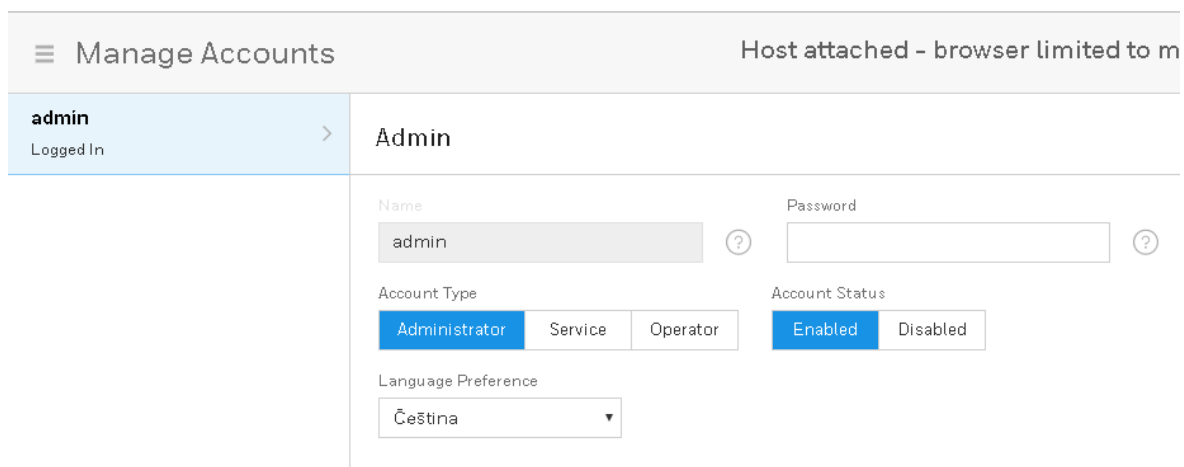


Obr. 22 – Dashboard – základní obrazovka pro konfiguraci webserveru.[Zdroj: vlastní]

Na ovládacím panelu NetAXS-123 (Dashboard) se zobrazují základní informace o systému:

- seznam všech připojených panelů,
- panely, které z jakéhokoliv důvodu nekomunikují,
- počet záznamů v databázi,
- odkazy v levém hlavním okně jsou aktivní.

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



Obr. 23 – Správa účtu, změna jazyka přes webový prohlížeč.[Zdroj: vlastní]

Základní konfigurační sekvence nastavení

1. Konfigurace Ethernet Virtual Loop (EVL)

Síť EVL umožňuje připojení řadičů do IP sítě, které jsou spravovány jako skupina prostřednictvím webserveru, který je umístěn v jednom panelu NetAXS-123. Celkem může být do jedné virtuální skupiny přiřazeno až 16 panelů NetAXS-123. Skupina je označována jako virtuální, protože způsob komunikace a řízení mezi jednotkami probíhá obdobně jako u sběrnice RS485. Panely NetAXS-123 musí být připojené ke společné podsíti LAN, která poskytuje dynamické přidělování IP adres (DHCP). Panel je v síti identifikován svou MAC adresou, pozice S1 až S5 na DIP přepínači nemají význam.

Nastavení DIP přepínačů u panelů NetAXS-123 se nastavuje u nadřazeného panelu dle tab. 5 a u podřazeného panelu podle tab. 6.

Tab. 5 – Nastavení DIP přepínače u nadřazeného panelu NetAXS-123.[7]

DIP Switch	Setting
1	On
2	Off
3	Off
4	Off
5	Off
6	On
7-10	Off, On, On, Off

Tab. 6 – Nastavení DIP přepínače u podřazeného panelu NetAXS-123.[7]

DIP Switch	Setting
1	On
2	Off
3	Off
4	Off
5	Off
6	Off
7-10	Off, On, On, Off

Důležité: Pokud máte panel NetAXS-123 před sebou dle obr.12, pak číslování jednotlivých pozic DIP přepínače označeného jako SW1 je provedeno zprava do leva! Pozice přepínače S1 je vpravo a pozice přepínače S10 je vlevo.

Vytvoření EVL

Připojte všechny panely NetAXS-123 k síti LAN. Podřazené panely musí mít nastaven DIP6=OFF. Podřazené panely budou konfigurovány přes nadřazený panel (DIP6=ON).

K nastavení komunikace se dostanete volbou:

MENU > PANEL CONFIGURATION > HOST/LOOP COMMUNICATIONS

V části Síť (NETWORK) nastavte buď dynamicky přiřazovanou IP adresu (DHCP) nebo ji zadejte jako statickou (Static). Nastavení následně uložte (SAVE).

Panel Configuration Host attached - browser limited to monitoring only

SKLAD Primary (Panel No 1)

Settings **Host / Loop Communications** Inputs Outputs Card Formats Advanced

HOST

Web WIN-PAK MAXPRO Cloud

LOOP

Mode RS-485 EVL Time Sync Enable Disable

Baud Rate (bps) 38,400 115,200 FORCE BAUD RESET

CANCEL SAVE

Obr. 24 – Nastavení hostitele Web a volba EVL. [Zdroj: vlastní]

Panel Configuration Host attached - browser limited to monitoring only

SKLAD Primary (Panel No 1)

Settings **Host / Loop Communications** Inputs Outputs Card Formats Advanced

GENERAL

Panel Name SKLAD Firmware Version 6.0.10.20 6.0.10.5 Reset

Panel Type NetAXS-123 Boot Time Thu Aug 22 19:48:29 2019 OS Version 2.6.25#107 Tue Jan 10 10:55:47 CST 2012

NETWORK

MAC Address 00:40:84:23:0EAD

Static DHCP IP Address 192.168.1.150 Subnet Mask 255.255.255.0

Default Gateway

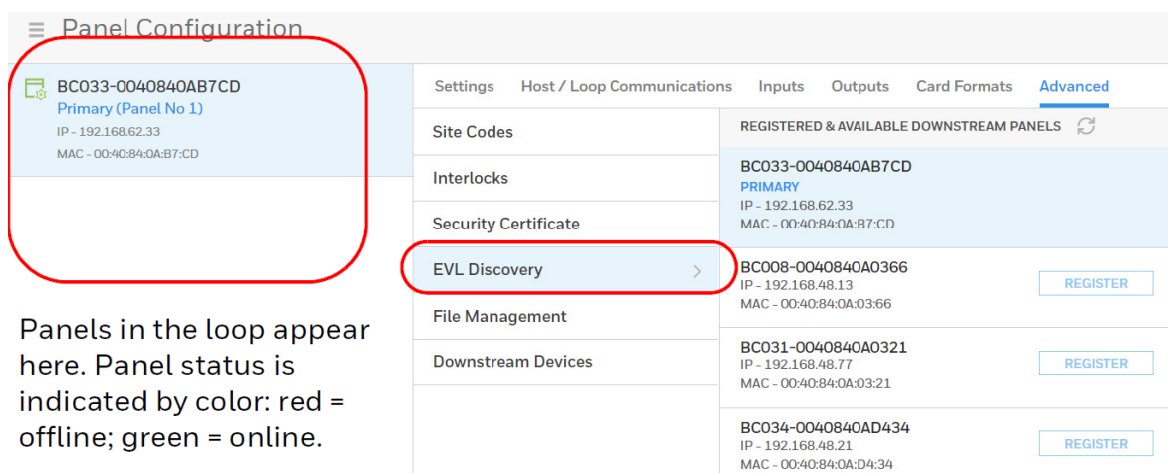
TIME MANAGEMENT Current Panel Time : Thursday, August 22, 2019 - 08:13:46 PM DST

Obr. 25 – Nastavení nadřazeného panelu NetAXS-123. [Zdroj: vlastní]

Podřazené panely NetAXS-123 se k nadřazenému panelu registrují nebo odhlašují pokud dřívější registrace panelu byla úspěšná (obr.26 a obr.27).

MENU > PANEL CONFIGURATION > ADVANCED > EVL DISCOVERY

Automaticky se zobrazí všechny nalezené panely NetAXS-123 v síti LAN. Následně se provede jejich registrace dle obr.40 (případně odhlášení pokud dřívější registrace byla úspěšná, obr.41).



Panel Configuration

Settings Host / Loop Communications Inputs Outputs Card Formats **Advanced**

Site Codes REGISTERED & AVAILABLE DOWNSTREAM PANELS

Interlocks

Security Certificate

EVL Discovery >

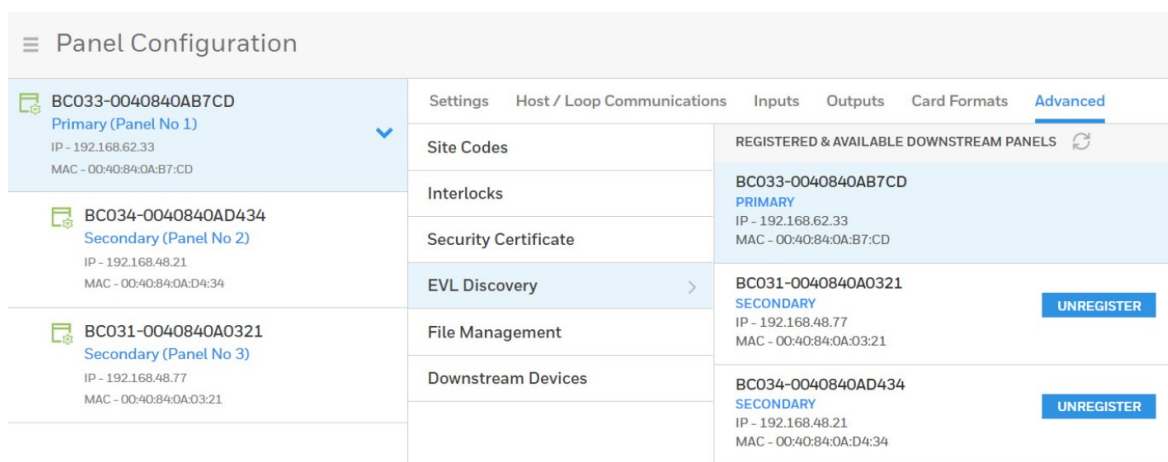
File Management

Downstream Devices

Panel ID	Status	IP	MAC	Action
BC033-0040840AB7CD	PRIMARY	192.168.62.33	00:40:84:0A:B7:CD	
BC008-0040840A0366		192.168.48.13	00:40:84:0A:03:66	REGISTER
BC031-0040840A0321		192.168.48.77	00:40:84:0A:03:21	REGISTER
BC034-0040840AD434		192.168.48.21	00:40:84:0A:D4:34	REGISTER

Panels in the loop appear here. Panel status is indicated by color: red = offline; green = online.

Obr. 26 – Registrace Podřadného panelu NetAXS-123. [7]



Panel Configuration

Settings Host / Loop Communications Inputs Outputs Card Formats **Advanced**

Site Codes REGISTERED & AVAILABLE DOWNSTREAM PANELS

Interlocks

Security Certificate

EVL Discovery >

File Management

Downstream Devices

Panel ID	Status	IP	MAC	Action
BC033-0040840AB7CD	PRIMARY	192.168.62.33	00:40:84:0A:B7:CD	
BC031-0040840A0321	SECONDARY	192.168.48.77	00:40:84:0A:03:21	UNREGISTER
BC034-0040840AD434	SECONDARY	192.168.48.21	00:40:84:0A:D4:34	UNREGISTER

Obr. 27 – Odhlášení Podřadného panelu NetAXS-123. [7]

2. Konfigurace systému s RS485 skupinou

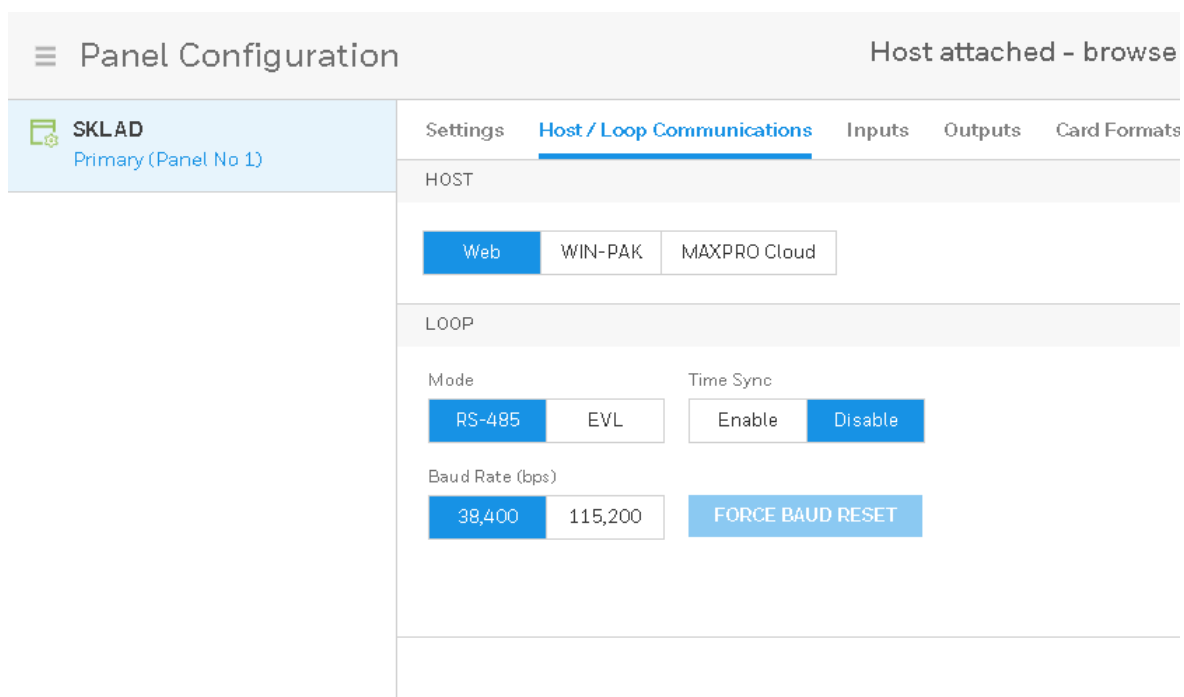
Výchozí nastavení panelu NetAXS-123 je pro řazení na sběrnici RS485. Pokud uživatel nastavil mód komunikace na EVL a následně přepnul mód komunikace na RS485, dojde k automatickému restartu panelu NetAXS-123. Na sběrnici může být zapojeno celkem 31 panelů NetAXS-123, jeden nadřazený (S6=ON) a 30 podřazených (S6=OFF). U podřazených panelů se nenastavuje IP adresa, proto je pozice S7 u DIP přepínače bez významu, přesto je

vhodné přepnout S7=OFF. U posledního podřazeného panelu se přepínají pozice S7 a S8 na DIP přepínači do pozice ON (zakončení sběrnice RS485).

