SPRÁVA UNIVERZITNÍHO
KAMPUSU BOHUNICE
Masarykova univerzita

Metodika
Nasazování a úpravy komponent BMS MU

Oddělení facility managementu
Správa Univerzitního kampusu Bohunice
Masarykova Univerzita

únor 2017
verze 2.0

Obsah

Vysvětlení pojmů a zkratek

AC (Air Conditioning) Klimatizace, proces chlazení a odvlhčování vzduchu.

Aktivní síťový prvek Aktivní síťové prvky jsou ta zařízení, která slouží ke vzájemnému propojení spolu komunikujících zařízení v počítačových sítích. Aktivní síťový prvek aktivně působí na přenášené signály (zesílení) a modifikuje a interpretuje přenášená data. V prostředí technologické sítě MU se jedná o zařízení typu přepínač (switch) a směrovač (router).

Alarm Typ události, který informuje o významném nežádoucím stavu.

Aplikační server Aplikační server je hardware, který zajišťuje některou ze služeb BMS MU.

Aplikační regulátor Regulátor, který odpovídá profilu zařízení BACnet Advanced Application Controller (B-AAC) dle normy BACnet. Je zpravidla využíván pro přímé řízení technologií.

Archivní databáze Archivní databáze slouží k ukládání veškerých provozních dat do jednotné struktury a do společného umístění. Data z archivní databáze lze využívat ke zpětné analýze provozu.

BMS MU (Building Management System Masarykovy univerzity) BMS MU je postupně budovaný integrovaný informační systém určený pro řízení, monitorování a následnou optimalizaci provozu technologií budov MU.

COV (Change Of Value) Metoda vzorkování snímáním hodnoty při změně hodnoty o zadaný práh.

DA (Dieselagregát) Motorgenerátor se spalovacím naftovým motorem – soustrojí složené ze spalovacího motoru a generátoru sloužící jako náhradní zdroj pro zajištění nepřetržité dodávky elektrické energie.

Datový bod Představuje hodnotu – měřené velčiny, žádané hodnoty, stavu vstupu, výstupu apod.

DDC (Direct Digital Control) Přímé číslicové řízení.

Deadband Pásmo necitlivosti.

Distribuovaná technologie Distribuované technologie jsou takové technologie, kde sledování a/nebo ovládání probíhá samostatně pro různé části budovy, typicky pro místnosti. Distribuované technologie využívají Vizualizační obrazovky s půdorysy podlaží nebo tabulkovým zobrazením.

DO Důležité obvody, obvody 2. kategorie důležitosti napájené dieselagregátem

Doplňkový protokol Jako doplňkový protokol lze pro dohled, napojení měřidel, polní instrumentace a rozšíření vstupů a výstupů použít otevřené protokoly (SNMP, Modbus RTU, M-Bus, MP-Bus a LINKnet). Použití doplňkového protokolu je podmíněno obousměrným funkčním převodem na základní protokol a souhlasem Garanta.

DVD Dokumentace pro výběr dodavatele.

Dveře Zahrnují veškeré prvky EKV, tedy zámek (otevírač), čtečku a případně magnetický kontakt, podílející se na funkci přístupového bodu.

EKV (Elektronická kontrola vstupu) Systém pro zajištění omezení vstupu do vybraných prostor, případně sledování pohybu osob. V rámci MU realizován zpravidla prostřednictvím bezkontaktních čteček karet, elektromechanických zámků či dveřních otevíračů, ev. dalších prvků.

EZS (Elektronická zabezpečovací signalizace, Elektronický zabezpečovací systém) Starší termín pro zabezpečovací systém, nahrazeno pojmem PZTS.

Fan-coil Zařízení pro udržení tepelné pohody, obsahující ventilátor (Fan) a výměník (Coil), zpravidla dva, jeden pro chladnou a druhý pro teplou vodu.

FM (Frekvenční měnič) Zařízení pro úpravu frekvence střídavého proudu, užívané pro plynulou regulaci otáček motorů.

