Požadavky na přístupový a zabezpečovací systém na Masarykově univerzitě

Verze 2.0
Ústav výpočetní techniky Masarykovy univerzity

Abstrakt

Tento dokument popisuje vlastnosti, které jsou závazně požadovány od přístupového (elektronická kontrola vstupu, dále EKV) a zabezpečovacího (elektronický zabezpečovací systém, EZS) systému, aby mohl být nainstalován a používán v budovách Masarykovy univerzity. Tento dokument je závazný také v případě rozšíření již instalovaného systému. V první části jsou popsány obecné požadavky na systémy a jejich integraci. Druhá část popisuje požadovanou funkcionalitu systémů pro jednotlivé typy budov a místností.

Cílem tohoto dokumentu je vymezení obecných zásad, jejichž dodržení při plánování uvedených systémů povede ke stavu, kdy jsou tyto systémy

- snadno udržovatelné a sledovatelné velkým počtem zodpovědných osob na různých úrovních
- škálovatelné a nákladově efektivní
- bezpečné vzhledem k ochraně majetku i osob užívajících příslušnou budovu
- dobře přizpůsobené potřebám výuky, výzkumu i provozu

Verze	Datum	Autoři/Revize	Pracoviště	Kontakt
1.0	30. 11. 2011	Martin Osovský Lukáš Rychnovský	Ústav výpočetní techniky Ústav výpočetní techniky	
2.0	20. 5. 2013	Adriana Strejčková Aleš Křenek	Ústav výpočetní techniky Ústav výpočetní techniky	strejckova@ics.muni.cz ljocha@ics.muni.cz

Obsah

1 Pojmy

Přístupový bod - zařízení nebo skupina zařízení, které řídí přístup do místnosti či budovy, uživateli se jeví jako čtečka, která načte jeho kartu (případně biometrická čtečka) a zařízení, které po načtení karty otevře dveře (resp. uvolní zámek), případně odstřeží místnost či skupinu místností

Stav přístupového bodu - režim řízení přístupu (otevřeno, vstup jen na kartu, zavřeno a podobně)

Konfigurace přístupů - nastavení, jak mají jednotlivé přístupové body reagovat na karty (např. které karty mohou otevírat které dveře)

Provozní konfigurace - konfigurace celkové struktury systému, tj. napojení přístupových bodů (čteček) na dveře místností, které se danou čtečkou zastřežují apod., obecně veškerá konfigurace, která nespadá pod konfiguraci přístupů

2 Požadavky

2.1 Autonomnost a rychlost odezvy

Celý systém je autonomní a obsahuje celou svoji konfiguraci (provozní i přístupovou), tedy přístupové body jsou plně funkční i při výpadku spojení s veškerými externími systémy (zejména databáze karet, osob a přístupů), současně v této situaci nedojde ke ztrátě sbíraných informací o průchodech. Přístupové body reagují na přiložení karty do 1 sekundy, v odůvodněných zvláštních případech nejvýše do 2 sekund.

2.2 Integrace EZS a EKV

Systémy EZS a EKV musí být plně integrovány. Zejména

- přístupové body umožňují ovládání EZS (zastřežení/odstřežení prostor kartou), čtečky jsou pro to uzpůsobeny, mají širší možnosti signalizace stavů (např. několik světelných či zvukových signálů pro různé odpovědi), tlačítko pro ovládání EZS, případně ovládací klávesnici
- chování přístupových bodů je určeno momentálním stavem EZS (do zastřežené místnosti není možno vstoupit)
- hlášení požáru umožní nastavení přístupů podle potřeby požárního zásahu (únik ap.), zejména systém EPS (elektronická požární signalizace) je systémům EKV a EZS nadřazen v souladu s předpisy bezpečnosti a požární ochrany
- je zakázáno instalovat jakákoliv zařízení, která blokují odchod z místnosti nebo průchod na únikové cestě čí únikovým východem

2.3 Konfigurace přístupů

Systém umožňuje

- přiřadit libovolné kartě zavedené v Informačním systému MU (IS MU) přístup případně jiné operace (zastřežení, odstřežení, deaktivace alarmu) na libovolné kombinaci přístupových bodů
- provádět tyto operace hromadně (mj. u všech osob evidovaných v IS MU v jedné dávce, tj. desetitisíce osob) a kdykoliv to bude vhodné