Přihlásíme se k panelu NetAXS-123 prostřednictvím internetového prohlížeče a vstoupíme na konfigurační obrazovku Loop Communications:

MENU > PANEL CONFIGURATION > HOST/LOOP COMMUNICATIONS

nebo z úvodní obrazovky ***Dashboard: PANELS > HOST/LOOP COMMUNICATIONS***.



Obr. 28 – Konfigurace komunikace RS485 panelu NetAXS-123. [Zdroj: vlastní]

Zde nastavíme atributy komunikace:

- typ připojení hostitele Web,
- režim RS485,
- uložit, panel se automaticky restartuje,
- přihlášení k panelu NetAXS-123.

Všechny podřazené panely NetAXS-123, které jsou k nadřazenému panelu připojeny prostřednictvím sběrnice RS485 se zobrazí v seznamu jako registrované. Pokud potřebujeme některý z panelů odhlásit, pak si zobrazíme příslušnou konfigurační obrazovku:

MENU > PANEL CONFIGURATION > ADVANCED > RS485 UNREGISTER

3. Správa konfiguračních dat

Konfigurační data jsou spravována v rámci skupiny panelů NetAXS-123 (EVL). Konfigurační data se dělí na sdílená (stejná pro všechny panely ve skupině) a specifická (jen pro příslušný panel).

Mezi sdílená data patří:

Plány – časové rozvrhy; Karty; Formáty karet; Svátky; Názvy přístupových skupin; Konfigurace (site codes).

Mezi data specifická pro panel patří:

Přístupové skupiny a plány přiřazené čtečkám; Konfigurace prostor/dveře/čtečka; Konfigurace panelu (obecné, verze firmware, síť, komunikace); Web uživatelé).

Konfigurace komunikace hostitel/skupina

Nastavujeme jeden ze tří režimů:

- Režim hostitel (jen sledování systému) – pomocí programu WIN-PAK nebo MAXPRO Cloud, připojují se k nadřazenému panelu NetAXS-123, se kterým komunikují. Sledujeme stav systému.
- Režim Web (konfigurace a sledování systému) – připojení k webserveru panelu umožňuje jeho konfiguraci a sledování stavu systému.

Nastavení parametrů komunikace pro režim hostitele

Přecházíme na konfigurační obrazovku Host/Loop Communications:

MENU > PANEL CONFIGURATION > HOST/LOOP COMMUNICATIONS

nebo z úvodní obrazovky ***Dashboard > PANELS > HOST/LOOP COMMUNICATIONS***.

Panel Configuration Host attached - browser limited to monitoring

SKLAD Primary (Panel No 1)

Settings **Host / Loop Communications** Inputs Outputs Card Formats Advanced

HOST

Web **WIN-PAK** MAXPRO Cloud

WIN-PAK

Connection (TCP/IP) Communication Host IP Address Port

Direct Reverse Non Ack/NAK **Ack/NAK** 0.0.0.0 3001

Generate Key Disable Encryption

Encryption Key

LOOP

Connection Time Sync

RS-485 Enable Disable

Baud Rate (bps)

38,400 115,200 **FORCE BAUD RESET**

Obr. 29 – Nastavení parametrů komunikace pro režim hostitele. [Zdroj: vlastní]

Možnosti nastavení komunikace hostitel/skupina v režimu hostitele WIN-PAK

Typ připojení:

- Určuje typ fyzického spojení mezi hostitelem a serverem nadřazeného panelu. Pokud je připojení realizováno z hostitelského programu WIN-PAK, pak lze vybrat jednu ze dvou možností:
 - Přímé připojení přes TCP/IP – WIN PAK inicializuje připojení k panelu.
 - Reverzní připojení TCP/IP – panel se připojuje přímo k WIN PAKU pomocí protokolu TCP/IP. Musí se zadat hostitelská IP adresa do pole pro IP. Panel inicializuje připojení k hostiteli (WIN-PAK).

Typ komunikace:

- Ack/NAK – doporučený způsob komunikace. Při komunikaci poskytuje informaci o přijetí nebo nepřijetí dat.
- Non Ack/NAK – používá se při řešení problémů. Přenos není potvrzován.

Hostitelská IP adresa:

- pokud je vybrán reverzní typ připojení, pak se do pole pro IP adresu uvádí adresa hostitelského systému (WIN-PAK serveru).

Číslo portu:

- 2101 je výchozí šifrovaný port,
- 3001 je port pro přímé připojení přes TCP/IP,
- 5001 je port pro reverzní připojení TCP/IP.

Generovat klíč:

- zaškrtnutí této volby generuje nový šifrovací klíč. Každým zaškrtnutím a uložením je generován nový klíč, který musí být zapsán do WIN-PAKu.

Zákaz šifrování:

- zaškrtnutím této volby se zakáže šifrovaná komunikace mezi nadřazeným panelem NetAXS-123 a systémem hostitele WIN-PAK. Tato volba se nedoporučuje z hlediska nezabezpečeného přenosu dat.

Šifrovací klíč:

- heslo, klíč pro šifrování komunikace mezi nadřazeným panelem NetAXS-123 a systémem hostitele WIN-PAK. Uvedený klíč se musí zadat do systému hostitele WIN-PAK.

Možnosti nastavení skupiny

Typ připojení:

- RS485 – pokud nadřazený panel poskytuje přístup ke skupině připojené sběrnici RS485.

Synchronizace času:

- Synchronizuje čas mezi nadřazenými a podřazenými panely. Pokud je povolen, pak je automaticky vysílán synchronizační pulz z nadřazeného panelu do podřazených panelů ve zvoleném intervalu 60 – 32767 minut.

Přenosová rychlost:

- určuje přenosovou rychlost mezi podřazenými panely (bity za sekundu). Volbou vynutit reset se nastaví zvolená přenosová rychlost do všech podřazených panelů.

Volbou uložit se nastavené parametry uloží.

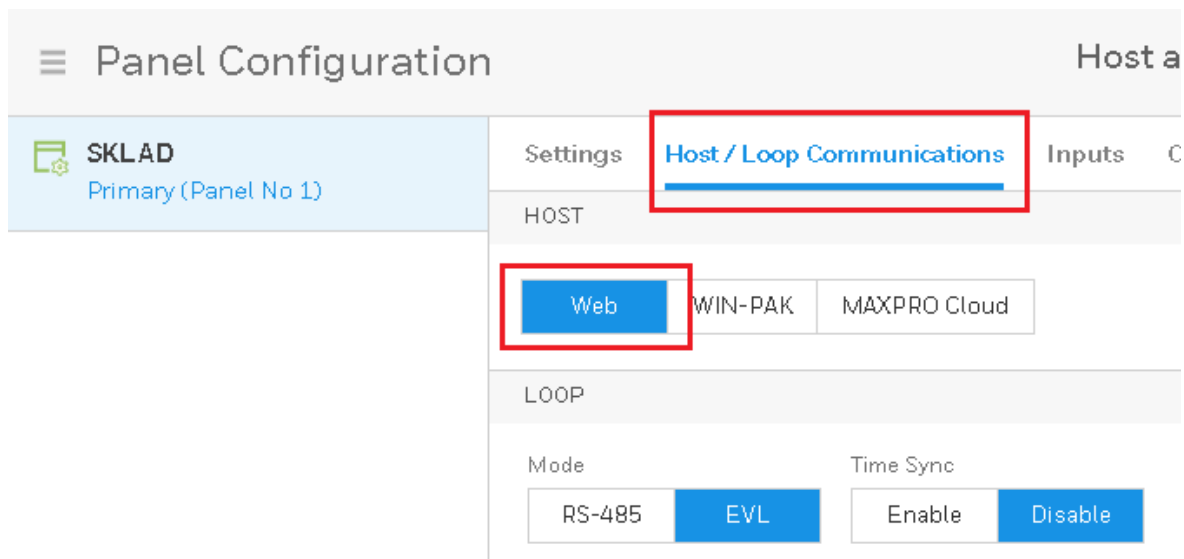
Nastavení parametrů komunikace pro režim Web

Přecházíme na konfigurační obrazovku Host/Loop Communications:

MENU > PANEL CONFIGURATION > HOST/LOOP COMMUNICATIONS

nebo z úvodní obrazovky **Dashboard > PANELS > HOST/LOOP COMMUNICATIONS**

V záložce Hostitel se vybere možnost Web.



Obr. 30 – Nastavení parametrů komunikace pro režim Web. [7]

Možnosti nastavení komunikace hostitel/skupina v režimu hostitele Web

Režim:

- RS485 – pokud nadřazený panel poskytuje přístup k podřazeným panelům přes sběrnici RS485.
- EVL – pokud nadřazený panel poskytuje přístup k virtuální skupině podřazených panelů připojených k LAN síti.

Synchronizace času:

- Synchronizuje čas mezi nadřazenými a podřazenými panely. Pokud je povolen, pak je automaticky vysílán synchronizační pulz z nadřazeného panelu do podřazených panelů ve zvoleném intervalu 60 – 32767 minut.

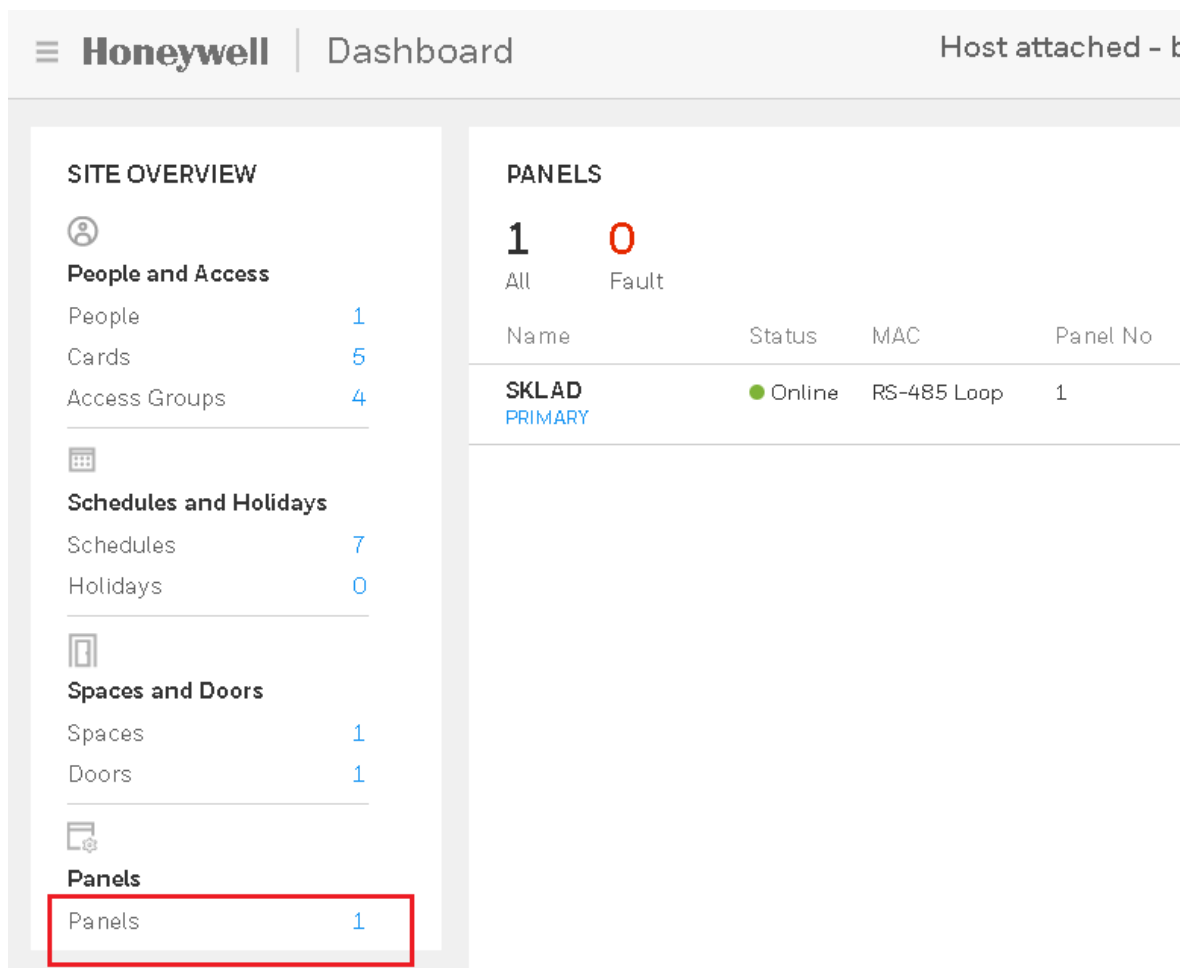
Přenosová rychlost:

- určuje přenosovou rychlost mezi podřazenými panely (bity za sekundu). Volbou vyvolat reset se nastaví zvolená přenosová rychlost do všech podřazených panelů.

Volbou uložit se nastavené parametry uloží.