FTP (Foiled twisted pair) Kabel s kroucenými páry stíněný celkovou fólií.

Garant investora pro BMS MU (Garant) 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.

Hromadná technologie Hromadné technologie jsou takové, které zajišťují některý z aspektů provozu budovy centralizovaně. Pro ovládání a sledování takových technologií jsou obvykle používány Vizualizační obrazovky s technologickými schématy dané technologie.

Integrační zařízení Integračními zařízeními jsou myšlena taková zařízení, jejichž funkcí je provádět agregaci dat a podobné úlohy, které slouží pro účely vizualizace provozu BMS a pro pohodlné ovládání obsluhou.

Integrovaný přístupový bod Zahrnuje prvky přístupového systému tohoto bodu (čtečka, zámek) a příslušnou zónu PZTS (tedy zónu, která leží za tímto přístupovým bodem).

Investor Investorem se rozumí Masarykova univerzita nebo její součást, která je smluvní stranou dodavatele ve věci realizaci díla, oprav, úprav, reklamací a podobných akcí souvisejících se zásahem do BMS MU.

IRC (Integrated Room Control) Integrovaný regulátor teploty v místnosti.

IS MU (Informační systém Masarykovy univerzity) Pro potřeby přístupového systému vystupuje jako správce identit a cílová destinace pro údaje o průchodech osob skrz přístupové body.

Kalendář Slouží pro nastavení hodnoty datového bodu v závislosti na datu v roce (nejčastěji např. rozlišení pracovní / nepracovní dny).

Kontroler Přejaté podst. jm. z anglického jazyka – Controller; v kontextu tohoto dokumentu synonymum ke slovu Regulátor.

Linkový prvek Prvek zabezpečovacího či přístupového systému, který je připojen na systémovou sběrnici (linku) a zprostředkovává přenos informací mezi ústřednou a periferiemi. U PZTS je zpravidla označen jako expandér či koncentrátor, u EKV řadič snímačů karet, řídící jednotka, dveřní jednotka.

Lokalita Uskupení budov MU, které jsou komunikačně propojeny z jedné hlavní centrální slaboproudé rozvodny, odkud je zajištěn přístup k centrálním datovým službám MU.

MaR Měření a regulace.

Master (Správce) Role (oprávnění) v systému PZTS či EKV, která umožňuje úplné ovládání systému (s případnými výjimkami, je-li zároveň zavedena role Technik).

MDO Méně důležité obvody, obvody s 3. kategorií důležitosti napájení.

Měnič Zařízení, které je součástí UPS za účelem přeměny stejnosměrného napětí na střídavé.

MIB (Tabulka Management Information Base) Databáze v textovém formátu, popisující význam objektů popsaných jednoznačnmh identifikátorem. Hlavní využití v protokolu SNMP.

Modul Viz Linkový prvek.

Notifikace Typ události, který informuje o významném stavu, který však nutně nemusí být nežádoucí (např. zastřežení).

Ostrovní režim Ostrovní režim je zvláštní režim provozu nové instalace, která má být připojena k BMS MU. Nová instalace je na úrovni sítě izolována od BMS MU. V ostrovním režimu jsou k nové instalaci doplněny Webové rozhraní BMS a Archivní databáze, případně další nutné komponenty. V ostrovním režimu je možné otestovat správnou funkci nové instalace. Po vydání souhlasu Garanta je instalace z ostrovního režimu přepojena do BMS MU.

Pasivní síťový prvek Pasivní síťové prvky jsou ty části počítačové sítě, které se podílejí na přenosu dat v síti, ale data žádným způsobem nemění ani neovlivňují. Mezi pasivní síťové prvky patří kabely (UTP, FTP, optické kabely), konektory, zásuvky, propojovací panely a datové rozváděče.