Technicky je konfigurace přístupu rozdělena na statickou a dynamickou část.
Statickou částí se rozumí jednoznačné přiřazení každého přístupového bodu ke konkrétní skupině osob (karet) evidované v IS MU. Pro různá práva (např. pouze vstup vs. vstup a odstřežení) mohou být

použity různé skupiny. Toto nastavení je typicky provedeno pouze jednou při předání systému k užívání, ke změnám dochází pouze výjimečně.
Dynamickou částí konfigurace se rozumí přiřazení práv (vstup, odstřežení atd.) konkrétním osobám (kartám), to je realizováno výhradně členstvím ve výše uvedených skupinách. Systém EKV musí zajistit načítání těchto dat specifikovaným komunikačním protokolem v dohodnutých intervalech (typicky jednou za 10 minut). Načítání konfigurace přístupu nemá vliv na chování přístupových bodů vůči uživateli (zejména ne zpomalení nebo dokonce výpadek či přepnutí do stavu, kdy dočasně systém nelze používat), kromě případného umožnění či odepření přístupu podle nově nahrávané konfigurace přístupů.
Systém musí být škálovatelný v úrovních cca. 100, 1 000, 50 000 karet podle potřeby užívání daných prostor a rozšiřitelný na kapacitu až 100 000 karet.
Vzhledem k velkému počtu uživatelů (karet) a různým kombinacím ve skupinách, které jsou k provozu systému na MU potřebné, není vhodné omezovat, kolik různých práv je přiřazeno jedné kartě a naopak, kolik karet ovládá jeden přístupový bod.

2.4 Provozní konfigurace

Počáteční provozní konfiguraci na straně EKV a EZS provede dodavatel podle specifikace stavby (kódy místností a identifikace zařízení, mapování přístupových skupin na přístupové body a podobně). Případné pozdější změny v provozní konfiguraci může provádět provozovatel. K tomuto účelu musí být dodána obslužná aplikace a tyto postupy musí být řádně zdokumentovány.

2.5 Sledování stavů a událostí

Systém dále umožňuje vzdáleně

- sledovat v reálném čase události na přístupových bodech (příchod, odchod, nepovolení přístupu, chybové stavy)
    - na událost je možné v reálném čase reagovat (zobrazení, umožnění přístupu k jiným zdrojům, např. povolení přihlášení na počítače v dané místnosti, otevření katedry ap.)
    - přístupové body musí být možné sledovat pomocí aplikací v IS MU a aplikací IRIS (ÚVT); informace o událostech jsou do těchto systémů importovány společným definovaným protokolem.
- sledovat a měnit aktuální stavy přístupových bodů
    - provozní (zamknuto, zavřeno, otevřeno atd.) i výjimečné (nefunkční, vypnuté ap.)
    - přepínat zejména mezi stavy volný přístup, otevřeno, odstřeženo a zastřeženo (tyto změny je možné provádět ručně nebo na základě nastavení časových rozvrhů, tj. přepnutí v daný den a hodinu)
    - sledování i změny se realizují výhradně komunikací vyhovující standardu BACNet pomocí k tomu definovaných objektů

2.6 Integrace do systémů MU

- IS MU — definuje konfigurace přístupů a sbírá informace o průchodech
- aplikace ÚVT (Iris) — umožňují sledování událostí a vzdálené odstřežování/zastřežování
- BMS systémy — systém musí být integrovatelný s dalšími BMS systémy pomocí protokolu BACnet, tj. existuje hardwarová BACnet brána pro EZS, EKV i EPS
- čipové karty — čtečky u přístupových bodů musí bezdotykově číst čipy karet EM 125 kHz (současné ISIC a zaměstnanecké karty) a MIFARE DESFire

2.7 Diagnostika problematického chování

Systémy EKV a EZS dovolují prostřednictvím své obslužné aplikace, nezávislé na integraci se systémy MU, základní diagnostiku chování. Detailní požadavky na tuto funkcionalitu jsou uvedeny v příloze.

3 Obecné principy fungování vazby EZS a EKV

Operace s kartami mají dvě úrovně

- neprivilegovaná (bez ovládání EZS) - umožňuje přístup a odchod do resp. z odstřežených prostor, kam má daná osoba přístup
- privilegovaná (umožňuje ovládání EZS) - umožňuje odstřežení a zastřežení prostor, zrušení hlášeného alarmu

Typy dveří

- turniket - umožní přístup i odchod jen jednotlivým osobám, které jsou oprávněny vstoupit, není vhodný pro prostory se zastřežováním
- posuvné dveře - omezují možnost vstupu a odchodu více osob na jednu kartu, lze je použít v zastřežovaných prostorách
- dveře s klikou zevnitř - místnost je možno libovolně opouštět (i bez karty), dovnitř je možno vstupovat jen pomocí karty nebo když jsou dveře odemčeny, není možné účinně regulovat počet osob vstupujících dovnitř na jedno přiložení karty
- dveře bez kliky - k odchodu i příchodu je nutné přiložit kartu, ale přesto není možné účinně regulovat počet osob vstupujících dovnitř na jedno přiložení karty (způsobuje problémy pro požární ochranu)
- závora, brána pro vjezd - umožní příjezd a odjezd jen jednotlivým dopravním prostředkům