4. Prvotní nastavení panelu

Pro přístup do konfigurační obrazovky nastavení panelu zvolte: Dashboard: PANELS



The screenshot shows the Honeywell Dashboard interface. The top navigation bar includes the Honeywell logo, the word 'Dashboard', and the text 'Host attached - k'. The main content area is divided into two columns. The left column, titled 'SITE OVERVIEW', contains several sections: 'People and Access' with 1 person, 5 cards, and 4 access groups; 'Schedules and Holidays' with 7 schedules and 0 holidays; 'Spaces and Doors' with 1 space and 1 door; and 'Panels' with 1 panel. The 'Panels' section is highlighted with a red box. The right column, titled 'PANELS', shows a summary with 1 'All' and 0 'Fault' panels. Below this is a table with the following data:

Name	Status	MAC	Panel No
SKLAD PRIMARY	● Online	RS-485 Loop	1

Obr. 31 – Přístup k nastavení panelu. [Zdroj: vlastní]

Po zvolení odkazu Panels se zobrazí konfigurační obrazovka nastavení panelu (obr.31).

Konfigurační okno v záložce Nastavení je členěno na čtyři oddíly:

1. Hlavní.

Zde se nastavuje jméno panelu, předvyplněná je MAC adresa panelu.

2. Síť.

Je zde vypsána MAC adresa panelu. Nastavujeme, zda bude IP adresa statická nebo bude přidělována DHCP serverem. Statickou adresu vyplňujeme, včetně masky podsítě a defaultní gateway.

Panel Configuration Host attached - browser limit

SKLAD
Primary (Panel No. 1)

Settings Host / Loop Communications Inputs Outputs Card Formats Advanced

GENERAL

Panel Name: SKLAD Firmware Version: 6.010.20 6.0105 [Reset]

Panel Type: NetAXS-123 Boot Time: Thu Aug 22 19:48:29 2019 OS Version: 2.6.25#107 Tue Jan 10 10:55:47 CST 2012

NETWORK

MAC Address: 00:40:84:23:0EAD

Static DHCP IP Address: 192.168.1.150 Subnet Mask: 255.255.255.0 Default Gateway:

TIME MANAGEMENT Current Panel Time : Thursday,

Format (in hr): 12 24

Geographic Time Zones: Europe/Budapest New Date: [Calendar Icon] New Time (H.M): [AM] [PM]

Obr. 32 – Konfigurační obrazovka nastavení panelu. [Zdroj: vlastní]

3. Nastavení času.

- Nastavujeme formát zobrazení času 12 nebo 24 hodin.
- Nastavujeme nové datum a čas.
- Nastavujeme geografickou časovou zónu.
- Lze povolit časový server a zadává se jeho IP adresa, určuje se interval aktualizace.
- Vynucení aktualizace času s časovým serverem.

4. Konfigurace nastavení chování.

BEHAVIOUR SETTINGS

Anti-Passback: [Enable] [Disable]

Free Egress: [Enable] [Disable] Detect Duress: [Enable] [Disable] Continuous Card Reads: [Enable] [Disable] Password Expiration: [Enable] [Disable] Reverse LED Colour: [Enable] [Disable]

Web Session Timeout: 30 [Minutes] [Hours]

Obr. 33 – Konfigurační obrazovka nastavení chování panelu. [7]

V části konfigurace nastavení chování panelu můžeme povolit/ zakázat následující:

Anti-Passback:

je-li tato funkce aktivována, pak je vyžadováno, aby uživatel používal kartu při průchodu přes čtečky vždy ve správném pořadí, tzn. pokud prošel čtečkou, která je označená jako „vstupní“ (do zabezpečené oblasti), pak jeho následný průchod musí být přes čtečku, která

je označena jako „odchozí“ (ze zabezpečené oblasti). Pokud není pořadí průchodu dodrženo, pak nedojde k povolení vstupu u druhé „vstupní“ nebo „odchozí“ čtečky.

Volný výstup:

Konfiguruje panel pro volný výstup. Pokud je povoleno (výchozí nastavení), pak panel automaticky konfiguruje vstupy 1, 9 a 13 tak, aby fungovaly jako výstupy pro dveře 1, 2 a 3. Pokud jsou deaktivovány, lze tyto vstupy 1, 9 a 13 použít jako obecné vstupy.

Detect Duress:

Nastavení výstupu, který se aktivuje v případě zadání „nátlakového PIN“. Tento PIN se liší v poslední cifře platného kódu, která je o jedničku vyšší nebo nižší. Uživateli je umožněn průchod, ale současně je spuštěn tichý poplach – zadání přístupového kódu pod nátlakem.

Nepřetržitě čtení karet:

Umožňuje číst kartu, i když je výstup aktivní po použití předchozí karty. Ve výchozím nastavení panelu je tato možnost povolena. Pokud je možnost zakázána, pak použití následné karty je možné až po přechodu dříve aktivovaného výstupu do výchozího stavu.

5. Nastavení plánu – časových zón

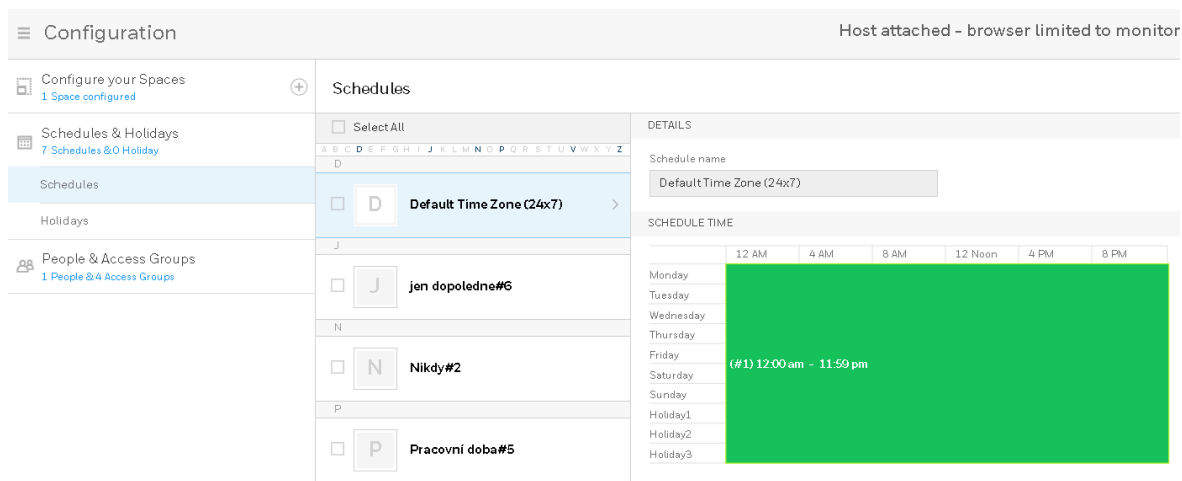
Panel NetAXS-123 řídí přístup prostřednictvím plánů a časových zón. Vstupy, výstupy, čtečky, přístupové skupiny a karty prostřednictvím přístupových skupin jsou svázané s časovými scénáři, podle kterých budou aktivovány, deaktivovány, povoleny nebo zakázány.

Konfigurační rozhraní časových zón umožňuje:

- Vytvářet plány, podle kterých je panelem řízena aktivita vstupů, výstupů, čteček, přístupových skupin.
- Upravovat časové zóny.
- Smazat časové zóny.
- Definovat svátky.

Pro přístup do konfigurační obrazovky nastavení časových zón lze zvolit odkaz

MENU > CONFIGURATION > SCHEDULES&HOLIDAYS > SCHEDULES



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

Vytvoření časové zóny.

Pro vytvoření nové časové zony slouží ikona + v kolečku v pravém horním rohu obrazovky. U časové zóny zadáváme název a časovou oblast – pohybem kurzoru v grafickém poli dnů a hodin. Nastavení uložíme volbou uložit, která je v pravém dolním rohu obrazovky.

Úprava časové zóny.

V abecedním seznamu časových zón lze vybrat písmeno, kterým začíná časová zóna, která má být upravena. Následně je možné vybrat příslušnou časovou zónu dvojklikem kurzoru. V grafickém poli je možné provést příslušné změny a ty následně uložit.

Smazání časové zóny.

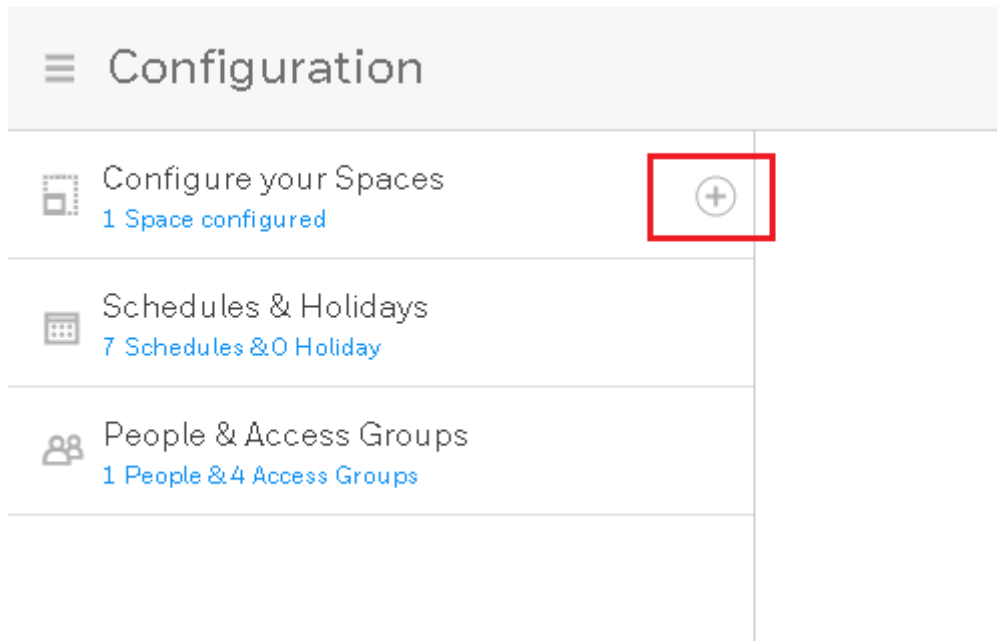
Nelze smazat časovou zónu, která je používána. Vyberte příslušnou časovou zónu, v pravém horním rohu obrazovky zvolte ikonu “koš” pro smazání vybrané časové zóny. Vybraná operace vyžaduje potvrzení, a po potvrzení smazání je možné operaci uložit.

6. Konfigurace prostor

Než bude možné přistoupit ke konfiguraci dveří, bude nutné dveře přiřadit oblasti (prostoru).

Přístup do konfiguračního okna nastavení oblasti:

DASHBOARD > SPACES nebo MENU > CONFIGURATION > Configure your Spaces



Obr. 35 – Přístup ke konfigurační obrazovce nastavení oblastí. [Zdroj: vlastní]

Pokud jsou všechny dveře přiřazené do oblastí, pak se o tomto stavu zobrazí informační zpráva a novou oblast nebude možné vytvořit.

ASSIGN DOORS TO A SPACE

Name your Space

AVAILABLE DOORS		ADDED DOORS
Door1.1 - Panel 1	+	
Door1.2 - Panel 1	+	
Door1.3 - Panel 1	+	

CANCEL SAVE

Obr. 36 – Přiřazení dveří do oblastí. [7]

Vytvořenou oblast je možné pojmenovat. Volbou + u dostupných dveří dojde k jejich přesunutí do pravého okna „Přidané dveře“. Po přiřazení požadovaných dveří do vytvoření oblasti lze nastavení uložit – volba v pravém dolním rohu obrazovky.

Nelze smazat dveře, které jsou přiřazené do oblasti, před smazáním je nutné dveře z oblasti odebrat.

7. Konfigurace dveří

Každý panel NetAXS-123 podporuje řízení 1 až 3 dveří. Pro každé dveře je nutné provést konfiguraci čteček, vstupů a výstupů. Přístup ke konfiguračnímu oknu dveří je umožněn:

MENU > CONFIGURATION nebo DASHBOARD > SPACES

Výběr Configure your Space rozbílí skupinu MASTER, pod kterou jsou jednotlivé dveře.

Obr. 37 – Konfigurace nastavení dveří. [Zdroj: vlastní]

V první záložce konfigurační obrazovky „Čtečky“ lze pojmenovat obě čtečky (A i B), nastavit časové zóny a přístupové režimy. Povolit nebo zakázat Anti-Passback a Duress Output.

U přístupových režimů se volí typ přístupu:

Vedoucí (Supervisor) – umožňuje přístup bez povolení obecného přístupu. Je-li tento režim povolen, LED kontrolky čtečky změny barvy čtyřikrát za sekundu.

Doprovod (Escort) – Doprovodný režim vyžaduje doprovod vedoucího, aby umožnil vstup držiteli karty s tímto typem přístupu.

Dále se ve stejném okně nastavuje Anti-passback a Duress Output pro dané dveře:

Antipassback – u nastavení se rozlišuje „těžká“ a „lehká“ varianta. U „lehké“ varianty anti-passbacku dojde při druhém přiložení karty na stejný typ čtečky k narušení antipassbacku, ale uživateli je povolen průchod.

Duress Output – použití nátlakového kódu pro aktivaci definovaného výstupu. Nátlakový kód se liší od přístupového kódu v hodnotě poslední cifry, která je o jedničku nižší nebo vyšší.

Ve druhé záložce konfiguračního okna dveří se nastavují „Vstupy“:

- Název vstupu.
- Režimy a vlastnosti vstupu.
- Přemostění a deaktivace.

The screenshot shows the configuration interface for 'Door1.1' in the 'Inputs' tab. On the left, there is a sidebar with 'Egress Input 1' selected. The main area is divided into sections: 'GENERAL' with a 'Name' field containing 'SKLAD - Odch.tl.dveří 1 V'; 'INPUT MODES' with 'Normally' set to 'Closed', 'State' set to 'Unsupervised', 'Resistor value' set to '1k', and 'Auto-Relock' set to 'Disable'; and 'SHUNT AND DEBOUNCE' with 'Shunt Time (H:M:S)' set to '0:0:0' and 'Debounce Time (sec)' set to '0'.