Periferie Prvek zabezpečovacího či přístupového systému, který je koncový a slouží pro snímání stavu (čidlo), signalizaci nebo interakci s uživatelem. V rámci PZTS jde např. o pohybové čidlo, magnetický kontakt, u EKV pak čtečka, zámek,...

PMO Protimrazová ochrana.

Podsystém Viz Zóna.

Polling Metoda vzorkování snímáním hodnoty v pravidelných časových intervalech.

Polní instrumentace Prvky, které jsou v bezprostředním kontaktu s danou technologií a slouží pro snímání a nastavování veličin potřebných pro regulaci. V systémech HVAC se primárně jedná o technologické snímače a spínače (teploty, tlaku, napětí, proudu, atd.), ventily, pohony a frekvenční měniče.

Poznámka ve vizualizační obrazovce Textové pole pro vepsání podrobností o provozním stavu zařízení. Provoz poznámkového systému je v režii Garanta.

Přístupová karta Prvek (token) sloužící k autentizaci uživatele a následné případné autorizaci vstupu do zabezpečeného prostoru. V rámci MU jsou použity zejména studentské karty ISIC, dále zaměstnanecké karty, ITIC, případně karty pro externisty.

Přístupový systém Viz EKV.

Přístupový bod Základní prvek EKV, zpravidla Dveře, případně jiná forma bariéry (turniket, závora, vrata,...). Přístupový bod umožňuje autentizované osobě (tzn. po načtení oprávněné karty) průchod či průjezd. Autentizace a autorizace se řídí daty získanými z IS MU, kam jsou rovněž zasílány informace o průchodech. Může být jednosměrný nebo obousměrný (čtečka z obou stran dveří).

Převodník Převodníkem je myšleno samostatné zařízení, které přijímá zprávy jiného protokolu než BACnet (z jednoho nebo více dalších zařízení) a ty poté překládá na zprávy protokolu BACnet.

Protokol technologické sítě MU Protokol technologické sítě je jakýkoliv protokol, který zajišťuje výměnu zpráv v rámci Technologické sítě MU. Výběr Protokolu technologické sítě MU podléhá schválení Garanta.

Protokol BMS MU Protokol BMS MU je protokol nejvyšší úrovně v dané síti dle abstraktního ISO OSI modelu, na kterém probíhá komunikace mezi Zařízeními BMS MU. Výběr Protokolu BMS MU podléhá schválení Garanta.

Provozní režim Možné strategie provozu technologie (den / noc, chod / stop).

PZTS (Poplachové, zabezpečovací a tísňové systémy) Novější termín nahrazující EZS, explicitně zahrnuje i prvky sloužící pro zajištění bezpečnosti osob, např. tísňová tlačítka.

Řídicí systém Soustava regulátorů, které spolupracují na regulaci technologického procesu.

Regulátor Zařízení, jehož úkolem je udržovat okamžitou hodnotu regulované veličiny na hodnotě žádané. V automatizaci budov také často jako DDC regulátor.

Rozvrh Nastavení hodnoty datového bodu v závislosti na denním čase (nejčastěji např. žádané hodnoty).

SLN Silnoproud.

SNMP modul Rozšiřující karta UPS umožňující převod stavů náhradního zdroje na síťový protokol SNMP.

SNMP (Simple Network Management Protocol) Komunikační protokol určený pro sledování stavu síťových prvků.

Specifický software (specifický SW) Specifický software je veškeré programové vybavení, které bylo vyvíjeno na míru pro Investora a danou instalaci.

Split Klimatizační zařízení, kdy je jednotka s výparníkem (vnitřní) fyzicky a vzdáleností oddělena od jednotky kondenzační (venkovní).

STP (Shielded twisted pair) Kabel s jednotlivě stíněnými kroucenými páry.

Sumární stav Stav, který je odvozen od stavu podřízených elementů. Typicky sumární stav podlaží je odvozen od stavu jednotlivých prvků na tomto podlaží, sumární stav pavilonu pak od sumárních stavů jednotlivých podlaží (a případně prvků společných pro celý pavilon).

