MUNI SUKB Správa Univerzitního kampusu Bohunice

POŽADAVKY NA BEZPEČNOSTNÍ SYSTÉMY

V2.21

OFM SUKB MU

Brno, 02/2021

MUNI SUKB Správa Univerzitního kampusu Bohunice

Obsah

1. ÚVOD

Tento dokument popisuje vlastnosti, které jsou závazně požadovány od přístupového systému (elektronická kontrola vstupu, dále EKV), zabezpečovacího systému (poplachový, zabezpečovací a tísňový systém, PZTS) a systému elektrické požární signalizace (dále EPS), aby mohl být nainstalován a provozován v budovách Masarykovy univerzity. Je závazný také v případě rozšíření již instalovaného systému.

Zadávací a provozní požadavky nelze zcela oddělit, protože struktura systému (rozmístění a zapojení prvků) do značné míry předurčuje možnosti používání i provozní režim. Cílem tohoto dokumentu je stanovit jednotné požadavky na zabezpečovací a přístupové systémy (souhrnně zde nazvané jako bezpečnostní systémy) a rovněž definovat koncepci jejich provozu. Pro všechny výše uvedené systémy jsou rovněž uvedeny požadavky na integraci do BMS MU.

V textu tohoto dokumentu se na vícero stranách vyskytuje slovo „Garant“, což zaslouží stručnou definici: *„Garantem se rozumí součást MU zodpovědná za provoz, rozvoj a údržbu BMS MU; v této roli vystupuje Oddělení facility managementu Správy Univerzitního kampusu Bohunice Masarykovy univerzity.“*

2. KOMUNIKAČNÍ PROTOKOLY

Tato kapitola se zabývá popisem prostředků protokolu BACnet, které jsou použity při implementaci požadované funkcionality uvedené v kapitole 3.

2.1 Objekty

Obecná pravidla pro použití variant objektů (Input/Output/Value) je třeba dodržet. Input objekty mají být použity pro vstupy, Value pro „virtuální proměnné“ a Output objekty pro výstupy. Výjimkou je vícestavový vstup, kde namísto MultiState Input je nutné využívat objekty typu MultiState Value.

Konkrétně je stanoveno použít:

- Některý z objektů MultiState Output, MultiState Value[1] pro:
  - Publikování stavů prvků systému (čidla, zámky, zóny, ústředna/řídící jednotka…);
  - Nastavování režimů prvků systému;
- Některý z objektů Binary Input, Binary Output, Binary Value pro:
  - Publikování stavů prvků systému (čidla, zámky, zóny, ústředna/řídící jednotka…), pokud existují pouze 2 možné stavy;
  - Nastavování režimů prvků systému, pokud existují pouze 2 možné stavy;
- Objekty Schedule a Calendar pro nastavování časových plánů;

[1] Podle normy BACnet nesmí MultiState objekty nikdy nabývat hodnoty 0

- Objekty Event Enrollment v případě, že není použit „Intrinsic reporting“;
- Objekty Notification class pro směrování a kategorizaci alarmových zpráv;
- Objekt Device se všemi povinnými vlastnostmi definovanými normou BACnet.

2.2 Služby

Následující seznam obsahuje seznam služeb, které zařízení musí podporovat pro komunikaci s ostatními zařízeními. Název služby *provedený kurzívou* značí schopnost odpovědět na požadavek (Execute), podtržení značí schopnost vytvořit požadavek (Initiate).

- Základní síťové služby protokolu BACnet (WhoIs, IAm, WhoHas, IHave, *TimeSynchronization*/*UTCTimeSynchronization*[2]);
- *ReadProperty* a *ReadPropertyMultiple* pro čtení dat;
- *WriteProperty* a *WritePropertyMultiple* pro zápis dat;
- ConfirmedEventNotification a UnconfirmedEventNotification pro zasílání událostí do BMS. Události musí být možné směrovat na seznam konkrétních zařízení definovaných pomocí ID zařízení a/nebo číslem sítě;
- ConfirmedCOVNotification, UnconfirmedCOVNotification, *SubscribeCOV* pro zasílání informací o změnách hodnot;
- *AcknowledgeAlarm* pro příjem potvrzení o přijetí alarmu obsluhou;
- *GetAlarmSummary, GetEnrollmentSummary* a *GetEventInformation* pro získání aktuálních platných událostí ze systému.

2.3 Názvy a adresy objektů

Názvy a adresy objektů jsou odvozeny od adresy prvku (např. zóny, přístupového bodu, čidla, tlačítka) v příslušném systému. V případě, že je název objektu odvozen od adresy v bezpečnostním systému, je třeba, aby tato adresa byla z názvu snadno zjistitelná.
Jména objektů sumárních stavů musí být konfigurovatelná a odpovídat jmenné konvenci objektů BMS MU.

2.4 Chování

Následující část popisuje požadované chování bezpečnostních systémů a konkrétní reakce na změny stavu systému, které jsou propagovány do BMS.
Příklady nastavení událostí, které vznikly v rámci bezpečnostních systémů:

- Informace o Odstřežení/zastřežení zóny, změna stavu integrovaného přístupového bodu (prostřednictvím čtečky) – Nepotvrzovaná událost (UnconfirmedEventService, NotifyType = Event, EventType = ChangeOfState, EventState = Normal, MessageText = podle konfigurace, EventValues = CHANGE_OF_STATE);

[2] Dostačuje pouze jedna z nich, časové služby mohou být nahrazeny NTP

- Poplach v PZTS = Potvrzovaný alarm vyžadující Ack (ConfirmedEventService, NotifyType = Alarm, EventType = ChangeOfState, EventState = OffNormal, AckRequired=True, MessageText = podle konfigurace, EventValues = CHANGE_OF_STATE;
- Poplach v EPS = Potvrzovaný alarm vyžadující Ack (ConfirmedEventService, NotifyType = Alarm, EventType = ChangeOfState, EventState = OffNormal, AckRequired=True, MessageText = podle konfigurace, EventValues = CHANGE_OF_STATE;

Dále se problematice alarmingu věnuje kapitola 5.

Vzdálené ovládání systémů:

- Varianta 0: Integrace je pouze jednosměrná, systém není nijak ovládán – platí pouze pro EPS;
- Varianta 1: Systém bude vzdáleně ovládán změnou hodnoty v příslušných objektech, které zároveň slouží pro předávání stavu systému do BMS MU. Např. BV (Binary Value) objekt se stavem zóny – odstřeženo, zastřeženo, přepnutí do „Inactive“ zónu odstřeží, přepnutí do „Active“ zastřeží);
- Varianta 2: Objekty pro ovládání jsou odděleny od objektů pro sledování stavu. Existují tedy např. objekty, které reprezentují jednotlivé příkazy: zastřežit zónu, odstřežit zónu, vynutit zastřežení, odložené zastřežení. Nastavením hodnoty na „Active“ se provede daný příkaz, po provedení se hodnota Present Value u objektu automaticky vrátí zpět na „Inactive“;
- Ovládání systému časovými plány a kalendáři může být zajištěno buď přímo (provázáním kalendářů s rozvrhy přes vlastnost Exception_Schedule u kalendářů a provázání kalendářů s objekty ovládajícími systém přes „Object property references“), nebo pomocí programu např. v integračním zařízení.