Režimy dveří jsou dány kombinací tří dílčích stavů

- jsou-li dveře mechanicky zamčeny, tj. je-li trvale vysunuta západka zámku (zamčené/odemčené)
- je-li možné otevřít stisknutím kliky nebo zatažením za úchytku bez použití karty (zavřené/s klikou)
- je-li v místnosti za dveřmi zastřeženo nebo odstřeženo

Možné režimy dveří

- „otevřeno, volný přístup“ - dveře odemčené s klikou, odstřeženo
- „zamčeno“ - dveře zamčené
- „zavřeno, odstřeženo“ - dveře odemčené, zavřené, odstřeženo; ke vstupu je nutno použít oprávněnou kartu
- „zavřeno, zastřeženo“ - dveře odemčené, zavřené, zastřeženo; ke vstupu je nutno použít oprávněnou kartu s ovládáním EZS

Způsob ovládání EZS

- tlačítko integrované ve čtečce
  - odstřežení se provede přiložením karty s ovládáním EZS ke čtečce přístupového bodu ve stavu „zavřeno, zastřeženo“
  - zastřežení přiložením karty a zároveň stisknutím tlačítka
- nezávislá ovládací klávesnice

4 Popis jednotlivých typů prostor na MU

4.1 Přednášková místnost

Slouží pro většinu velkých přednáškových místností MU, kde kvůli kapacitním možnostem není možné vpouštět studenty jednotlivě. Zodpovědná osoba (vyučující učitel nebo správce) místnost odstřeží, čímž dveře převede ze stavu „zavřeno, zastřeženo“ do stavu „otevřeno, volný přístup“ a studenti dále vstupují do místnosti bez použití karty. Po ukončení výuky zodpovědná osoba zastřeží, čímž dveře převede do stavu „zavřeno, zastřeženo“. Systém musí umožnit zamykání a odemykání místností dle časových rozvrhů, stejně tak odstřežování a zastřežování.

4.2 Seminární místnost

Slouží pro menší přednáškové místnosti a seminární místnosti MU a místnosti, kde je třeba monitorovat či omezovat vstup studentů. Zodpovědná osoba místnost odstřeží, čímž dveře převede ze stavu „zavřeno, zastřeženo“ do stavu „zavřeno, odstřeženo“ a studenti dále po přiložení karty vstupují do místnosti. Po ukončení výuky zodpovědná osoba opět zastřeží, čímž dveře převede do stavu „zavřeno, zastřeženo“. Nelze úplně zajistit, aby osoby po identifikaci vstupovaly jednotlivě a ne hromadně. Systém musí umožnit zamykání a odemykání místností dle časových rozvrhů, stejně tak odstřežování a zastřežování.

4.3 Místnost s více dveřmi

Pokud má některá z výše uvedených místností více dveří, jsou jedny z nich označeny jako hlavní. Chování hlavních dveří je popsáno výše v odstavcích Přednášková místnost a Seminární místnost (u ostatních typů místností, s výjimkou Chodby popsané níže, není použití přístupového systému na více dveřích vhodné). Ostatní dveře mají chování závislé na stavu hlavních dveří; pokud jsou hlavní dveře ve stavu "otevřeno, volný přístup" nebo "zavřeno, odstřeženo", jsou ve stejném stavu i ostatní dveře. Pokud jsou hlavní dveře ve stavu "zamčeno" nebo "zavřeno, zastřeženo", jsou ostatní dveře ve stavu "zamčeno", zejména nevpouštějí žádné karty.

4.4 Katedry v přednáškových místnostech

Katedry v přednáškových a seminárních místnostech jsou kromě dataprojektoru často jediným cenným majetkem fakulty v místnosti. Zamykatelná katedra se prvním přiložením oprávněné karty odemkne a otevře, druhým přiložením pak zavře a uzamkne. Katedra může být opatřena čidlem násilného vniknutí, které je připojeno na systém EZS.

4.5 Počítačová učebna

V počítačových učebnách a studovnách je největší koncentrace majetku a také nejsnadnější možnost krádeže ze všech standardně dostupných prostor. Důležité je, aby každý před vstupem do místnosti musel použít svoji kartu. Toho lze dosáhnout buď použitím turniketu (drahé řešení) a/nebo vazbou na přihlašování k počítačům v dané místnosti (kdo kartu nepřiložil, ten se nepřihlásí). Tím se omezí nežádoucí chování, kdy více osob vstupuje na jednu kartu, případně používá společné jméno a heslo k počítači. U těchto prostor je vhodné řídit kromě vstupu také výstup (odchod z místnosti).