Systémový regulátor Regulátor, který odpovídá profilu zařízení `BACnet Building Controller (B-BC)` dle normy BACnet. Je zpravidla využíván ve vyšších patrech topologie řídícího systému.

Technik Role (oprávnění) v systému PZTS či EKV, která je použita v některých systémech PZTS či EKV. Její přihlášení je pak podmíněno povolením prostřednictví role Master, slouží pro zásahy při změně fyzické instalace.

Technologie budov Technologie budov je soubor trvale instalovaných zařízení (Zařízení technologie budov), které se podílejí na provozu budovy, a to buď přímým sledováním, nebo přímým, aktivním a cíleným ovlivňováním dějů ve fyzickém světě. Každé zařízení technologie budov musí být unikátně adresovatelné v některém z používaných protokolů BMS MU.

TeNe MU (Technologická síť MU) Technologická síť MU (TeNe MU) je soustava vzájemně komunikujících Zařízení Technologické sítě včetně zařízení, které tuto komunikaci zprostředkovávají – ty jsou z pohledu systému BMS transparentní. Technologická síť není přímo připojena k internetu (nesmí existovat TCP/IP brána z TeNe MU do veřejné části sítě).

Termoelektrická hlavice Ventil s termoelektrickým pohonem určený především pro montáž na radiátory ÚT nebo rozvody chladu.

Transfer Okamžik kdy dojde ke změně zdroje výstupního napětí UPS: síť-měnič nebo zpět.

Trendlog Trendolog je datová struktura, uchovávající historická data o hodnotách jedné sledované nebo ovládané veličiny v BMS MU.

Událost Zpráva v BMS MU, která slouží k upozornění lidské obsluhy (Uživatelů BMS MU) na změnu do nebo z významného stavu. Zpráva není bezprostředně vyžádaná – nejedná se o zprávu, která by byla odpovědí na zaslaný požadavek. V protokolu BACnet události odpovídají zprávám `(Un)Confirmed Event Notification Service`.

UPS Nepřerušitelný zdroj napájení.

ÚT Ústřední topení.

UTP (Unshielded twisted pair) Nestíněný kabel s kroucenými páry.

Uživatel EKV Osoba vybavená kartou zavedenou v IS MU, která může být v závislosti na konfiguraci v IS MU oprávněna použít přístupový bod (otevřít dveře). Pojem privilegovaný uživatel EKV označuje takového uživatele, který má u konkrétních přístupových bodů vyšší práva, typicky může zpřístupnit místnost odblokováním zámku. Privilegovaný uživatel EKV je vybaven privilegovanou kartou. Neprivilegovaný uživatel EKV pak může vstupovat pouze do odstřežených prostor atp., podrobněji je popsáno v Požadavcích na zabezpečovací a přístupové systémy.

Uživatel budovy Zaměstnanci Investora, kteří využívají budovu jako své pracovní prostředí.

VDO Velmi důležité obvody, obvody s 1. kategorií důležitosti napájení.

Vizualizace Viz Webové rozhraní BMS.

Vizualizační obrazovka Vizualizační obrazovky jsou výhradním prostředkem pro ovládání BMS MU v běžném provozu.

VRV/VRF Variable refrigerant volume/flow - klimatizační jednotka umožnující hospodárnější a efektivnější regulaci chlazení díky použití frekvenčního měniče pro plynulé řízení otáček kompresoru.

Významný stav Stav některého ze zařízení BMS MU nebo zařízení technologie budov, který vyžaduje pozornost od Uživatelů BMS.

VZT Vzduchotechnika.

Webové Rozhraní BMS MU Rozhraní přístupné Uživatelům BMS MU. Jeho hlavní součástí jsou Vizualizační obrazovky.

Zabezpečovací systém Zkrácený zápis pojmu poplachový, zabezpečovací a tísňový systém.