K zaslání události o změně stavu systému (viz výše) musí dojít i tehdy, pokud byla akce vyvolána vzdáleně z BMS MU. Pokud z nějakého důvodu nebylo možné akci provést, bude o tom systém informovat BMS MU zasláním alarmu.

3. DEFINICE ROZHRANÍ S BMS

Následující část dokumentu popisuje data a funkce, které musí bezpečností systémy poskytovat do integračního prostředí BMS MU. Zde se využívá jako základní prostředek komunikace protokol BACnet. Data, získávaná ze zařízení pomocí tohoto protokolu, jsou poté uživatelům prezentována prostřednictvím webového rozhraní BMS MU. Pro zajištění bezproblémového chodu BMS MU tedy Garant neověřuje pouze kompatibilitu s protokolem BACnet, ale také se softwarem firmy Delta Controls. Převodník musí splňovat požadavky stanovené v dokumentu „Infrastruktura BMS“, zejména požadavky kladené na zařízení tohoto typu.

Obecně systém, který musí komunikovat jak s BMS MU, tak se správou identit, vyžaduje dvě samostatná síťová rozhraní.

3.1 Předávaná data a funkce systému

V následujících částech jsou popsány data a funkce, které musí bezpečnostní systémy PZTS, EKV a EPS poskytovat uživatelům a správcům prostřednictvím systému BMS MU, to znamená poskytovat je prostřednictvím standardních objektů a služeb protokolu BACnet, popsaných v normě ČSN EN ISO 16484-5. V případě, že není možné některé z funkcí implementovat přímo do ústředny systému, je nutné řešení doplnit vhodným integračním zařízením, které schopnosti systémů rozšíří o požadované funkce (např. Delta Controls eBMGR, Delta Controls eBCON). Toto integrační zařízení musí projít testováním kompatibility v laboratoři BMS.

3.1.1 PZTS

Data:

- Veškeré systémem rozeznávané stavy periferií (zejména čidel a napájecích zdrojů, příp. tísňových tlačítek a výstupů, jsou-li použity)[3]. Přenášení stavu „narušeno bez poplachu“ je možné, ale s možností vyřazení
- Stavy zón[4]
- Stavy linkových prvků (expandér/koncentrátor, klávesnice)
- Sumární stavy – podlaží, budova (budova je zastřežena, pokud jsou zastřeženy všechny zóny, které se v ní nacházejí)
- Stav ústředny/stav komunikace s ústřednou

Funkce:

- Vzdálené odstřežování a zastřežování zón včetně všech variant, které systém podporuje (odložené, nucené,…)[4]

[3] Stav některých čidel/zámků může být nahrazen tzv. stavem „dveří“, pokud je čidlo/zámek součástí takového celku (viz dále)

[4] Může být nahrazen stavem/funkcí „integrovaného přístupového bodu“, pokud je zóna/přístupový bod součástí takového celku (viz dále)

- Vytváření a konfigurace časových rozvrhů pro odstřežování/zastřežování
- Synchronizace času (příjemce TimeSynchronization po BACnetu), alternativně lze řešit pomocí NTP
- Notifikace indikující odstřežení a zastřežení zóny včetně nastavitelných alarmových textů (nastavení nemusí probíhat přes BACnet)
- Alarmy indikující poplach včetně volně nastavitelných alarmových textů (nastavení nemusí probíhat přes BACnet)
- Alarmy indikující změnu stavu ústředny/komunikace s ústřednou včetně volně nastavitelných alarmových textů (nastavení nemusí probíhat přes BACnet)

3.1.2 EKV

Data:

- Stavy zámků (Odemknut, Uzamknut + případné další, které systém detekuje – porucha,…)[3]
- Režim zámku (Výuka/Mimo výuku)[4]
- Stav ústředny/komunikace s ústřednou

Funkce:

- Vzdálené odemykání a zamykání zámků
- Vytváření a konfigurace časových rozvrhů pro odemykání/zamykání zámků
- Vzdálená změna režimu zámku (Výuka/Mimo výuku)[4]
- Vytváření a konfigurace časových rozvrhů pro změnu režimu zámků[4]

3.1.3 EPS

Data:

- Veškeré systémem rozeznávané stavy periferií
- Sumární stavy
- Stav ústředny/stav komunikace s ústřednou

3.1.4 Společné

Data:

- Indikace stavu „integrovaného přístupového bodu“ (zóny PZTS + přístupového bodu EKV):
    - Zamčeno + zastřeženo – čeká na privilegovaného uživatele EKV /vzdálené odstřežení
    - Zamčeno + odstřeženo – vpouští neprivilegované uživatele EKV
    - Výuka – režim učebny ve výuce, trvale otevřený zámek
    - Případné další, které systém detekuje (Sabotáž, Porucha)

- Indikace stavu „dveří“ (čidla PZTS + zámku EKV):
    - Zavřeno + Zamčeno – dveře jsou zavřeny, zámek uzamčen, systém čeká na přiložení karty
    - Zavřeno + Odemčeno – nastává během režimu učebny „Výuka“;
    - Otevřeno – dveře jsou otevřeny
    - Případné další, které systém detekuje (Sabotáž, Porucha)

Funkce:

- Vzdálené nastavení režimu „integrovaného přístupového bodu“ (Zamčeno + zastřeženo, Zamčeno + odstřeženo, Výuka) včetně případného automatické odstřežení a zastřežení (včetně všech variant podporovaných systémem)
- Vytváření a konfigurace časových rozvrhů pro změny režimu „integrovaného přístupového bodu“
- Události indikující změnu stavu „integrovaného přístupového bodu“ včetně nastavitelných alarmových textů (nastavení nemusí probíhat přes BACnet)

4. TRENDOVÁNÍ

Vytvoření trendlogů je realizováno v prostředí BMS dle požadavku na konkrétní realizaci a řídí se běžnými požadavky na trendování (preference COV apod.), standardně trendování provozních stavů neprobíhá. Vzhledem k výčtu prvků, jejichž stavy mají být předávány do BMS (kapitola 3.1), je tedy možné trendovat libovolný fyzický či virtuální prvek systému.

5. ALARMING

Nastavení alarmingu (resp. zasílání událostí) zpravidla probíhá na převodníku systému PZTS, případně přímo v konfiguraci ústředny, je-li převodník integrovaný. Požadavky na implementaci alarmingu prostřednictvím protokolu BACnet a další požadavky jsou uvedeny v 2.

Pro potřeby zabezpečovacích a přístupových systémů rozeznáváme následující stavy objektů a jim příslušející přechody:

- Normal -> Alarm – přechod z klidové stavu do alarmu
- Alarm -> Normal – přechod z alarmu do klidového stavu
- Fault -> Normal – přechod z poruchy do klidového stavu
- Normal -> Fault – přechod z klidového stavu do poruchy

Platí, že pro každý typ přechodu je umožněna konfigurace všech příslušných událostí plošně, tedy jedno společné nastavení pro všechny. Zejména je nezbytné, aby měl Garant možnost konfigurovat režim zasílání alarmů na úrovni uvedených typů přechodu, tzn. např. je možné nastavit, aby poplach byl zasílán jako událost vyžadující potvrzení (BACnet acknowledgement), ale návrat do normálu z téhož zdroje už nikoliv. Stejně tak musí být možné zasílání událostí pro vybraný typ přechodu

zcela vyřadit. Dále musí být umožněno nastavovat jednotlivý událostem typ Alarm, nebo Notification, a to jak jednotlivě, tak dle typů události podle zdroje (např. nastavit, že všechny události zastřežení jsou typu Notification, všechny události porucha napájecího zdroje jsou typu Alarm atp.).