Obr. 38 – Záložka „Vstupy“ konfigurace dveří. [Zdroj: vlastní]

Ve třetí záložce konfiguračního okna dveří se nastavují „Výstupy“:

Konfigurace a nastavení výstupů se provádí přes skupinu výstupů v okně konfigurace panelu.

Door1.1

Readers Inputs **Outputs**

Lock
Output 1

Discrete Group 1

Reader LED
Output 2

GENERAL

Name SKLAD - Zámek dveří 1 V0 Pulse (H:M:S) 0 0 10

Latch Enable Disable Interlocks Enable Disable TZ Card Toggle Enable Disable

First Card Rule Enable Disable

SCHEDULING

Energized Choose a Schedule Disable Interlocks Choose a Schedule

Obr. 39 – Záložka „Výstupy“ konfigurace dveří. [Zdroj: vlastní]

Settings Host / Loop Communications Inputs **Outputs** Card Formats Advanced

Individual Groups

SKLAD - Pom. V0t.3
Auxiliary Output 3

GENERAL

Name SKLAD - Pom. V0t.3 Pulse (H:M:S) 0 0 10

Latch Enable Disable Interlocks Enable Disable

SCHEDULING

Energized Choose a Schedule Disable Interlocks Choose a Schedule

Obr. 40 – Přejít na konfiguraci „Samostatného výstupu“. [Zdroj: vlastní]

U samostatného výstupu se zadává název výstupu, doba aktivace výstupu – maximální doba aktivace výstupu je 1:45:59 (h:mm:ss). Dále je možné výstup nastavit jako přepínací kontakt, nebo přiřadit kontaktu časovou zónu, ve které výstup aktivní, nebo programově výstup blokovat nebo přemostovat.

Konfigurace skupin výstupů

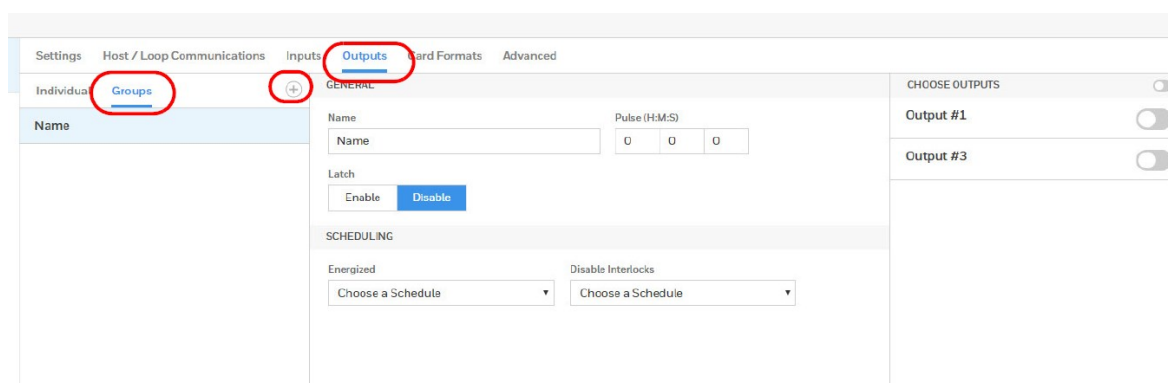
Před vytvořením skupiny výstupů musí být alespoň jeden výstup definován.

Na záložce Výstupní skupiny je možné konfigurovat následující:

- Název skupiny výstupů.
- Doba aktivace výstupů skupiny.
- Zakázat/ povolit překlápění.
- Aktivace výstupů skupiny dle časové zóny.
- Zakázat blokování výstupů skupiny dle časové zóny.

Přístup k nastavení „Skupiny výstupů“:

MENU > PANEL CONFIGURATION > OUTPUTS > GROUPS



Obr. 41 – Konfigurační okno nastavení „Skupiny výstupů“. [7]

8. Nastavení formátů karet

Formát karty určuje panelu jak bude číst číslo karty. Přístup k nastavení formátu karet:

DASHBOARD > PANELS > CARD FORMATS nebo

MENU > CONFIGURATION > CARD FORMATS

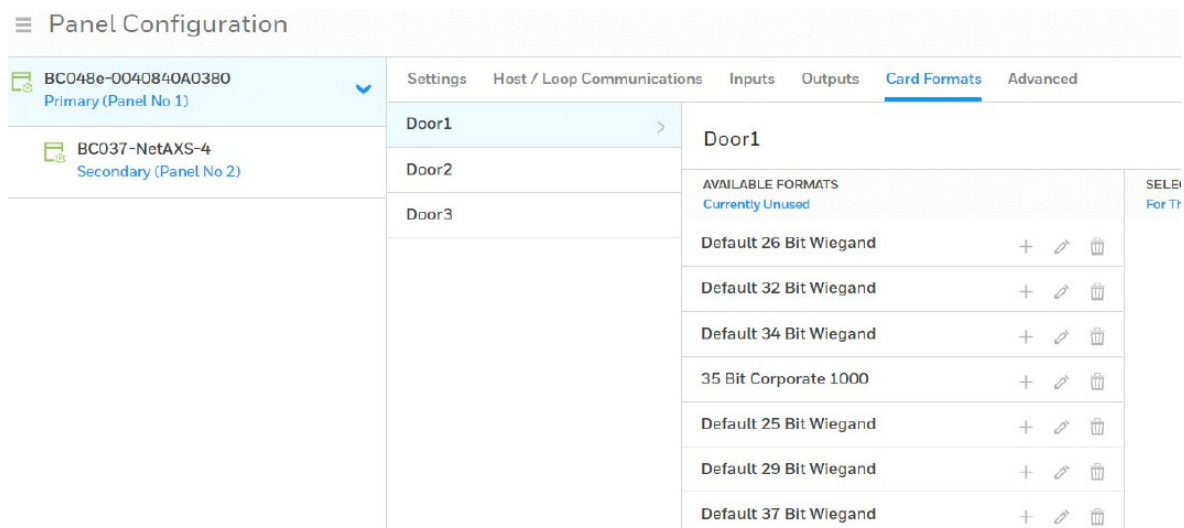
Nastavení formátu karet:

Dostupné formáty – seznam všech dostupných formátů karet pro panely.

Vybrané formáty – uvádí konkrétní formáty vybrané uživatelem z nabídky Dostupné formáty. Pokud je vybrán alespoň jediný formát, pak jsou ignorovány všechny formáty uvedené ve sloupci Dostupné formáty.

System umožňuje přidat do seznamu formátů karet vlastní formát.

Po výběru formátů karet pro jednu dveře je možné nastavení uložit a pokračovat nastavením formátů karet pro další dveře.



Obr. 42 – Konfigurační okno nastavení „Formátů karet“. [7]

9. Konfigurace lidí a karet

Konfigurace lidí:

V záložce “lidé” v konfigurační obrazovce “Lidé a karty” lze provést následující nastavení:

- Vytvořit záznam osoba včetně přiřazení/přidání karty.
- Upravit záznam osoba.
- Odstranit záznam osoba.

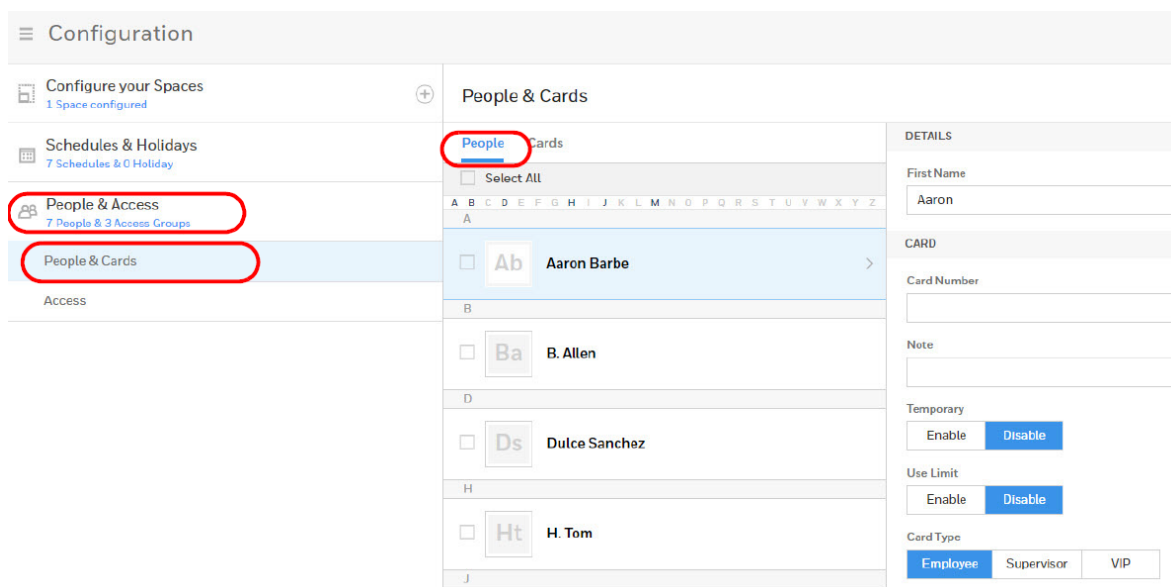
Záznam osoba lze nastavit tak, aby měla přiřazen jedne ze tří možných typů karet: vedoucí, zaměstnanec a VIP.

Přístup k nastavení záznamu osob:

DASHBOARD > PEOPLE nebo

MENU > CONFIGURATION > PEOPLE&ACCESS > PEOPLE&CARDS

Zde je možné vytvořit novou osobu volbou symbolu + v kroužku v pravém horním rohu obrazovky. U nové osoby vyplňujeme jméno a příjmení, zadáváme číslo karty nebo vybíráme ze seznamu dostupných karet. Můžeme zadat přístupový kód (PIN). Volitelně lze u osoby zadat poznámku (20 znaků), lze zapnout nebo vypnout sledování, při volbě dočasného typu použití se zadává datum ukončení platnosti, lze zadat typ přístupu: vedoucí, zaměstnanec, VIP (obr.42).



Obr. 43 – Konfigurační okno nastavení „Záznamu osob“. [7]

Konfigurace karet:

Rozhraní pro konfiguraci karet umožňuje vytvářet záznamy s těmito údaji:

- Číslo karty.
- Jméno držitele karty.
- Typ karty.
- Osobní identifikační číslo (PIN).
- Sledování (trasování).
- Datum platnosti.
- Poznámka.
- Přístupové skupiny.

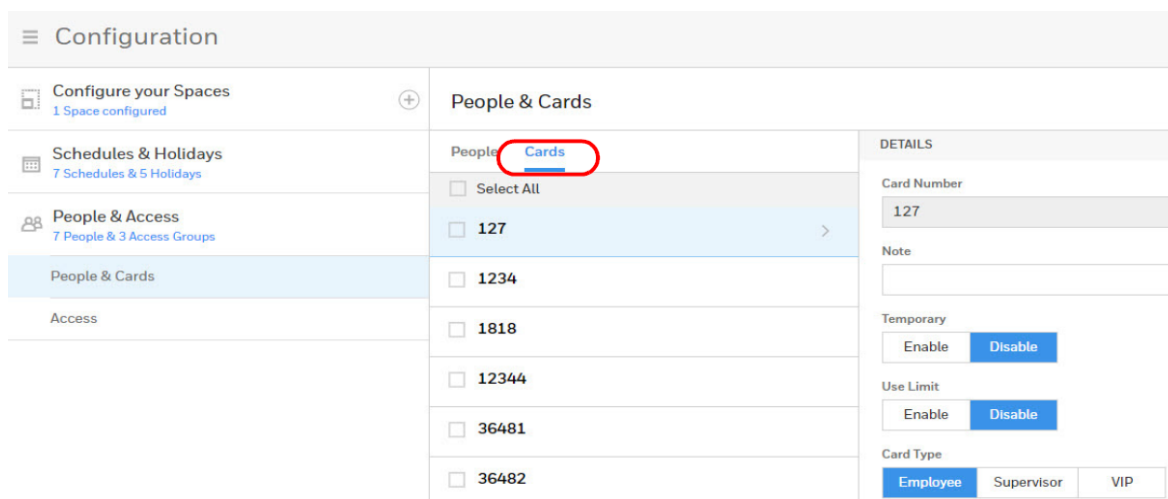
Poznámka: jedná osoba může být držitelem více karet.

Přístup k nastavení záznamu karet:

Dashboard: PEOPLE&CARDS > CARDS nebo

MENU > CONFIGURATION > PEOPLE&ACCESS > PEOPLE&CARDS > CARDS

Zde je možné vytvořit novou kartu volbou symbolu + v kroužku v pravém horním rohu obrazovky (obr.43). U jedné karty zadáváme číslo u více karet zadáváme rozsah čísel. Můžeme zadat PIN, poznámku, zapnout sledování, zvolit dočasné použití karty nebo omezení maximálním počtem přístupů (1 – 255).



Obr. 44 – Konfigurační okno nastavení „Karet“. [7]

10. Konfigurace přístupových skupin

Každé kartě je přidělena přístupová skupina, která specifikuje časový rozvrh, během kterého může být držitel karty umožněn průchod konkrétními dveřmi.