Základní komunikační protokol Základním protokolem je definován normou ČSN EN ISO 16484-5 dále jako BACnet. Možné jsou jeho další implementace (IP – UDP/IP, Ethernet a MS/TP (485)).

Zařízení technologické sítě MU Zařízení technologické sítě zajišťují komunikaci v rámci BMS MU, a to buď jako vysílač, přijímač, nebo mezilehlý prvek. Každé zařízení TeNe MU musí být unikátně adresovatelné v některém z používaných protokolů technologické sítě. Každý prvek, podílející se na komunikaci v Technologické síti MU, musí být zařízením technologické sítě MU a používat některý z povolených protokolů technologické sítě MU.

Zařízení BMS MU Zařízení BMS MU je takový prvek BMS MU, který se jakkoliv podílí na řízení a monitorování provozu technologií budov MU.

1 Úvod

Metodika Nasazování a úpravy komponent BMS MU (dále jen Metodika) definuje požadavky a pravidla pro realizaci jakýchkoliv změn, úprav, doplnění a jiných zásahů (dále jen akcí) do BMS MU. Tato Metodika je závazným podkladem pro projektování a realizaci všech akcí, které mají nebo mohou mít jakýkoliv dopad na BMS MU. Metodika je vždy součástí smluvních podmínek či objednávky realizace akcí souvisejících s BMS MU. V případě sporu jakékoliv části dokumentace, smluvních podmínek či objednávky předmětné akce má Metodika vždy přednost před zmíněnými dokumenty.

Případné výjimky z v této Metodice uvedených požadavků a pravidel je možné povolit pouze na základě výslovného souhlasu Garanta s těmito výjimkami.

1.1 Obsah dokumentu

Jednotlivé kapitoly Metodiky popisují způsob připojení a integrace jednotlivých technologií budov do BMS MU. Společné požadavky na integraci a připojení všech technologií jsou popsány v kapitolách 2 a 4. V případě, že technologie budovy, která se v rámci akce doplňuje, opravuje či upravuje, není v Metodice explicitně zmiňována, je třeba se řídit především společnými požadavky a vyžádat si u Garanta informace a podmínky, jak technologii do BMS MU integrovat.

1.2 Obecné podmínky realizace akce

Následující seznam obsahuje hlavní zásady, které jsou dále podrobněji vysvětleny v dalších částech tohoto dokumentu.

- Do BMS MU jsou integrovány všechny technologie budov, pokud Investor či Garant neurčí jinak;
- Základním komunikačním protokolem BMS MU je protokol BACnet (ČSN EN ISO 16484-5). Další možné komunikační protokoly jsou případně uvedeny v kapitolách popisujících integraci jednotlivých technologií budov do BMS MU;
- Z důvodu optimalizace budoucích provozních nákladů Investor požaduje dodávku a nasazení výrobků Delta Controls Inc. všude tam, kde je to možné a ekonomické;
- Předpokladem dodávky a nasazení zařízení BMS MU je jejich schválení Garantem. Garant si vyhrazuje právo požadovat úspěšné otestování kompatibility zařízení s BMS MU a s BACnet dle **Metodiky Testování zařízení pro BMS MU**;
- Součástí dodávky akce jsou i komentované zdrojové kódy aplikačních programů vytvořených či upravených pro potřebu akce;
- Součástí dodávky akce jsou i programy s časově neomezenou licencí k užití potřebné pro konfiguraci dodávaných zařízení BMS MU;

- Dodavatel musí respektovat jmennou konvenci BMS MU 2.12;
- Připojení dodávaných zařízení BMS MU do technologické sítě může být provedeno až po vydání výslovného souhlasu Garanta a při respektování podmínek **Metodiky Připojování nových zařízení do BMS MU** (Příloha B).

1.3 Obecný postup realizace akce

Obecný postup při realizaci jakékoliv akce, která má vliv na BMS MU, je popsán v následujícím textu. Tento postup může být doplněn či upraven na základě požadavků Investora či Garanta.