6. POPIS UŽIVATELSKÉHO ROZHRANÍ BMS

Systémy PZTS, EKV i EPS je třeba integrovat do BMS včetně vytvoření příslušných obrazovek. Pro EPS pak platí požadavek na jednosměrnou integraci, ostatní zůstává (viz kapitola 13). Obecně platí, že všechny datové body na převodníku mají v obrazovkách grafickou reprezentaci, se zohledněním všech jejich možných stavů. Nejedná se tedy pouze zobrazení stavů periferií, ale i dalších, jako např. napájecích zdrojů, tamperů,… i objektů bez fyzické reprezentace – např. komunikace s ústřednou.

Vizualizace bezpečnostních systémů v rámci webového rozhraní BMS MU musí být provedena ve standardu stávajícího řešení a začleněna do jeho struktury. Konkrétně:

1. Pro každé podlaží budovy vytvořit obrazovku se zastoupením všech zde obsažených zařízení, která bude obsahovat přehled zón a tlačítka pro jejich ovládání
2. Do přehledové obrazovky budovy začlenit odkazy na jednotlivé obrazovky podlaží
3. Do přehledové obrazovky budovy přidat přehled všech jejích zón (s aktuálním stavem) spolu s tlačítky pro jejich ovládání
4. Vytvořit souhrnné přehledové obrazovky pro:
    a. Napájecí zdroje
    b. Tísňová tlačítka
    c. Tampery (ústředen, modulů, skříní)
5. Definovat alarmová hlášení pro každou zónu (může být upřesněno Investorem či Garantem)

Pro prvky PZTS a EKV jsou stanoveny následující barevné kódy jednotlivých stavů:

ID		STAV	R	G	B
1		stav neznámý	255	255	255
2		neaktivní	128	128	128
3		aktivní/otevřeno	0	128	0
4		zastřeženo	0	128	255
5		přemostěno	255	0	255
6		sabotáž/porucha	255	255	0
7		poplach	255	0	0
8		byl poplach	255	128	128
9		zavřeno + zamčeno	128	0	255
10		zavřeno + odemčeno	0	255	255

Význam položek:

1. Neaktivní – čidlo je v klidu
2. Aktivní/otevřeno – číslo je aktivní (tzn. PIR zaznamenává pohyb, magnetický kontakt je rozpojen), ale není zastřeženo, tedy nevzniká alarm
3. Zastřeženo – čidlo je zastřeženo a zároveň neaktivní
4. Přemostěno – čidlo bylo vyřazeno ze zastřežování
5. Sabotáž/porucha – na čidle (resp. kabeláži k čidlu) je detekován poruchový stav způsobený závadou nebo úmyslným poškozením
6. Poplach – čidlo bylo zastřeženo a následně aktivováno, což vyvolalo poplach. Tento stav trvá.
7. Byl poplach – čidlo bylo v poplachovém stavu, který již netrvá, nicméně nebyl dosud resetován.
8. Zavřeno + zamčeno - dveře jsou zavřeny, zámek uzamčen
9. Zavřeno + odemčeno - dveře jsou zavřeny, zámek je odemčen, dveře lze tedy otevřít

Uvedené barevné kódy platí výhradně pro grafickou reprezentaci stavů jednotlivých prvků, nikoliv pro jiné použití v rámci webového rozhraní BMS MU.

Důležitým aspektem vizualizace bezpečnostních systémů je omezení přístupových práv – geografické a funkční (tedy omezení na jednotlivé lokality a omezení na pouze sledování nebo ovládání). Oba tyto rozměry mohou být samozřejmě kombinovány – v jedné lokalitě smí uživatel prvky pouze sledovat, v další i ovládat, v některých nemá žádná práva.

Prvotní nastavení práv je věcí dodavatele BMS MU, který bude tuto oblast koordinovat s Garantem. Dále přechází správa těchto práv na Garanta.

Základní dělení práv na bezpečnostní systémy ve vizualizaci (další položka v seznamu zahrnuje vše z předchozí):

1. Uživatel
    a. má právo prohlížet objekty (obrazovky) na jemu příslušné skupině obrazovek/zařízení
    b. má právo prohlížet alarmy na jemu příslušné skupině obrazovek/zařízení
2. Ostraha
    a. má právo zastřežovat a odstřežovat zóny na jí příslušné skupině obrazovek/zařízení
    b. má právo potvrzovat alarmy na jí příslušné skupině obrazovek/zařízení
3. Správa budovy
    a. má právo přemosťovat objekty a zóny na jí příslušné skupině obrazovek/zařízení
    b. má právo nastavovat režim přístupových bodů na jí příslušné skupině obrazovek/zařízení
4. Administrátor
    a. má prohlížet a ovládat všechny objekty a zařízení
    b. spravuje práva ostatních uživatelů

Příslušnost obrazovek a zařízení k jednotlivým uživatelům stanovuje Garant.

7. NAPÁJENÍ

Pro systémy PZTS, EKV a EPS platí požadavek na kategorii napájení 2, tzn. zálohování dieselagregátem.

Tyto systémy jsou vybaveny vlastními záložními akumulátory, které umožní provoz bez externího napájení, a to po dobu nejméně 6 hodin od přerušení napájení (ve specifických případech dobu zálohy určí Garant). Dodány budou akumulátory určené pro provoz s PZTS (EKV, EPS).

Napájení bude navrženo tak, že při maximálním odběru připojených zařízení zůstane výkonová rezerva zdroje 40%.

8. INTEGRACE S OSTATNÍMI TECHNOLOGIEMI

Tato část popisuje rozhraní systému IS MU, které musí být použito pro synchronizaci údajů o lidech a jim přidělených přístupových kartách. Jde o stahování oprávněných karet do systému EKV a rovněž nahrávání údajů o průchodech zpět do IS MU, přičemž obě tyto funkcionality jsou požadovány, není-li Garantem stanoveno jinak. Text části byl poskytnut Centrem výpočetní techniky Fakulty informatiky.

8.1 Integrace s univerzitní správou identit

8.1.1 Pojmy

Lidé

- Jsou v systému evidováni svým Univerzitním číslem osoby (UČO), případně dalším identifikátorem (RZ automobilu, biometrické údaje)

Karty

- Jeden člověk může mít nejvýše jednu aktivní (= nezrušenou) kartu, zároveň musí mít možnost přidělení více identifikátorů v systému (např. RZ automobilu, biometrické údaje atp.)

Externisté

- Kromě lidí můžou být karty vázány na tzv. externisty (např. úklidová firma).
- Externista má také své číslo, přičemž se jedná o jinou sekvenci než UČO (obě sekvence nejsou vzájemně unikátní – může se vyskytovat člověk i externista se stejným číslem; je podstatné, jak dané číslo interpretovat).