V konfiguračním okně „Přístupových skupin“ lze nastavit:

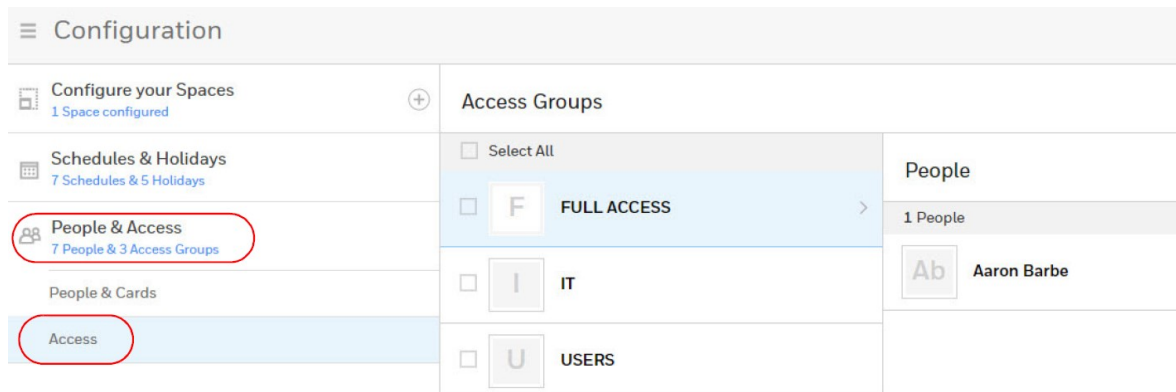
- Vybrat čtečku A nebo B (je-li definována) pro každé dveře.
- Vytvořit přístupovou skupinu.
- Upravit přístupovou skupinu.
- Odstranit přístupovou skupinu.
- Nastavit časovou zónu pro každé dveře.
- Zobrazit další panely se čtečkami v této přístupové skupině.

Před konfigurací přístupové skupiny je nutné mít provedenu konfiguraci dveří, osoby a časové zóny.

Přístup k nastavení přístupové skupiny:

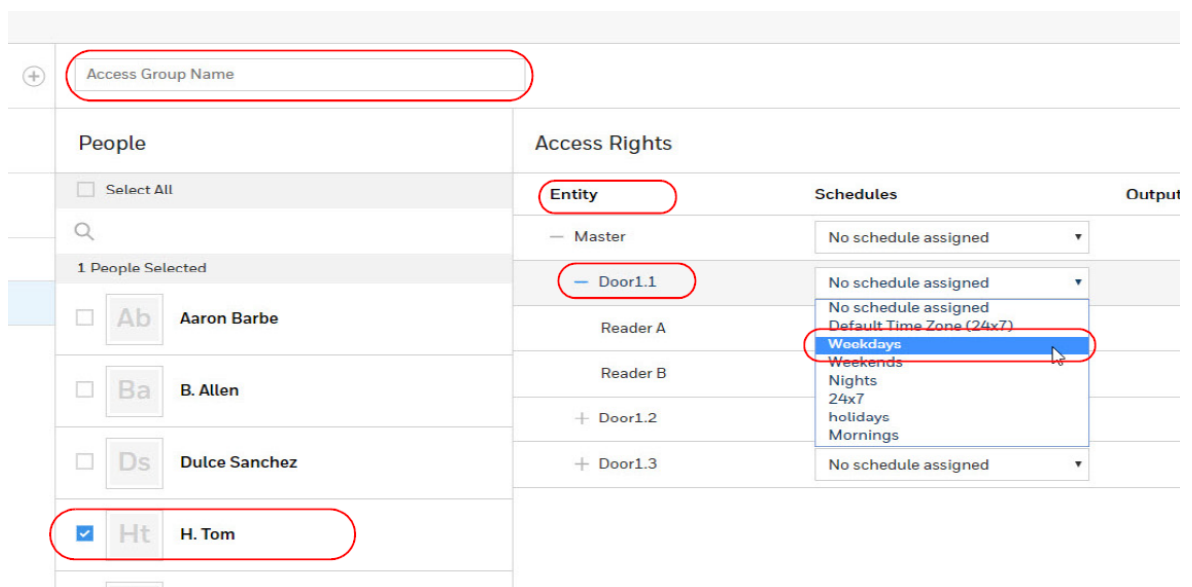
DASHBOARD > ACCESS GROUPS > CREATE AN ACCESS GROUP nebo

MENU > CONFIGURATION > PEOPLE&ACCESS > ACCESS > CREATE AN ACCESS GROUP



Obr. 45 – Konfigurační okno nastavení „Přístupové skupiny“. [7]

Zde je možné vytvořit novou přístupovou skupinu volbou symbolu + v kroužku v pravém horním rohu obrazovky (obr.44). Nově vytvořenou přístupovou skupinu pojmenujeme v poli pro název. Ve sloupci Lidé se vyberou osoby, které budou patřit do nové přístupové skupiny. Ve sloupci přístupových práv se vyberou dveře a časové zóny platné pro novou přístupovou skupinu (obr. 45). Nastavení se uloží.



Obr. 46 – Vytvoření nové přístupové skupiny. [7]

9.2 Sledování stavů systému a podávání zpráv

System NetAXS-123 umožňuje sledovat následující události:

Poplach: Poplachy jsou události nebo systémové stavy, kterým je přiřazen stav poplach, včetně použití neplatných karet nebo neautorizovaný průchod

Událost: Události jsou zaznamenány systémové stavy, například stav dveří, změna v databázi, zneplatnění karty, autorizace karty ... atp.

Dveře: Dveře jsou soubory vstupů a výstupů panelu spojené se čtečkami.

Vstupy: Vstupy jsou prezentovány svorkovnicí, která je umístěna na panelu a jsou připojené k výstupnímu zařízení, například snímač polohy dveří, odchodové tlačítko ... atp.

Výstupy: Výstupy jsou relé umístěné na panelu, a která jsou připojená k výstupnímu zařízení, například elektromagnetický zámek nebo siréna ... atp.

Sledování poplachů a událostí

Poplachu jsou zprávy generované systémem, které mají za úkol vzbudit pozornost uživatele. Pro sledování poplachů a událostí je nutné přejít do samostatného okna.

Události jsou generovány panelem i webem. Panel zaznamenává události vytvoření kartami a čtečkami. Web zaznamenává události spojené s přihlášením operátorů do systémů.

Přístup k zobrazení okna poplachů a událostí:

MENU > ALARMS&EVENTS > ACCESS > CREATE AN ACCESS GROUP

Date/Time	Panel Number	Device Name	Space	Severity	Type	LN	PN	Cred-PIN/Site	Card Holder Name
01/29/2018 18:00:55	11	Input 11: Door 2 TMPR-A	Space1, Door11.2	CRITICAL	Alarm State	11	4	0	
01/29/2018 18:00:55	11	NX3Big-P11 - Door 2 Statu	Space1, Door11.2	CRITICAL	Alarm State	10	3	0	
01/29/2018 18:00:55	27	Input 11: Door 2 TMPR-A	Space1, Door27.2	CRITICAL	Alarm State	11	4	0	
01/29/2018 18:00:55	15	NX3Big-P15 - Door 2 Statu	Space1, Door15.2	CRITICAL	Alarm State	10	3	0	
01/29/2018 18:00:55	27	NX3Big-P27 - Door 2 Statu	Space1, Door27.2	CRITICAL	Alarm State	10	3	0	
01/29/2018 18:00:55	11	Aux IO Board Devices		NORMAL	Online	0	0	0	
01/29/2018 18:00:55	12	Input 16: Door 3 TMPR-B	Space1, Door12.3	CRITICAL	Alarm State	16	9	0	
01/29/2018 18:00:55	15	Aux IO Board Devices		NORMAL	Online	0	0	0	
01/29/2018 18:00:55	12	Input 15: Door 3 TMPR-A	Space1, Door12.3	CRITICAL	Alarm State	15	8	0	
01/29/2018 18:00:55	27	Aux IO Board Devices		NORMAL	Online	0	0	0	

Obr. 47 – Okno pro sledování poplachů a událostí. [7]

Podávání zpráv

Generování zpráv o událostech

Přístup k zobrazení okna poplachů a událostí:

MENU > ALARMS&EVENTS > ACCESS > CREATE AN ACCESS GROUP

V pravém horním rohu jsou volby „Stážení poplachů/událostí“ a „Stážení webových událostí“ (obr. 46). Volbou jednoho nebo druhého stažení se objeví dialogové okno, které upozorní, že stažený soubor není zabezpečený. Po potvrzení se data generují do excelovské tabulky, která se zobrazí na spodním panelu nástrojů prohlížeče. Kliknutím se otevře stažená sestava v excelu.

Další možnosti vytvářet přehledy událostí systém umožňuje:

- Generování diagnostických zpráv.
- Vytváření zpráv o lidech a kartách.

10 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. 48 – Verze a návaznosti WIN-PAK.[6]

10.1 Konfigurace demonstračního panelu s využitím WIN-PAKu

Níže je uveden podrobný postup všech nutných kroků pro připojení panelu NetAXS-123 k softwarovému programovému prostředí WIN-PAK.

1. Připojení panelu NetAXS-123 k počítači, viz obr.20 a obr.21.

Nastavení lokální sítě:

IP adresa panelu (defaultní) 192.168.1.150

Maska podsítě 255.255.255.0

Nastavení IP adresy v počítači se provede:

Centrum síťových připojení > Připojení k místní síti > Vlastnosti > Protokol IP verze 4 (TCP/IPv4) > Vlastnosti > Použít následující adresu:

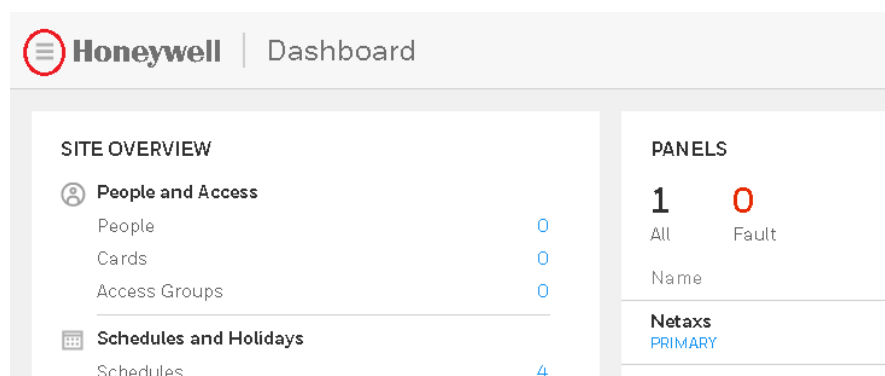
IP adresa počítače 192.168.1.10

Maska podsítě 255.255.255.0

Výchozí brána 192.168.1.1

IP adresa může být libovolná, ale v rozsahu podsítě panelu.

Pokud potřebujeme panel NetAXS-123 včlenit do stávající sítě LAN, pak po přihlášení do webového konfiguračního prostředí volíme:



Obr. 49 – Ikona pro vstup do MENU webového konfiguračního prostředí panelu NetAXS-123 [Zdroj: vlastní]

Dashboard: Menu > Panel Configuration > NETWORK

Kde se nastaví typ IP adresy (Pevná/přidělená DHCP serverem), dále se nastaví IP adresa v rozsahu podsítě, do které bude panel zařazen, maska podsítě a případně výchozí brána (dle požadavku na nastavení sítě LAN). Změnu uložíme. Systém vyžaduje před uložením

vyplnit nastavení času ve stejném konfiguračním okně webového prostředí. Dále musíme přistoupit ke změně IP adresy v počítači dle výše popsaného postupu, ale zadáváme IP adresu v rozsahu nově zadané sítě LAN panelu NetAXS-123.

2. Spuštění konfiguračního webového prostředí.

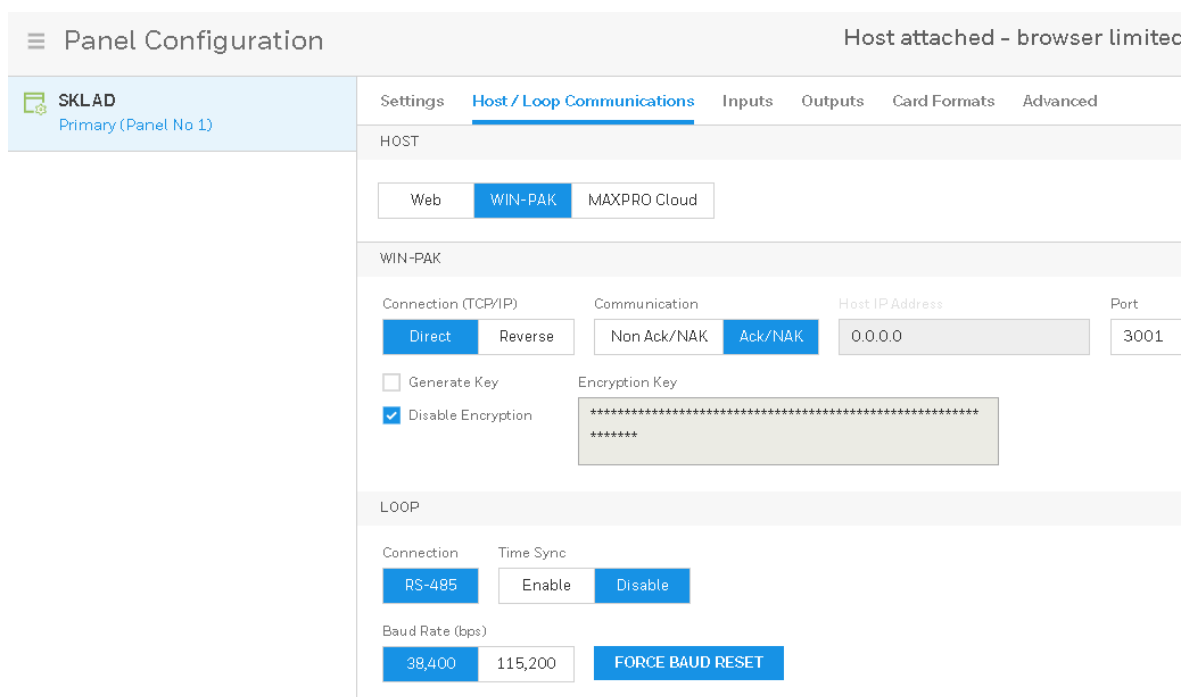
Od verze 6 je doporučeným webovým prohlížečem Google CHROME. Ten spustíme a do řádky napíšeme: **https://192.168.1.150** nebo IP adresu vlastní sítě LAN, ke které jsme panel Net-AXS připojili. Do přihlašovacího okna poprvé zadáváme jméno **admin** a heslo **admin**.