4.6 Chodba resp. hlavní vchod

Čtečka hlavního vchodu, resp. vstupu do chodby může řídit EZS společných prostor, resp. celé budovy. K tomu se používají tzv. závislé zóny. To znamená, že zastřežit hlavní vchod je možné jedině když jsou zastřeženy všechny ostatní zóny v příslušné budově či části budovy. Za tím účelem musí být u hlavního vchodu signalizace zastřežení ostatních prostor.

4.7 Garáž

Garáž je obvykle uzavřena závorou nebo bránou. Ta se otvírá přiložením karty, prozvoněním z vybraných telefonních čísel nebo rozpoznáním, že SPZ vozidla se nachází v příslušném seznamu. Zavírá se samostatnými technickými prostředky, např. detekcí průjezdu fotobuňkou. Vjezd může být dále omezen kapacitou parkoviště. Bránu je též možno otevřít vzdáleně z vrátnice. Za tím účelem je nutné sledování kamerou nebo alespoň přítomnost komunikačního zařízení (interkom).

4.8 Serverovna, technická místnost, pokladna a podobně

Velmi restriktivní přístup do místnosti, kde se nachází majetek velké hodnoty. Dveře jsou stále ve stavu „zavřeno, zastřeženo“, do místnosti mohou vstupovat jen osoby s kartou, která ovládá EZS, kartu přikládají na vstupu, při odchodu vždy uvedou zpět do stavu „zavřeno, zastřeženo“. Dveře se nikdy nemohou dostat do stavu „otevřeno, volný přístup“. Přístup do místnosti je také možno doplnit biometrickými čtečkami, například čtečkami otisků prstů.

4.9 Laboratoř

Také v laboratořích se nachází majetek velké hodnoty. V těchto místnostech bývá větší pohyb než v prostorech typu technická místnost, proto se nepředpokládá jejich trvalé zastřežení, nicméně dveře by se neměly dostávat do stavu „otevřeno, volný přístup“.
Do laboratoří má obvykle přístup užší skupina lidí než do počítačových učeben, avšak i zde může být vhodné kontrolovat výstup (odchod z místnosti).

4.10 Další typy místností

Výše uvedený výčet typů prostor je pouze orientační a pokrývá typické případy. Specifické požadavky konkrétní lokality si mohou vynutit odlišný režim přístupu, jeho popis je vždy součástí konkrétního zadání.

Příloha A: Podrobné požadavky na funkcionalitu

Operace obslužné aplikace dodavatele

Subjekty a karty

- přidání/odebrání karty subjektu
- úprava oprávnění spojených s kartou
- zjištění úplného nastavení subjektu, jeho karet a oprávnění podle skutečného stavu v systému (ústředně)
- zapnutí/vypnutí dávkového plnění
- konfigurace a diagnostika dávkového plnění

Přístupové body

- zjištění stavu (otevřeno, zavřeno, zamčeno, nefunkční)
- přepnutí z jednoho stavu do jiného
- nastavování časových rozvrhů

Zabezpečení

- zjištění stavu zabezpečení v zabezpečeném prostoru (zastřeženo, odstřeženo)
- přepnutí stavu zabezpečení (zastřežení, odstřežení)
- hlášení všech druhů alarmů
- zrušení alarmu

Provozní konfigurace

- přidání/odebrání/změna identifikace přístupových bodů

Příloha B: Podrobné požadavky na integraci do systémů MU

1. Informační systém (IS MU)
    a. pravidelná dávková konfigurace přístupů v EKV podle nastavení v IS MU
    b. informace o průchodech z EKV do IS MU
2. Building Management System (BMS)
   Součástí dodávky je vytvoření a ověření funkcionality BACnet objektů, které umožní
    a. sledovat stavy jednotlivých detektorů, snímačů, zámků a nouzových tlačítek
    b. ovládání zámků či pohonů dveří pomocí kalendářů a plánovačů
    c. zastřežení a odstřežení jednotlivých zón
    d. detekci poplachových stavů
    e. sledování napájení (výpadky sítě, provoz na baterii)
    f. sledování stavu brány (GW)

   Požadavky související s integrací do BMS systémů jsou podrobněji specifikovány v dokumentu „Metodika nasazování a úprav komponent BMS MU“
3. Aplikace ÚVT (Iris)
    a. sledování událostí na přístupových bodech v reálném čase (kompatibilní protokol s 1.b)
    b. sledování stavů jednotlivých zón a jejich zastřežení a odstřežení (BACnet 2.c)

Příloha C: Požadavky na harmonogram dodání systému

- Na začátku realizace stavby je třeba dodat zkušební sadu, která obsahuje všechny prvky, které budou v systému použity a veškerou technickou dokumentaci k systému.
- Instalaci a konfiguraci systému je potřeba dokončit alespoň 2 měsíce před odevzdáním stavby k užívání a předat ÚVT informace potřebné k implementaci systému Iris.