Skupiny osob

- Skupina má svoje číslo a lze do ní zařadit lidi a externisty.
- Skupina má své správce, kteří mohou zařazovat a vyřazovat členy skupiny: buďto přímo, anebo nastavením tzv. plnicí funkce (studenti předmětu XY, zaměstnanci pracoviště Z, členové skupiny A,...).

8.1.2 *Skupiny a EKV*

- Skupiny mohou být mapovány na jednu nebo více čteček EKV.
- Doporučuje se mapování 1:1, s výjimkou případu, kdy více čteček řídí přístup do toho stejného prostoru (více dveří do učebny).
- Je-li třeba kombinovat EKV s PZTS, můžou být pro jeden přístupový bod zavedeny dvě skupiny - "smějí vstoupit" a "smějí zastřežit".
- Mapování se provádí na straně EKV, IS MU neřeší vztah skupin a čteček EKV.

8.1.3 *Komunikace se serverem*

- Server na straně IS MU je dostupný na adrese is.muni.cz.
- Je třeba přistupovat protokolem HTTPS a ověřovat certifikát serveru.
- Certifikát je třeba ověřovat proti bundle certifikačních autorit dostupnému v rámci běžných prohlížečů nebo operačního systému.

8.1.4 *Export osob a externistů k dané skupině osob*

- URL aplikace pro export je https://is.muni.cz/export/skupiny_osob.pl?skupina=N;format=F kde N je číslo skupiny osob, F je formát výstupu. Pro ostrý provoz je třeba použít formát "csv" - u žádného jiného formátu nelze zaručit jeho neměnnost v budoucnosti. Dále existuje formát "debug" pro zobrazení HTML přímo do stránky.
- Přístup k výše uvedenému URL je omezen na IP adresu a skupinu (skupiny) osob.
- K aplikaci se přistupuje metodou GET, v případě úspěchu vrátí 200 OK a data v příslušném formátu a kódování.
- V HTTP hlavičce Content-Length je uvedena délka vrácených dat v bajtech. Tímto lze rozpoznat například data uříznutá kvůli nějaké chybě přenosu. Tuto hlavičku je tedy třeba vždy kontrolovat.

Výstupní formát CSV

- Oddělovač je středník, kódování je UTF-8.
- Sloupce jsou:
  - UČO (univerzitní číslo osoby)
  - ID externisty (vždy je uveden právě jeden z prvních dvou sloupců)
  - jméno osoby nebo externisty (včetně titulu)
  - číslo čipu karty (pozor, někteří výrobci používají opačné pořadí bitu v šestnáctkových číslicích, tedy záměnu 1 <--> 8, 2 <--> 4, 3 <--> c, 5 <--> a, 7 <--> e, b <--> d)

Příklad výstupního souboru (pro formát=csv):

```
1337;;08084554c0;"XXX"
27380;;08065f0de1;"XXX"
;1742;0f048636ac;"vrátnice"
```

Výchozí perioda stahování je 10 minut (není-li MU stanoveno jinak), u extrémně velkých skupin (nad 10 000 osob) může systém EKV podle své potřeby použít adekvátně delší interval, například hodinu. Toto omezení ale není omezením ze strany IS MU.

Pokud přístupový systém stahuje údaje pro větší počet skupin, je třeba nestahovat vždy přesně od začátku každé desáté minuty skutečného času, ale stahování dat posunout o náhodnou dobu tak, aby se přístupy ze všech EKV systémů rozložily v čase – je třeba koordinovat prostřednictvím Garanta.

8.1.5 Import údajů o průchodech

- URL aplikace pro import je https://is.muni.cz/export/skupiny_osob_pruchody.pl
- Přístup k výše uvedenému URL je omezen na IP adresu a skupinu (skupiny) osob.
- K aplikaci se přistupuje metodou POST, kde se v parametru "pristupy" posílá CSV s následujícími sloupci:
  - čas přístupu (počet sekund od 1. 1. 1970 GMT, je třeba uvádět skutečný čas průchodu, nikoliv čas importu
  - číslo skupiny osob/přístupového bodu
  - číslo čipu
  - typ operace:
    0 = nepovolený přístup
    1 = vstup
    2 = výstup
- Je-li osazena jen vstupní čtečka, nebo nemá-li pojem vstup/výstup smysl, uvádí se hodnota 1.
- Přístupy je třeba vkládat setříděné podle času od nejstaršího.

Příklad importovaných dat (posílat jako HTTP POST parametr s názvem "pristupy"):

```
1184849407;134;0f084136bc;1
1184849410;134;0f084136bc;2
```

Výchozí perioda importu průchodů je 10 minut (není-li MU stanoveno jinak), je možné pro všechny přístupové body (skupiny osob) ukládat jedním společným požadavkem POST.

Pokud bude potřeba synchronizovat přesný čas zařízení kvůli přesnému času průchodu, doporučuje se použít protokol NTP proti serveru time.fi.muni.cz. Méně preferovaný, ale možný je protokol SNTP, případně i timep (zde je přístup povolen jen ze sítě MU).
Z hlediska systému se nerozlišuje, jestli jde o průchod, nebo odstřežení/zastřežení. Pokud má přístupový bod zvlášť skupinu osob s oprávněním odstřežit/zastřežit, pak "průchod" zaznamenaný k této skupině se bere jako záznam o odstřežení/zastřežení, zatímco průchod zaznamenaný k běžné skupině "smí vstoupit" se bere jako skutečný průchod.

Chybové stavy

Pokud HTTP POST neprojde vůbec nebo vrátí jiný HTTP status než 200 OK, import do IS MU neproběhl a je třeba během příštího importu data zaslat znovu.
Pokud IS převezme data, vrátí se 200 OK a dokument typu text/plain, který bude mít na prvním

řádku "ERROR: <popis_chyby>", vyskytl se nějaký globální problém, který importní aplikace dokázala rozpoznat. Opět platí, že k importu nedošlo. Příkladem tohoto stavu je nepoužití metody POST.
Jinak bude HTTP status 200 a bude vrácen dokument text/plain, který bude mít na prvním řádku "OK". Pak se importovaly ty záznamy, které níže nebyly označeny za chybné. Chybné záznamy (nesmyslné datum, neoprávněný přístupový bod k IP adrese klienta atd.) se hlásí na dalších řádcích ve formátu CSV s těmito sloupci:

```
cislo_radku;<radek samotny>: <zprava>".
```

Příklad:
Pro vstup se dvěma řádky, z nichž druhý má v sobě chybu toho typu, že z dané IP adresy není povolen import průchodů k příslušné skupině osob, by byl obdržen tento výstup:

```
OK
2;1184849410;107;0f054636bc;2: nepovolena skupina osob
```

Testování

Aplikace https://is.muni.cz/export/skupiny_osob_pruchody.pl bez parametrů zobrazí HTML formulář, do kterého lze rovnou vložit CSV data ve výše uvedeném formátu a použít tak pro testování.

Další možnosti konfigurace importu

Následující dvě možnosti rozšířené konfigurace importu průchodů budou použity pouze na základě požadavku MU a po nezbytné koordinaci.