3. Nastavení panelu pro správu prostřednictvím WIN-PAKU

Dashboard: Menu > Panel Configuration > Host/Loop Communications

Zde provedeme nastavení dle obr. 50.

Jako první provedeme volbu WIN-PAK. Tuto změnu musíme uložit před zadáváním dalších parametrů připojení. Informační okno potvrdíme, panel se automaticky restartuje. Pro další nastavování musíme počkat až se zeleně rozsvítí komunikační LED označená jako RUN na obr. 18. Pokud by ani po rozsvícení LED nebylo možné pokračovat v nastavování panelu, je nutné okno prohlížeče zavřít a znovu se k panelu přihlásit.



Obr. 50 – Nastavení parametrů komunikace panelu a WIN-PAKU. [Zdroj: vlastní]

Po zadání všech parametrů pro komunikaci WIN-PAK s panelem NetAXS-123 můžeme nastavení uložit a prohlížeč zavřít.

4. Spuštění programu WIN-PAK

Před spuštěním programu WIN-PAK User Interface je vhodné zkontrolovat, zda je spuštěna služba WIN-PAK Database Server prostřednictvím programu WIN-PAK Service Manager

Po spuštění programu WIN-PAK se zobrazí přihlašovací okno. První přihlášení:

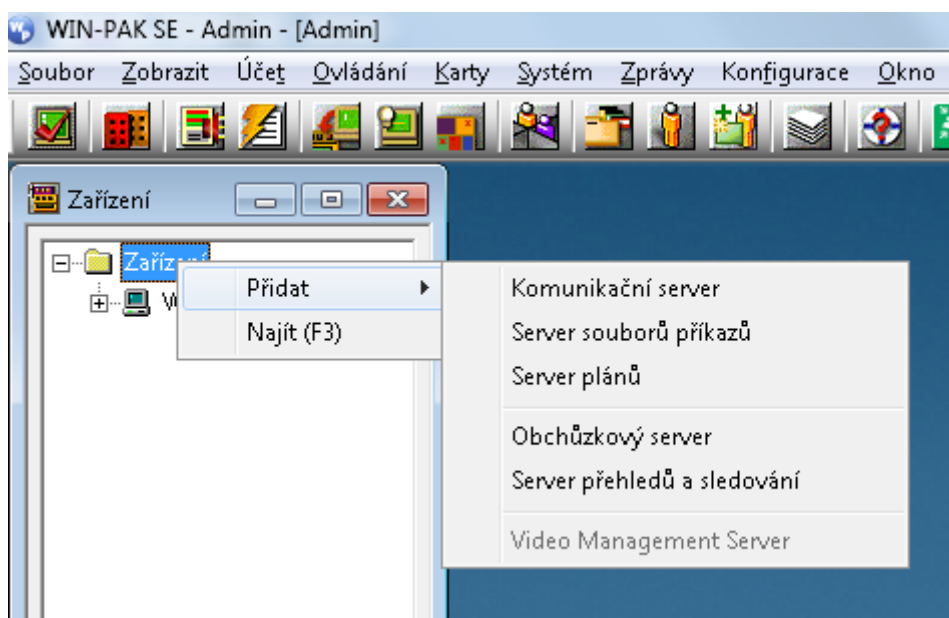
jméno: admin
heslo: <prázdné>

Následuje výzva k zadání silného hesla, tzn. alespoň 12 znaků v kombinaci malá a velká písmena, cifry a speciální znaky.

5. Konfigurace WIN-PAKu

Konfigurace > Zařízení > Mapa zařízení

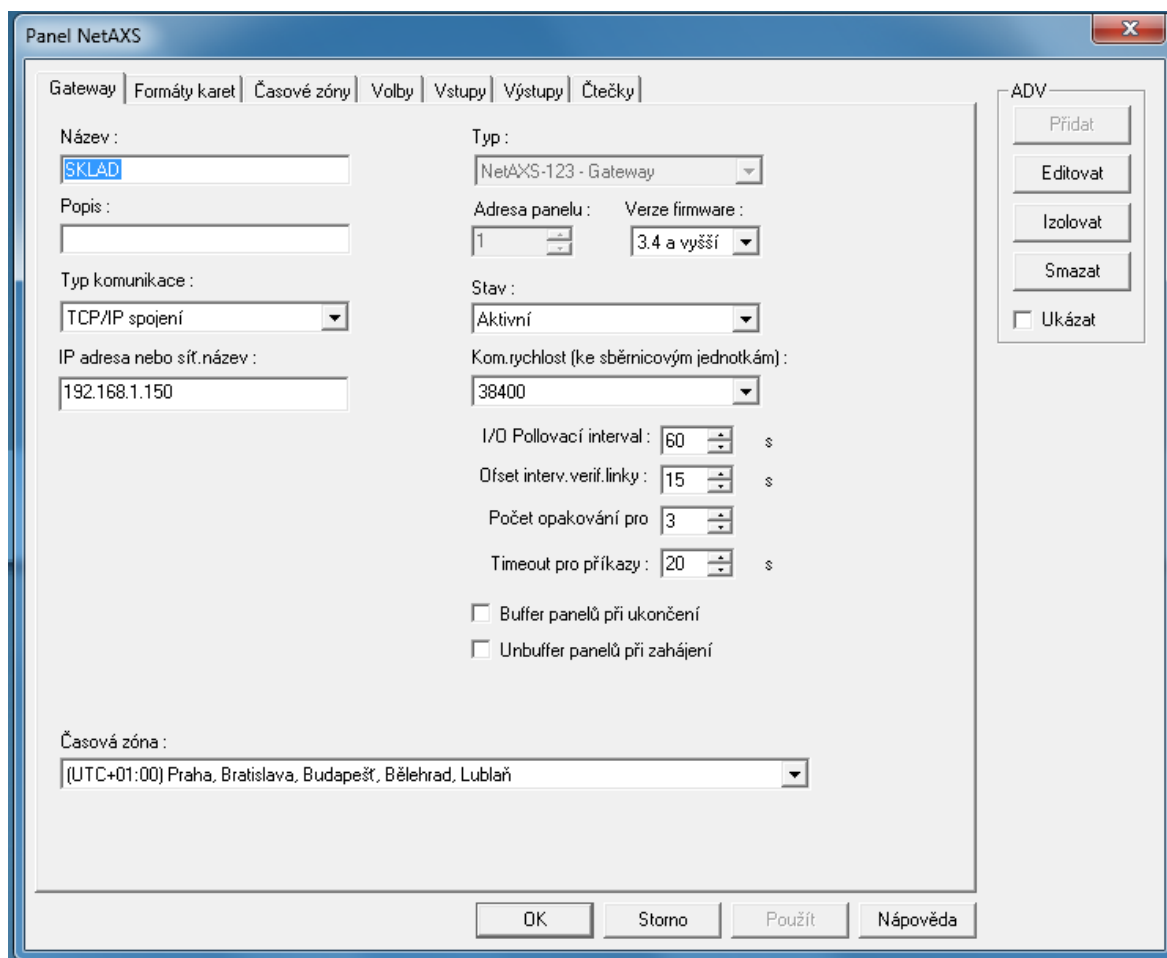
Ethernetové jednotky přidat pod komunikační server jako "NetAXS Gateway Panel - Přímé připojení" (obr.51).



Obr. 51 – Přidání jednotky ve WIN-PAKu. [Zdroj: vlastní]

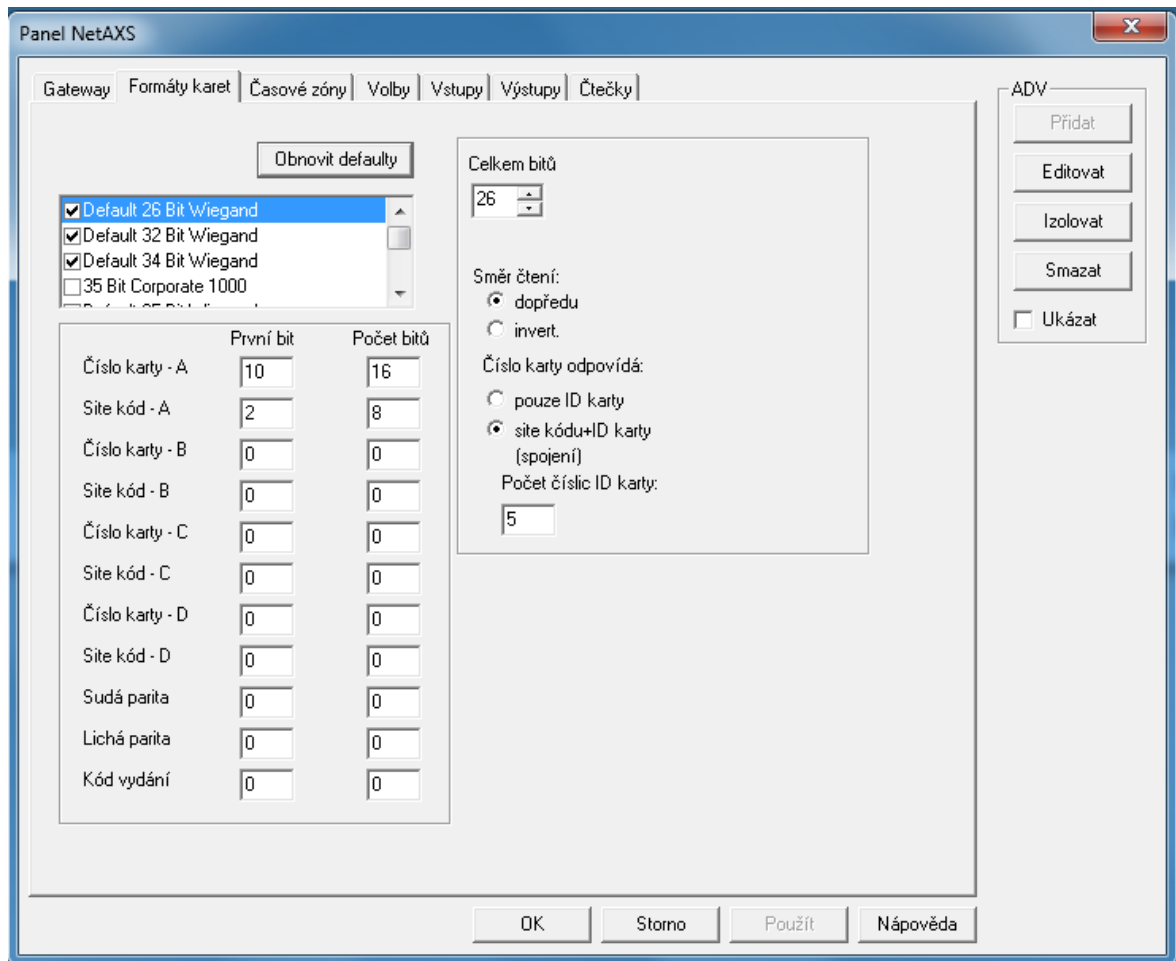
Před přidáním ADV vybrat jako "Typ" položku "NetAXS123 - Gateway" (defaultně je zadáno NetAXS4). Název jednotky by měl odpovídat umístění nebo označení v projektové

dokumentaci u rozsáhlých přístupových systémů. Zadáme typ komunikace, pro demonstrační panel TCP/IP spojení s IP adresou 192.168.1.150 (obr.52).



Obr. 52 – Nastavení parametrů jednotky ve WIN-PAKu. [Zdroj: vlastní]

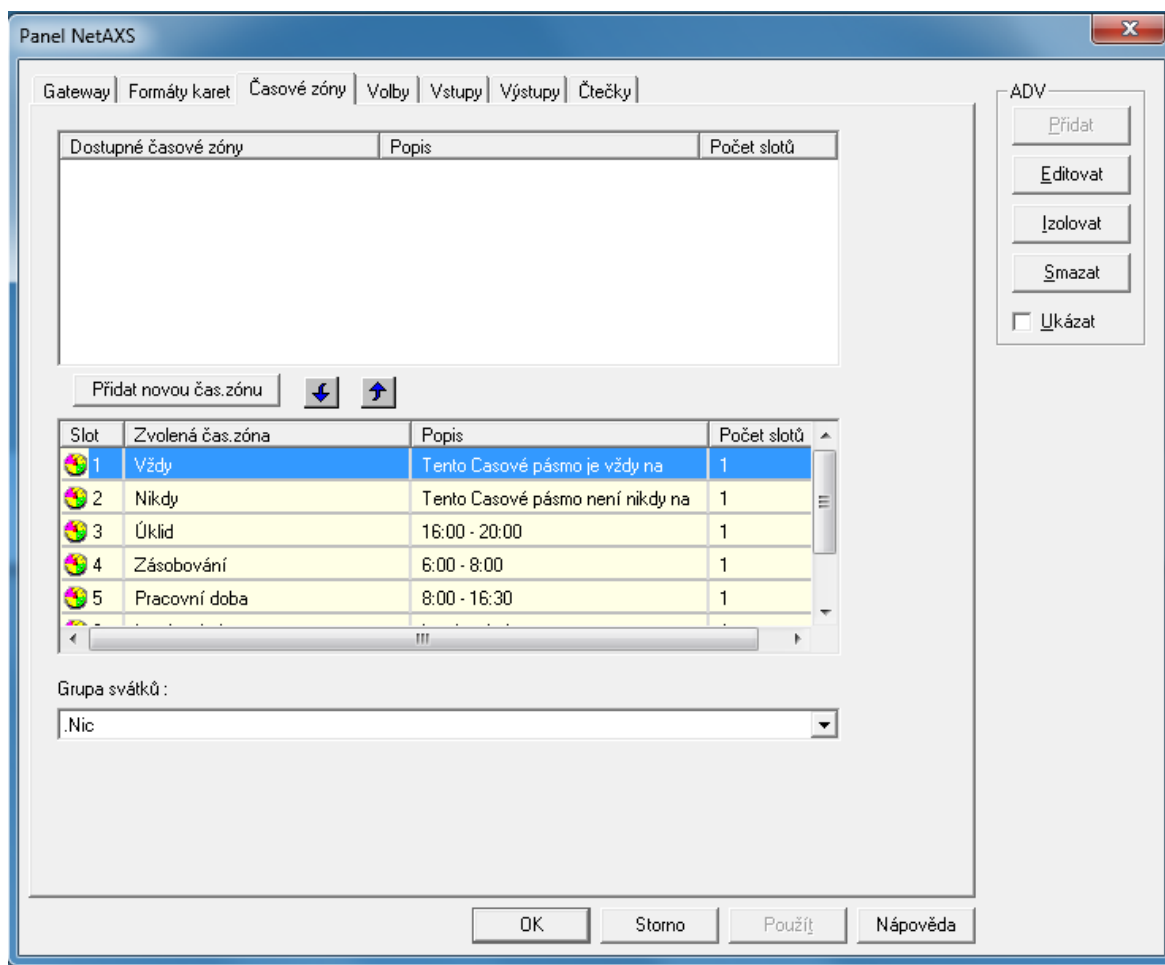
Nyní můžeme přidat pro panel ADV (**A**bstrak**D**e**V**ice – abstraktní zařízení). Volbou další přejdeme na záložku pro nastavení formátu karet. Na záložce Formát karet zaškrtneme pro formát Default 26 Bit Wiegand volbu "Číslo karty odpovídá: site kódu+ID karty (spojení)" a zadat jako "Počet číslic ID karty" = 5 (obr.53).



Obr. 53 – Nastavení formátu karet jednotky ve WIN-PAKu. [Zdroj: vlastní]

Volbou další přecházíme do nastavení časových zón. Pro demonstrační panel jsme zadali k systémovým časovým zónám navíc (obr.54):

Pracovní doba: 8:00 – 16:30 v pracovní dny.
 Zásobování: 6:00 – 8:00 v pracovní dny.
 Úklid: 16:00 – 20:00 v pracovní dny.



Obr. 54 – Nastavení časových zón ve WIN-PAKu. [Zdroj: vlastní]

Volbou další se přejde k záložce „Volby“, kde se nastavuje Anti-Passback, průběžné čtení karet, LED reverzního čtení a site kódy.

Volbou další se přejde k záložce „Vstupy“. Zde se přidává samostatné ADV ke každému zařízení, které bude sledováno v Mapě řízení. Týká se vstupů, výstupů a čteček. Je vhodné vstupům, které se nebudou v rámci dveřních obvodů využívat (např. vstup pro dveřní kontakt, když není instalovaný) nastavit logiku „NO bez EOL“, aby zbytečně nehlásily poplachy.

Volbou další se přejde k záložce, kde se ADV přiřazuje vstupům. Pro demonstrační panel nastavujeme:

- 1 – SKLAD – Odch.tl.dveří 1 Vst.1
- 2 – SKLAD – Stav.kont.dveří 1 Vst.2

Volbou další se přejde k záložce, kde se ADV přiřazuje výstupům. Pro demonstrační panel nastavujeme:

1 – SKLAD – Zámek dveří 1 Výst.1

3 – SKLAD – Pom. Výst.3

Volbou další se přejde k záložce, kde se ADV přiřazuje čtečkám. Pro demonstrační panel nastavujeme: 1a – SKLAD – Čtečka 1a

Volbou další se přejde na záložku Dokončení. Volbou dokončit se zobrazí dialogové okno, které vyzve administrátora k ruční inicializaci panelu z Mapy řízení.

Nyní přejdeme na **Konfigurace > Definice > Oblasti řízení**

Do oblasti řízení přidáme pravým tlačítkem myši místo a pojmenujeme. Pro demonstrační panel přidáváme „Místa“:

SERVER – z nabídky zařízení vybíráme **server**, položku WinPak.

FIRMA – z nabídky zařízení vybíráme **panel**, položku SKLAD.

Čtečka – z nabídky zařízení vybíráme **vchod**, položku SKLAD – 1a.

Vstupy – z nabídky zařízení vybíráme **vstup**, položky:

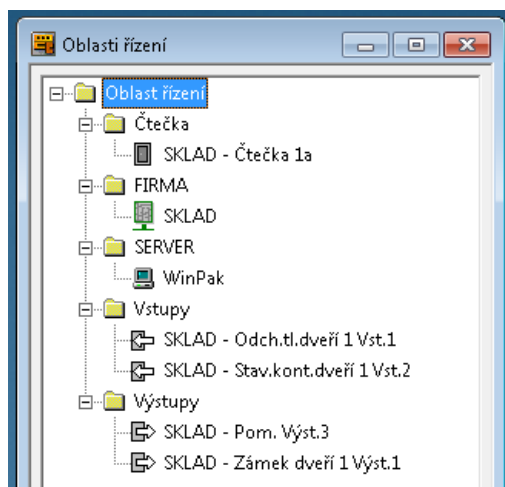
SKLAD – Odch.tl.dveří 1 Vst.1

SKLAD – Stav.kont.dveří 1 Vst.2

Výstupy – z nabídky zařízení vybíráme **výstup&grupa**, položky:

SKLAD – Zámek dveří 1 Výst.1

SKLAD – Pom. Výst.3



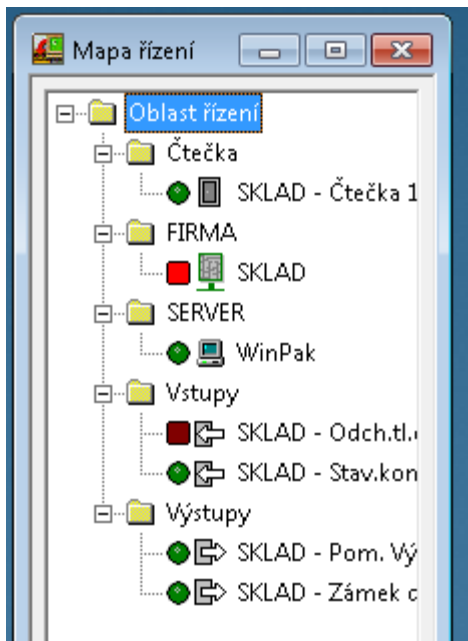
Obr. 55 – Nastavení prvků oblasti řízení ve WIN-PAKU. [Zdroj: vlastní]

Nyní přejdeme na **Konfigurace > Definice > Přístupové oblasti**

Zde do složky Přístupové oblasti pravým tlačítkem myši přidáváme dveře. Pro demonstrační panel přidáváme SKLAD – Čtečka 1a.

Nyní přejdeme na **Ovládání > Mapa řízení > Oblast řízení**

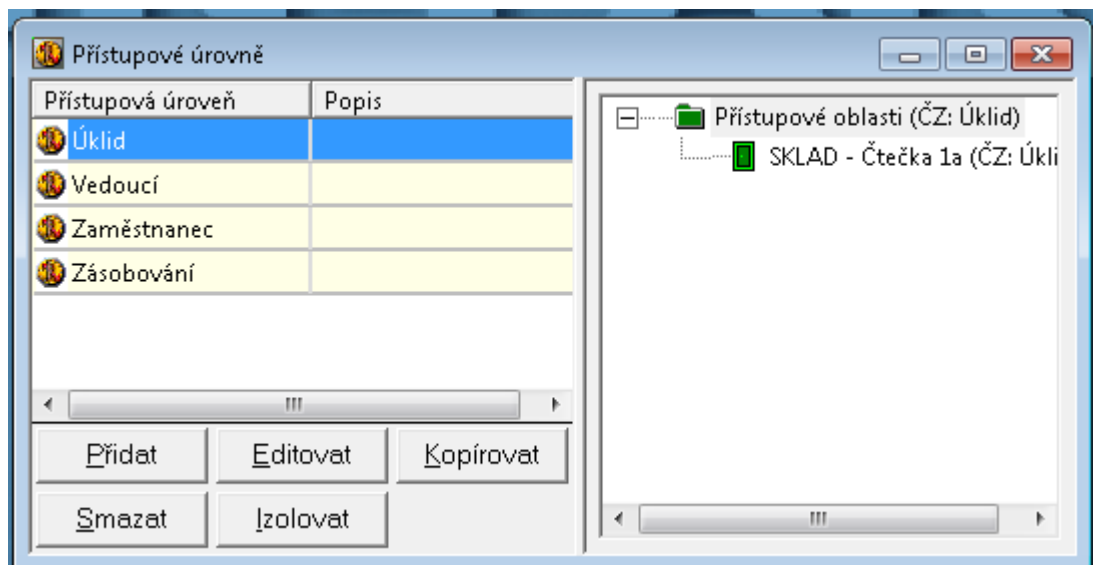
Dále se přidává každému zařízení, které bude sledováno v Mapě řízení, samostatné ADV (většinou stačí dvakrát kliknout na text "Žádné ADV" a zadat jedinečný název prvku. Týká se to vstupů, výstupů a čteček).



Obr. 56 – Mapa řízení pro demonstrační panel. [Zdroj: vlastní]

V prvním kroku provedeme inicializaci panelu. Pravým tlačítkem na ikonu panelu, vybrat vše dostupné a potvrdit spuštění inicializace. Nyní bude jednotka fungovat podle konfigurace a je možné nastavovat přes **Karty > Přístupové úrovně** přístupová práva do nových čteček. Pro demonstrační panel přidáváme přístupové úrovně:

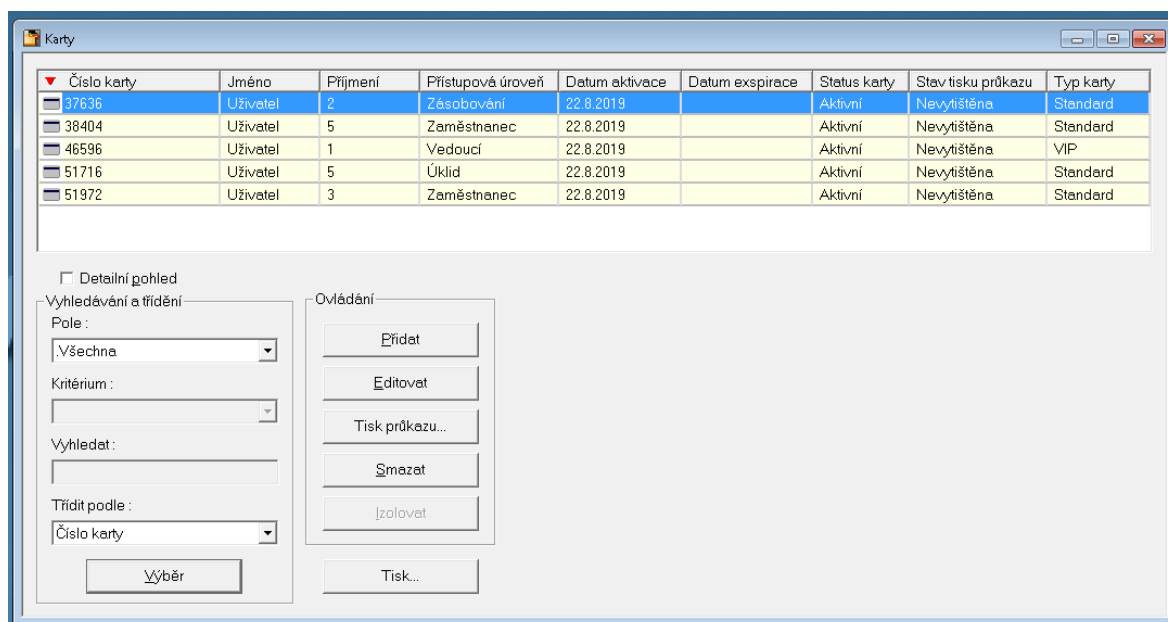
- Vedoucí.
- Zaměstnanec.
- Zásobování.
- Úklid.