Použití CRC místo čísel karet

S parametrem "crc=1" lze importovat průchody nikoli prostřednictvím čísel karet,
ale použitím jejich CRC. Díky použití tohoto parametru pak systém EKV nebude pracovat se skutečnými čísly karet, což slouží jako prevence pro případný únik.

Dodatečné zabezpečení pomocí klíče

V případě, kdy je systém EKV v síti se sdílenou veřejnou adresou s dalšími stanicemi (při použití NAT), lze použít parametr „klic=.....“, který se přidá do URL. Kromě omezení na IP adresu registrovanou v IS MU se pak ověřuje zadaný klíč.

Kontakt

Vývojový tým Informačního Systému MU:
XXXXXXXXX

8.2 Integrace do prostředí technologické sítě

Systémy PZTS a EKV jsou jednotně ovládány prostřednictvím centrálního serveru, který připojuje řídící jednotky. Server slouží k obousměrné komunikaci s IS MU prostřednictvím firewallu, chránícího přístup do technologické sítě MU (jednoduchá definice pravidel).

9. PROVOZNÍ (FUNKČNÍ) POŽADAVKY

Provozní požadavky se vztahují na fungování systému při běžném provozu. Vymezují potřebnou funkcionalitu ve vztahu k uživateli systému.
Veškeré nově instalované systémy, či systémy rozšiřované, musí být na všech úrovních kompatibilní se systémy již provozovanými v rámci lokality. Pokud nelze jinak, je nutné kompatibilitu zajistit úpravou (případně výměnou) již provozovaných (pod)systémů.

9.1 EKV

- Integrace s BMS – sledování provozního stavu a ovládání přístupových bodů (kap. 6.1.1);
- Integrace s univerzitní správou identit – konfigurace přístupových bodů a zaznamenávání průchodů a pokusů o průchod (kap. 6.2);
- Integrace se systémem PZTS (kap. 5);
- Odezva systému (tzn. otevření zámku nebo zamítnutí vstupu) na přiložení karty do 1s;
- Možnost nastavení doby, po kterou zůstane zámek otevřený;
- Kapacita jednoho přístupového bodu 50 000 karet;
- Vizuální a zvuková signalizace stavu zámku na čtečce u přístupového bodu – možnost odlišení následujících stavů:
    - připraven na přiložení karty;
    - přístup povolen/zámek otevřen;
    - přístup odmítnut;
- Podpora různých režimů zámků:
    - „Běžný prostor/Učebna mimo výuku“ – po přiložení karty se zámek jednorázově otevře a po zavření dveří opět zamkne;
    - „Učebna během výuky“ – po přiložení karty se zámek otevře a zůstane otevřený až do průchodu přes odchodovou čtečku/přiložení karty se stisknutým tlačítkem/zastřežení místnosti ((kap. 11) – režim Učebna).

- Čtečky karet musí bezdotykově číst čipy EM4102 125 kHz (současné ISIC a zaměstnanecké karty) a MIFARE DESFire EV1. Na výzvu Garanta bude dodána testovací sada pro ověření kompatibility (čísla čipů musí být čtena/interpretována shodně se stávajícími systémy).

9.2 PZTS

- Integrace s BMS – sledování stavu periferií a sledování a ovládání stavu systému (viz dále)
- Veškeré klávesnice jsou vybaveny čtečkou (integrovaná, externí)
- Integrace se systémem EKV (viz dále)

9.3 EPS

- Integrace s BMS – sledování stavu periferií a sledování a ovládání stavu systému (viz dále)

10. POŽADAVKY PRO SPRÁVU SYSTÉMU

Požadavky pro správu systému jsou myšleny vyžadované vlastnosti řešení, které jsou nutné pro zajištění funkčnosti systému jeho správcem, ať už za běžného provozu, nebo při řešení nestandardních situací (např. uživatel EKV není vpuštěn do dveří, došlo k selhání HW, chyba synchronizace s nadřazeným systémem,…).

10.1 Struktura a správa práv

Zabezpečovací a přístupové systémy (či spíše jejich provoz) jsou ovlivněny množstvím různých vstupních bodů, které mohou ovlivňovat jejich chování. Následuje výčet možných vstupních bodů:

1) IS
   a) Oprávnění na správu skupin osob
   b) Oprávnění na zavádění/přidělování karet (externistům)
   c) Další oprávnění v ISu (definice skupin osob,…)
2) Převodník, softwarové nástroje
   a) Přístup do převodník pro synchronizaci s IS (OS, aplikace)
   b) Přístup do ústředny přes konzoli (technik)
   c) Přístup do převodník BACnet (OS, aplikace)
3) Technologická síť
   a) Přístup přes nástroj pro přímý přístup do sítě (typicky ORCAview)
   b) Přístup přes Webové Rozhraní BMS MU
   c) Jiný přístup přes technologickou síť (SW dalších výrobců, vlastní SW)
4) Fyzický přístup
   a) Lokální kódy (uživatelské, Master a Technik)
   b) Přidělování klíčů a konfigurace zámků

Uvedený výčet pokrývá celý „životní cyklus“ přístupových práv, od manipulace s oprávněními pro karty, které musí být zadávány výhradně prostřednictvím IS MU, dále práva na ovládání zabezpečovacího systému, ať už lokálně nebo prostřednictvím BMS, a nakonec přidělování klíčů (kde je třeba přihlédnout ke struktuře systému generálního klíče).

Skupina 1 (IS) je mimo doménu tohoto dokumentu, správu skupin osob, identit a dalšího zajišťují jiná pracoviště MU.

Skupina 2 je v kompetenci dodavatele, zde je třeba koordinovat s Garantem přístup během záruky díla a po jejím skončení. Během záruky MU požaduje přístup k těmto zařízením a nástrojům minimálně v režimu sledování (čtení), který umožní detekovat případné poruchové stavy a uvědomit dodavatele o problému. Administrátorský přístup zůstává po dobu záruky dodavateli, pokud není dohodnuto jinak.

Po skončení záruky a převzetí administrátorských oprávnění je ze strany Garanta třeba provést následující kroky:

1. Administrátorské účty (zpravidla v OS nebo specializované aplikaci)
    a. Změna veškerých přístupových údajů ve všech uvedených bodech
    b. Uchování těchto údajů ve vyčleněném, zabezpečeném dokumentu – administrátorská dokumentace
    c. Tyto účty nebudou nadále určeny pro běžný provoz, pouze pro řešení havarijních situací
    d. V případě, že je třeba zásah dodavatelské/servisní firmy a tedy poskytnutí těchto údajů, musí být po skončení zásahu změněny (a aktualizována administrátorská dokumentace)
2. Provozní účty
    a. Pokud nebyly dosud vytvořeny, provést nyní a provádět nadále potřebné operace (včetně provozu služeb apod.) pod těmito účty
    b. Uchování těchto údajů v administrátorské dokumentaci

Skupina oprávnění 3 je v kompetenci Garanta, dodavatel do technologické sítě nemá přístup. Platí pravidla pro provoz TeNe.
Skupina 4 zahrnuje dvě poměrně odlišné oblasti. Kódy pro místní ovládání PZTS (běžné účty, správcovské účty) nejsou synchronizovány se správou identit, ale drženy pouze v paměti ústředny (případně obslužné databáze). Zvláštním případem je virtuální klávesnice (funkcionalita řešení Asset), která emuluje místní přístup pomocí nástavbové aplikace. Funkčně se neliší od fyzické klávesnice.

Běžné lokální uživatelské účty PZTS (tedy číselný kód svázaný s jistou funkcionalitou) jsou provozně značně problematické, zejména z důvodu nepohodlné a nekoncepční správy (účty je většinou třeba spravovat ručně pro každou ústřednu), nízkou důvěryhodnost a s tím související netransparentnost (kódy mají tendenci se šířit a nelze pak zamezit neoprávněnému použití či vysledovat skutečného uživatele). Z těchto důvodů se oddělené ovládání PZTS jeví jako nevyhovující, maximálně preferované je pak ovládání prostřednictvím EKV, které tyto problémy odbourává. Použití neintegrovaného PZTS je možné po doložení neexistence jiné varianty (např. kvůli úplné absenci EKV), podléhá schválení Garanta.

Kódy Master (příp. Správce) a Technik, se kterými ústředny pracují, je třeba pečlivě chránit proti zneužití. Obdobně jako u údajů pro správu SW nástrojů (druhá skupina), i zde je po dobu trvání záruky správa systému v rukou dodavatele. Po skončení záruky budou uplatněna obdobná opatření (změna hesla, zavedení do administrátorské dokumentace, vytvoření běžných provozních účtů,…) i pro tyto účty.

10.2 EKV

- Se systémem musí být dodán obslužný SW, který umožní kompletní správu systému. To znamená zejména přístup k veškerým servisním informacím ze systému – zejména logy, oprávnění karet, přístupové body;
- V případě, že je pro správu nutný i specifický HW, bez kterého není možná vzdálená (tzn. po počítačové síti) správa (např. sériový port nebo různé převodníky), musí být součástí dodávky i HW, který vzdálenou správu umožní.
- Ústředna EKV je umístěna v rozvodně SLP, případně je EKV plně integrováno – je součástí řešení PZTS.

10.3 PZTS

- Systém musí umožnit konfiguraci zón Garantem, tzn. umožnit definici rozsahu zón a prvků, které jsou jejich součástí.
- Systém splňuje požadavky platných norem (ČSN EN 50131) na plášťovou a prostorovou ochranu.
- Ústředna PZTS je umístěna v rozvodně SLP, u ústředny je umístěna klávesnice s integrovanou čtečkou, případně klávesnice a čtečka.

10.4 EPS

- V případě, že je EPS dodáváno v rámci lokality, kde již existuje EPS integrovaný do BMS MU, požaduje se možnost nově dodané řešení s původním funkčně propojit (zakruhování ústředen);
- Ústředna EPS je umístěna v rozvodně SLP.

11. TYPOLOGIE PROSTOR

Důležitou součástí koncepce bezpečnostních systémů je rozdělení prostor na jednotlivé druhy podle jejich charakteru, předpokládaného využití a tedy i požadavků na jejich zabezpečení a provozní režim. Toto rozdělení nemůže být zcela vyčerpávající, nicméně postihuje většinu potřebných situací. Po dohodě s Garantem či Investorem je možné konkrétní řešení upravit, režim fungování musí být detailně popsán v technické zprávě v rámci DSPS. V některých případech je účelné uvažovat spíše o skupinách místností, kde např. jedna z místností může být průchozí a místnosti za ní již nebudou např. zajištěny EKV (jde tedy o analogii zón PZTS). Místnosti mohou mít více dveří, které jsou buď na stejné úrovni (např. z chodby), nebo vedou do prostor různých úrovní (chodba má na jedné straně dveře ze společných prostor, na druhé straně dveře do prostoru laboratoří). Na rozhraní mezi jednotlivými zónami je vždy třeba zohlednit požadavky prostor s vyšším zabezpečením. Následuje výčet jednotlivých typů prostor s bodovou charakteristikou a požadavky.

11.1 Veřejné prostory

- veřejně přístupné – venkovní prostory, vstupní haly, chodby, koridory
- nezastřežuje se, není vybaveno PZTS
- z těchto prostor vedou dveře pouze ven a do prostor s omezeným přístupem

11.2 Společné prostory MU

- Je vybaveno EKV, přístupné pro všechny zaměstnance, studenty,…
- prostorová ochrana PZTS (pohybová čidla vybavená antimaskingem), v přízemních podlažích čidla tříštění skla a bezpečnostní magnetické kontakty na oknech
- typicky omezený přístup do celých budov a větších celků (nicméně provozně nelze zajistit vstup po jednom)
- jednosměrné přístupové body, nesleduje se obsazenost

11.3 Knihovny

- sleduje se příchod i odchod
- prostory s větší kapacitou osob, současně i požadavky na důsledné zabezpečení a ochranu proti krádežím, z toho důvodu je zpravidla použito další zabezpečení (rámy, turnikety), zároveň jsou zabezpečeny i únikové východy (akustická signalizace obsluze)

11.4 Auly, velké posluchárny[5]

- prostory pro více jak 50 osob, je možné EKV vyřadit (na základě rozvrhu, manuálně)
- nesleduje se odchod

11.5 Uzavřené chodby

- typicky chodby, ze kterých vedou vstupy do jednotlivých kanceláří, laboratoří
- nižší pohyb osob, vyšší požadavky na zabezpečení
- zpravidla zde neprobíhá výuka
- je možné provádět sledování odchodu/přítomnosti

11.6 Učebny

- je potřeba zajistit kompromis mezi přístupností pro studenty a dostatečným zabezpečením (řízení přístupu na základě synchronizace s rozvrhy atp.)
- mohou být vybaveny katedrami, tyto jsou pak zabezpečeny zvlášť (čtečka pro zapnutí výukových pomůcek, autorizace pouze pro vyučující)
- zpravidla se nesleduje odchod

[5] Garant může požadovat režim „11.6 Učebny“

- při odchodu možnost zastřežení čtečkou s odchozím tlačítkem

11.7 Laboratoře, specializované učebny

- požadavky jsou do značné míry závislé na místním uživateli, provozní možnosti závisejí na specifikaci v zadávací dokumentaci
- zpravidla se sleduje pouze příchod, je ale vhodné zvážit i sledování odchodu/přítomnosti
- mohou být doplněny hygienickou smyčkou
- vyšší požadavky na zabezpečení i bezpečnost, zpravidla tísňová tlačítka

11.8 Technické místnosti mimo SLP rozvodny

- typicky BVS, rozvodna ÚT, VZT, chlazení
- není vybaveno EKV
- klíče má k dispozici technický personál

11.9 SLP rozvodny[6]

- vysoké požadavky na zabezpečení, elektromechanický zámek
- má být sledován příchod i odchod, antipassback
- klíč má být použit pouze v odůvodněných případech – porucha, výpadek

11.10 Prostory s auty – parkoviště, garáže, koridory

- opatřeno závorou nebo roletou na vjezdu, příp. i výjezdu, autentizace kartou, případně RZ vozidla
- při výjezdu není nutná autentizace (dle konkrétních potřeb)
- sledování obsazenosti
- možnost vyhradit privilegovaná místa

11.11 Další typy prostor

Mezi další typy prostor mohou patřit např. různé specializované místnosti, které nelze postihnout v rámci jednotné metodiky. Jejich provozní režim má být stanoven v případě nové výstavby nebo rekonstrukce v zadávací dokumentaci, protože dodatečné změny mohou znamenat komplikované zásahy do již existující instalace.