Obr. 57 – Definice a přiřazení přístupových úrovní. [Zdroj: vlastní]

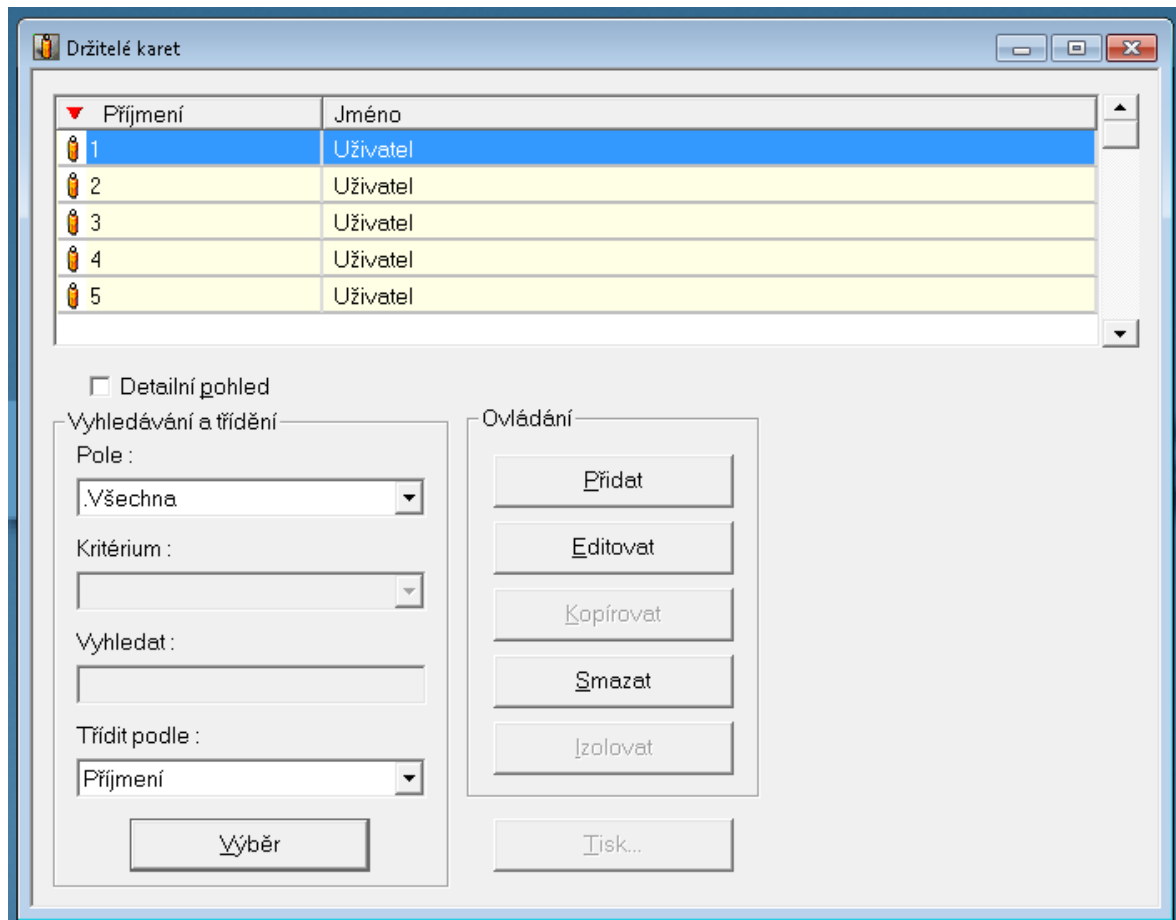
Konfiguraci čtečky provedeme stiskem pravého tlačítka myši na ikonu čtečky. Přidáme požadovanou přístupovou úroveň.

Nyní lze přistoupit k vytvoření seznamu karet. K prostředí pro vytvoření seznamu karet se dostaneme volbou: **Karty > Karty**. Karty lze zadávat hromadně, kdy se zadává počáteční číslo a počet karet (demo verze WIN-PAKu je v tomto ohledu omezená).



Obr. 58 – Vytvoření seznamu karet. [Zdroj: vlastní]

Po vytvoření seznamu karet je možné přes **Karty > Držitelé karet** vytvořit seznam uživatelů, kterým budou přidělovány karty.



Obr. 59 – Vytvoření seznamu uživatelů. [Zdroj: vlastní]

Po vytvoření obou seznamů, karty a uživatelé (např. zaměstnanci), může správce systému (nebo personalista) přiřazovat uživatele ke kartám a fyzicky karty vydávat, přičemž jednomu uživateli může být vydáno více karet.

Číslo karty	Jméno	Příjmení	Přístupová úroveň	Datum aktivace
37636	Uživatel	2	Zásobování	22.8.2019
38404	Uživatel	5	Zaměstnanec	22.8.2019
46596	Uživatel	1	Vedoucí	22.8.2019
51716	Uživatel	5	Úklid	22.8.2019
51972	Uživatel	3	Zaměstnanec	22.8.2019

Obr. 60 – Přiřazení karet uživatelům. [Zdroj: vlastní]

Uvedení panelu do továrního nastavení

V praxi se občas vyskytne situace, kdy je lepší začít úplně znovu od začátku, než se pokoušet něco opravit. Sekvence pro uvedení panelu NetAXS-123 do továrního nastavení je:

1. V zapnutém stavu přepněte všechny DIP přepínače SW1 do polohy vypnuto (OFF).
2. Odpojte napájení a následně napájení k panelu připojte.
3. Vyčkejte na spuštění panelu. Kontrolka RUN bude rychle blikat.
4. Nastavte DIP přepínače SW1 do původní polohy.
5. Odpojte napájení a následně napájení k panelu připojte.
6. Po spuštění panelu bude kontrolka RUN blikat normální (pomalejší) rychlostí.

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.

Srovnání SW parametrů řídicích jednotek

Parametr	A22	NetAXS-123
Česká lokalizace	ANO	ANO
OFF line provoz	ANO	ANO
ON line provoz	ANO	ANO
Správa přes WEB	ANO	ANO
Hybridní SW+WEB	ANO	ANO
Dostupné integrační (API) rozhraní	NE	ANO
MS SQL Server	ANO	ANO
Architektura klient – server	NE	ANO
SW pro správu jednotek	ATRIUM SW	WIN-PAK
Anti-Passback	ANO	ANO
Režim PIN+Karta	ANO	ANO
Režim PIN nebo karta	ANO	ANO
Podpora uživ.inerlocků v HW j.	ANO	ANO
Podpora tiggerů a procedur v HW	ANO	NE
SW integrace CCTV	NE	ANO
HW podpora CCTV	ANO	NE

Srovnání HW parametrů řídicích jednotek

Parametr	A22	NetAXS-123
Paměť událostí pro off-line režim	25.000	25.000
Paměť karet (příp. na 1 podsystém)	10.000	10.000
Omezení počtu karet v SW	10.000	NE
Max. počet čteček na kontrolér	10	1, resp. 2
Max. počet dveří na kontrolér	10	1(2)
Rozšiřující I/O moduly	ANO	NE
Rozšiřující čtečkové moduly	NE	ANO
Max. počet kontrolérů na sběrnici	5	31
Max. počet kontrolérů v systému	50	NE
RS-232	NE	NE
RS-485	ANO	ANO
TCP/IP	ANO	ANO
USB	NE	ANO
Časové zóny/svátky	250/ANO	63/ANO
Automatická změna letního/zimního času	ANO	ANO
Wiegand 26b	ANO	ANO
Wiegand 27b	ANO	ANO
Wiegand 32b	ANO	ANO
Wiegand 37b	ANO	ANO
Wiegand 40b	ANO	ANO
Wiegand – multiformat	ANO	ANO
Rozhraní OSDP (RS485) pro čtečky	ANO	NE
Podpora rozhraní ABA (Clock&Data)	ANO	NE
Připojení odchod.tlačítek	ANO	ANO

Signalizace stavu dveří	ANO	ANO
Konfigurovatelné vst./výst.	ANO	ANO
Interní zdroj	ANO	NE
Interní AKU	ANO	ANO
Napájení 12 Vss	NE	ANO
Napájení 24 Vss	ANO	NE
PoE	NE	ANO
Rozměr PCB (V x Š x H) [mm]	199x180x40	138x150x18 (54)
Rozměr krytu (V x Š x H) [mm]	400x320x90	197x197x70
Teplotní rozsah (bez AKU)	-20 až 70°C	0 až 49°C

Z uvedeného srovnání SW a HW jsou patrné jen minimální odlišnosti. Oba systémy bude možné nasadit do většiny reálných aplikací. V případě požadavku na zvýšenou bezpečnost a celkovou robustnost systému lépe vyhovuje přístupový systém NetAXS-123.

Přístupové systémy vybudované s jednotkami A22 mají uplatnění především v objektech, kde je požadována velká flexibilita při vydávání RFID karet. Umožnění nastavení přístupu a vydání karty za použití tabletu připojeného k Wi-Fi je velmi komfortní a vyhledávané především správci bytových areálů, kde počet vstupů se pohybuje nad 20 a počet uživatelů přes 1.000.

Oproti tomu panel NetAXS-123 má nezastupitelné místo především v bezpečnostních aplikacích. Jeho architektura a programové vybavení WIN-PAK splňují všechny bezpečnostní požadavky, které jsou dnes na přístupové systémy kladeny, především v souvislosti se zapojením jednotlivých panelů do sítě LAN, která nemusí být vždy určena primárně pro přístupový systém.

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.
Wi-Fi	Způsob bezdrátové komunikace mezi technologickými zařízeními

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 – Architektura přístupového systému, kombinace IP a RS485.[5].....	20
Obr. 9 – Architektura přístupového systému, sběrnice RS485.[5]	21
Obr. 10 – Řídicí jednotka přístupového systému NetAXS–123 v plastové skříni.[5]22	
Obr. 11 – Přídavné karty pro 1 a 2 dveře pro NetAXS-123.[5].....	23
Obr. 12 - Schéma připojení uživatelských a systémových rozhraní.[6]	24
Obr. 13 – Nastavení přepínačů pro konfiguraci relé.....	27
Obr. 14 – Elektromagnetický zámek DORCAS.[Zdroj: vlastní].....	32
Obr. 15 – Elektromechanický zámek EL460 (vlevo) a přídržný magnet V3SR (vpravo).[Zdroj: vlastní].....	33
Obr. 16 – Převodník RS-485 na Ethernet VESP211-485.[Zdroj: vlastní].....	34
Obr. 17 – Demonstrační panel s řadičem NetAXS-123 typ NX1P.[Zdroj: vlastní] ...	37
Obr. 18 – Zapojení demonstračního panel s řadičem NetAXS-123 typ NX1P.[6]	38
Obr. 19 – Přímé propojení počítače a panelu NetAXS-123.[7].....	39
Obr. 20 – Propojení počítače a panelu NetAXS-123 přes LAN přepínač.[7]	39
Obr. 21 – Přihlašovací okno pro konfiguraci web serveru.[7].....	40
Obr. 22 – Dashboard – základní obrazovka pro konfiguraci webserveru.[Zdroj: vlastní]	41
Obr. 23 – Správa účtu, změna jazyka přes webový prohlížeč.[Zdroj: vlastní].....	41
Obr. 24 – Nastavení hostitele Web a volba EVL. [Zdroj: vlastní]	43
Obr. 25 – Nastavení nadřazeného panelu NetAXS-123. [Zdroj: vlastní].....	43
Obr. 26 – Registrace Podřadného panelu NetAXS-123. [7].....	44
Obr. 27 – Odhlášení Podřadného panelu NetAXS-123. [7]	44
Obr. 28 – Konfigurace komunikace RS485 panelu NetAXS-123. [Zdroj: vlastní]....	45
Obr. 29 – Nastavení parametrů komunikace pro režim hostitele. [Zdroj: vlastní]	47

Obr. 30 – Nastavení parametrů komunikace pro režim Web. [7].....	49
Obr. 31 – Přístup k nastavení panelu. [Zdroj: vlastní].....	50
Obr. 32 – Konfigurační obrazovka nastavení panelu. [Zdroj: vlastní].....	51
Obr. 33 – Konfigurační obrazovka nastavení chování panelu. [7].....	51
Obr. 34 – Konfigurace řídicí jednotky, nastavení časových zón. [Zdroj: vlastní].....	53
Obr. 35 – Přístup ke konfigurační obrazovce nastavení oblastí. [Zdroj: vlastní].....	54
Obr. 36 – Přiřazení dveří do oblastí. [7].....	54
Obr. 37 – Konfigurace nastavení dveří. [Zdroj: vlastní].....	55
Obr. 38 – Záložka „Vstupy“ konfigurace dveří. [Zdroj: vlastní].....	56
Obr. 39 – Záložka „Výstupy“ konfigurace dveří. [Zdroj: vlastní].....	57
Obr. 40 – Přejít na konfiguraci „Samostatného výstupu“. [Zdroj: vlastní].....	57
Obr. 41 – Konfigurační okno nastavení „Skupiny výstupů“. [7].....	58
Obr. 42 – Konfigurační okno nastavení „Formátů karet“. [7].....	59
Obr. 43 – Konfigurační okno nastavení „Záznamu osob“. [7].....	60
Obr. 44 – Konfigurační okno nastavení „Karet“. [7].....	61
Obr. 45 – Konfigurační okno nastavení „Přístupové skupiny“. [7].....	62
Obr. 46 – Vytvoření nové přístupové skupiny. [7].....	62
Obr. 47 – Okno pro sledování poplachů a událostí. [7].....	63
Obr. 48 – Verze a návaznosti WIN-PAK.[6].....	65
Obr. 49 – Ikona pro vstup do MENU webového konfiguračního prostředí panelu NetAXS-123 [Zdroj: vlastní].....	66
Obr. 50 – Nastavení parametrů komunikace panelu a WIN-PAKu. [Zdroj: vlastní].....	67
Obr. 51 – Přidání jednotky ve WIN-PAKu. [Zdroj: vlastní].....	68
Obr. 52 – Nastavení parametrů jednotky ve WIN-PAKu. [Zdroj: vlastní].....	69
Obr. 53 – Nastavení formátu karet jednotky ve WIN-PAKu. [Zdroj: vlastní].....	70
Obr. 54 – Nastavení časových zón ve WIN-PAKu. [Zdroj: vlastní].....	71
Obr. 55 – Nastavení prvků oblasti řízení ve WIN-PAKu. [Zdroj: vlastní].....	72
Obr. 56 – Mapa řízení pro demonstrační panel. [Zdroj: vlastní].....	73
Obr. 57 – Definice a přiřazení přístupových úrovní. [Zdroj: vlastní].....	74
Obr. 58 – Vytvoření seznamu karet. [Zdroj: vlastní].....	74
Obr. 59 – Vytvoření seznamu uživatelů. [Zdroj: vlastní].....	75
Obr. 60 – Přiřazení karet uživatelům. [Zdroj: vlastní].....	75

SEZNAM TABULEK

Tab. 1 – Stupně klasifikace [2]	12
Tab. 2 – Základní parametry bezkontaktní čtečky iCLASS SE R10 [4]	16
Tab. 3 – Barevné označení a význam vodičů bezkontaktní čtečky iCLASS SE R10 18	
Tab. 4 - Technické parametry řídicí jednotky NetAXS-123.[5].....	30
Tab. 5 – Nastavení DIP přepínače u nadřazeného panelu NetAXS-123.[7].....	42
Tab. 6 – Nastavení DIP přepínače u podřazeného panelu NetAXS-123.[7]	42