Mezi další aspekty typologie prostor patří místnosti s více dveřmi (tyto jsou vnímány jako rovnocenné), průchozí místnosti (s výjimkou chodeb), únikové východy, požární koridory, střešní prostory přístupné zevnitř. Rovněž zde platí, že tyto případy řeší projektant dokumentace v koordinaci s Garantem a Investorem.

[6] Dle dohody s Garantem

12. INTEGRACE SYSTÉMŮ PZTS A EKV

Systémy PZTS a EKV musí být integrovány tak, aby PZTS reagoval na události z EKV a na základě nich byl schopný odstřežit a zastřežit příslušnou zónu. Konfigurace vazeb mezi přístupovými body z EKV a zónami v PZTS musí být možná vlastními silami MU. Vazba mezi přístupovými body EKV (čtečkami) a zónami PZTS je potenciálně až **M:N** - do jedné zóny PZTS je možné se dostat přes více přístupových bodů a jeden přístupový bod umožňuje vstup do více zón PZTS.

Osoby na MU se dají z pohledu přístupových a zabezpečovacích systémů rozdělit na dvě základní skupiny:

- Osoby s právem vstupu (studenti)
- Osoby s právem vstupu a odstřežení/zastřežení (pověření zaměstnanci a doktorandi) – tzv. „privilegovaní uživatelé EKV“

Systémy PZTS a EKV musí zvládat následující scénáře:

12.1 Chodba (11.2)

Prostor je odstřežován a zastřežován vzdáleně nebo automaticky (obsluhou BMS, časovým plánem). V případě, že je prostor odstřežený, uživatel EKV s právy k přístupovému bodu svázanému s příslušnou zónou PZTS je oprávněn vstoupit. Po jeho průchodu se zámek opět uzamkne.

12.2 Laboratoř/počítačová učebna (11.7)

Pokud je zóna PZTS zastřežena, systém EKV nevpouští neprivilegované uživatele EKV. Prostor může odstřežit privilegovaný uživatel EKV přiložením karty ke snímači. Je možné tento stav realizovat dvojitým přiložením karty – první přiložení odstřeží, druhé otevře zámek – toto chování však musí být doprovázeno odpovídající signalizací (vizuální/zvukovou). Po odstřežení prostoru systém EKV vpouští i neprivilegované uživatele EKV. Prostor je zastřežen přiložením privilegované karty k odchodové čtečce/přidržením tlačítka spolu s přiložením privilegované karty.

12.3 Učebna (11.6)

Prostor je odstřežován a zastřežován vzdáleně nebo automaticky (obsluhou BMS, časovým plánem) a čtečkou s odchozím tlačítkem. Právo vstupu (otevření zámku po přiložení karty) budou mít pouze oprávněné osoby („vyučující“). Studenti se do místnosti mohou dostat pouze tehdy, kdy je zámek trvale odemčený (viz dále). Ve chvíli, kdy je zóna PZTS odstřežena, mohou se přístupové body EKV příslušející k dané zóně nacházet ve dvou režimech (přepínání režimů je řešeno časovými plány přes integraci z BMS):

- Mimo výuku – běžné chování jako ve scénáři Chodba
- Výuka – Po průchodu oprávněné karty zůstane zámek trvale otevřen až do chvíle, než dojde k jedné z následujících událostí:

- přiložení oprávněné karty se současným stiskem tlačítka;
- Změně režimu na „Mimo výuku“;
- Zastřežení místnosti.

12.4 Zastřežovaná učebna (11.4)

Prostor je odstřežován a zastřežován přiložením oprávněné karty. Právo vstupu (otevření zámku po přiložení karty) budou mít pouze oprávněné osoby („vyučující“). Studenti se do místnosti mohou dostat pouze tehdy, kdy je zámek trvale odemčený (viz dále). Po odstřežení zóny zůstane zámek trvale otevřen, aby umožnil vstup studentům. Při zastřežení zóny přiložením oprávněné karty a stisknutím odchodového tlačítka dojde k uzamčení zámku.

12.5 Uzavřená chodba s laboratořemi (11.5)

Za dveřmi, opatřenými čtečkou, se nachází společný prostor, ze kterého se vstupuje do jednotlivých kanceláří/laboratoří. Ty již zpravidla nejsou opatřeny čtečkami. Společný prostor je samostatná zóna PZTS, pracovní prostory jsou sdruženy do zón podle příslušnosti k oddělením/katedrám/projektům.
Společný prostor je odstřežen s příchodem první oprávněné osoby. Ta zároveň odstřeží i svou „pracovní“ zónu, ve které má kancelář. Další osoby již odstřežují pouze své „pracovní“ zóny. Zastřežování pracovních zón probíhá samostatně, spolu se zastřežením poslední pracovní zóny dojde i k zastřežení společné zóny.
Možné řešení:

- Čtečka před vstupem do společné zóny (případně doplněná o tlačítkové/signalizační tablo) - slouží pro odstřežení společné a poté pro vstup do společné zóny případně i pro odstřežování pracovních zón);
- Čtečka za vstupními dveřmi (případně doplněná o tlačítkové/signalizační tablo) – zastřežování (případně i odstřežování) pracovních zón;
- Vizuální signalizace stavu zón (tablo u vstupu, kontrolky nade dveřmi).

Pozn.: Tento scénář může být dále rozšířen o privilegované a neprivilegované uživatele EKV a další čtečky u vstupu do konkrétních pracovních zón, které budou vpouštět studenty v případě odstřežení společného prostoru.

13. EPS

Elektrická požární signalizace je vyhrazené požárně bezpečnostní zařízení, a jako takové musí fungovat autonomně, bez ovlivnění jinými systémy (podrobnosti stanovuje ČSN 730875 v platném znění). Integrace tohoto systému do BMS je výhradně jednosměrná, z EPS jsou přenášeny a dále zpracovány informace prostřednictvím převodníku.
Ústředna EPS je umístěna v rozvodně SLP.

14. DOKUMENTACE

Kromě obecných požadavků na dokumentaci, uvedených v dokumentu Infrastruktura BMS, platí pro oblast PZTS, EKV a EPS následující specifika:

14.1 Popis prvků včetně adresace

Instalace PZTS a EKV zpravidla sestává z řídícího prvku – ústředny, který po linkách komunikuje s podřízenými prvky (moduly, expandéry,…), na kterých jsou zapojeny periferie (magnety, pohybová čidla, čtečky, zámky,…). Adresace těchto prvků pak je realizována prostřednictvím hierarchického kódu obsahujícím kód ústředny, kód linky, kód modulu a kód prvku. Tento kód má být použit v co nejranější fázi návrhu systému a musí se objevit ve všech půdorysech i v blokovém schématu. Blokové schéma musí být vedeno na úrovni jednotlivých periferií, včetně popisu typu a umístění.

Instalace EPS je organizována do kruhových linek, na kterých jsou společně umístěna jak čidla (a tlačítka nebo další prvky), tak prvky vstupů a výstupů (reléové moduly, kopplery), které slouží pro komunikaci (signály do rozvaděčů SLN a MaR, hlídání napájecích zdrojů) a připojení dalších prvků (sirény, přídržné magnety). Adresace těchto prvků je realizována prostřednictvím hierarchického kódu obsahujícím kód ústředny, kód linky, kód skupiny a kód prvku. Tento kód má být použit v co nejranější fázi návrhu systému a musí se objevit ve všech půdorysech i v blokovém schématu. Blokové schéma musí být vedeno na úrovni jednotlivých prvků, včetně popisu typu a umístění.

Některé prvky nemusí mít v systému jednoznačnou adresu (společně spínané sirény), stále však platí, že musí být jednoznačně, unikátně označeny v dokumentaci.

14.2 Popis složení zón

Systém PZTS je pro potřeby uživatelů rozdělen na jednotlivé zóny (podsystémy), které mohou být obsluhovány zvlášť a jsou mapovány na uživatelská oprávnění. Obdobně jako u požadavků na vizualizaci, i zde je třeba dodat dokumentaci tohoto rozdělení včetně případných návazností (např. zastřežení společné zóny v závislosti na jiné), formou výčtu zón, označení v ústředně i grafickému zobrazení. U EKV pak obdobně dodat seznam přístupových bodů, typu (jednosměrný/obousměrný), případně dalších údajů (turniket, hygienická smyčka, biometrická čtečka atp.).

14.3 Popis struktury instalace

Pro každou dodanou instalaci je třeba dodat výpis jejího kompletního složení, tzn. řídících prvků a připojených periferií, v tabulkovém formátu. Tuto funkcionalitu zpravidla nabízí nástavbový SW ústředny.

Součástí dokumentace je rovněž kompletní evidence použitých záložních akumulátorů, včetně jejich přesného typu, stáří, provozního napětí, kapacity a vypočteného zatížení.

15. SOUVISEJÍCÍ TECHNICKÉ NORMY A LEGISLATIVA

Přehled nejdůležitějších zákonů a norem, které definují způsob návrhu, montáže a servisu slaboproudých technologii, které se používají pro tento typ bezpečnostních systémů.

15.1 Poplachové zabezpečovací a tísňové systémy (PZTS)

ČSN EN 50131-1 ed. 2 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky

ČSN CLC/TS 50131-7 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace

TNI 33 4591-1: část 1 návrh systému PZTS
návrh systému, bezpečnostní posouzení, obsah projektové dokumentace, značky a zkratky pro projektování, vzorové zabezpečení objektu

TNI 33 4591-2: část 2 montáž PZTS
montáž systému – ústředny, napájecí zdroj, ovládací zařízení, detektory, signalizační zařízení, kabeláž

TNI 33 4591-3: část 3 uvedení PZTS do provozu a jeho následný provoz, údržba a servis
prohlídka systému, funkční zkouška, revize elektrického zařízení, proškolení obsluhy, zkušební provoz, pravidelná kontrola a údržba

ČSN EN 50131-6 ed. 2 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy – Část 6: Napájecí zdroje

ČSN EN 50131-3 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy – Část 3: Ústředny

15.2 Poplachové systémy – Systémy kontroly vstupů v bezpečnostních aplikacích

ČSN EN 60839-11-1 - Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty

ČSN EN 50133-1- Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky

ČSN EN 50133-2-1 - Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 2-1: Všeobecné požadavky na komponenty

ČSN EN 50133-7 - Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace

15.3 Elektrická požární signalizace (EPS)

ZÁKON č. 133/1985 Sb. o požární ochraně ze dne 17. prosince 1985 - Vytváří podmínky pro ochranu života a zdraví před požáry

VYHLÁŠKA 246/2001 Sb. o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci) ze dne 29. června 2001 (určuje množství, druhy a způsob vybavení prostor a zařízení požárně bezpečnostními zařízeními a jeho provozování)

VYHLÁŠKA 23/2008 o technických podmínkách požární ochrany staveb ze dne 29. ledna 2008, doplněna Vyhláška 286/2011 ze 9/2011 (změny) - Technické podmínky pro navrhování, provádění a užívání staveb

ČSN 730875 - Požární bezpečnost staveb - Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení (norma je určena pro projektanty stupně UP (požárně bezpečnostní řešení – systém jaké funkce, jaké rozhraní s jinými PB systémy)

ČSN 342710 „Elektrická požární signalizace - Projektování, montáž, užívání, provoz, kontrola, servis a údržba k tomu Změna Z1 8/2013 (norma je určena pro projektanty DKPS)

ČSN EN 60332 - Zkoušky elektrických a optických kabelů v podmínkách požáru

IEC 60331 - řada norem definuje celistvost obvodu při požáru

B2ca – Klasifikace dle reakce na oheň CPD 2006/751/EC - označení pro kabel:

- S1 - množství kouře při hoření v rozsahu 1 až 3 (1 = nejméně)
- D1 – možnost odkapávání hořících částeček izolace (1 = malé)

VDE 4102-12 - definuje funkční schopnost celého nosného systému (včetně kabelu)

ZP 27/2008 - zkušební předpis PAVUS pro zkoušky funkční schopnosti

ČSN EN 54-1 - Elektrická požární signalizace - Část 1: Úvod

ČSN EN 54-2 - Elektrická požární signalizace - Část 2: Ústředna

ČSN EN 54-3 - Elektrická požární signalizace - Část 3: Požární poplachová zařízení – Sirény

ČSN EN 54-4 - Elektrická požární signalizace - Část 4: Napájecí zdroj

ČSN EN 54-5 - Elektrická požární signalizace - Část 5: Hlásiče teplot - Bodové hlásiče

ČSN EN 54-7 - Elektrická požární signalizace - Část 7: Hlásiče kouře - Hlásiče bodové využívající rozptýleného světla, vysílaného světla a ionizace

ČSN EN 54-10 - Elektrická požární signalizace - Část 10: Hlásiče plamene - Bodové hlásiče

ČSN EN 54-11 - Elektrická požární signalizace - Část 11: Tlačítkové hlásiče

ČSN EN 54-12 - Elektrická požární signalizace - Část 12: Poplachová a poruchová přenosová zařízení

ČSN EN 54-13 - Elektrická požární signalizace - Část 13: Posouzení kompatibility komponentů systému

ČSN EN 54-16 - Elektrická požární signalizace - Část 16: Ústředny pro hlasová výstražná zařízení

ČSN EN 54-17 - Elektrická požární signalizace - Část 17: Izolátory

ČSN EN 54-18 - Elektrická požární signalizace - Část 18: Vstupní/výstupní zařízení

ČSN EN 54-24 - Elektrická požární signalizace - Část 24: Komponenty pro hlasové výstražné systémy – Reproduktory

15.4 Poplachové systémy – Kombinované a integrované systémy

ČSN CLC/TS 50398 - Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky

16. PODKLADY A SOUVISEJÍCÍ DOKUMENTY

Požadavky na přístupový a zabezpečovací systém na Masarykově univerzitě, verze 2.0, ÚVT MU
Požadavky na bezpečnostní systémy v2.1, OFM SUKB MU
Koncepce řídicího systému budov – BMS MU
Metodika testování zařízení BMS