1. Vyhotovení příslušné dokumentace (prováděcí, realizační či obdobné) dodavatelem, požadavky na dokumentaci viz 2.17;
2. Případné opravy a doplňky dokumentace na základě požadavků Investora a Garanta;
3. Schválení dokumentace Investorem a Garantem;
4. Předložení seznamu zařízení, která budou v rámci akce připojena do BMS MU;
5. Výběr zařízení, která musí projít Testováním. Zařízení, která je nutno otestovat, stanovuje Garant;
6. Testování zařízení dle **Metodiky Testování zařízení pro BMS MU** (Příloha A) v Laboratoři OFM SUKB za přítomnosti dodavatele. Testování každého zařízení je možno opakovat maximálně 2x. Úspěšné otestování všech zařízení BMS MU je nutným předpokladem realizace akce. Viz také 2.7;
7. Provedení instalace zařízení BMS MU v ostrovním režimu, tedy bez připojení do technologické sítě BMS MU;
8. Otestování funkcionality v ostrovním režimu;
9. Vyžádání stanoviska Garanta k možnému připojení zařízení do BMS MU v souladu se splněním podmínek uvedených v **Metodice Připojování nových zařízení do BMS MU** (Příloha B);
10. Připojení zařízení do BMS MU na základě kladného stanoviska Garanta;
11. Realizace bezchybného ověřovacího provozu v délce minimálně 14 po sobě jdoucích kalendářních dní;
12. Vyhotovení dokumentace skutečného provedení za splnění podmínek na dokumentaci, uvedených v dalších částech tohoto dokumentu;
13. Případné opravy a doplňky dokumentace na základě požadavků Investora a Garanta;
14. Schválení dokumentace Investorem a Garantem.

2 Infrastruktura BMS

Pojmem Building Management System (BMS) označujeme prostředí (ve smyslu souboru software, hardware a síťové infrastruktury), které zajišťuje integraci a spolupráci jednotlivých systémů zajišťujících *provoz budovy* – tzv. *technologií budovy*. BMS sjednocuje jednotlivé autonomní technologie tak, že se z pohledu uživatelů jedná o jeden provázaný celek.

BMS MU tohoto cíle dosahuje poskytováním několika základních služeb. Jedná se zejména o:

- **Sledování a ovládání stavu zařízení** – Zajišťuje komunikaci se systémem v reálném čase, zobrazuje aktuální provozní data z budovy a zajišťuje předávání povelů od obsluhy dotčeným zařízením;
- **Alarming** – BMS MU aktivně upozorňuje obsluhu na výskyt definovaných událostí - poruch, překročení prahových hodnot u sledovaných veličin v prostředí budovy (např. teploty v místnosti) apod.;
- **Archivace** – Ukládání dat do společné *archivní databáze*.

V rámci BMS MU jsou integrovány **všechny systémy technologií budov**, zejména:

- Systém měření a regulace (MaR);
- Ovládání osvětlení;
- Monitoring výtahů;
- Odečty energií;
- Přístupový systém/Elektronická kontrola vstupu (EKV);
- Poplachový zabezpečovací a tísňový systém (PZTS);
- Elektronická požární signalizace;
- Kamerový systém (CCTV);
- Sledování stavu napájení (jističe, UPS).

V prostředí MU tedy obecně musí být každá technologie budovy sledována a ovládána pomocí BMS MU. Výjimky musí být odsouhlaseny Garantem. Zároveň může Investor, Garant nebo Uživatel budovy požadovat integraci dalších technologií, které nespadají pod definici technologií budovy.

Ke svému chodu BMS MU využívá tzv. *Technologickou síť MU* (**TeNe MU**). Jedná se o infrastrukturu **oddělenou** od standardní (tzv. akademické) datové sítě připojené do internetu (dále viz kapitola 4). Zařízení TeNe MU jsou v naprosté většině případů od internetového provozu **oddělena** – neexistuje síťová cesta umožňující zařízením komunikovat vně technologické sítě. Jedinými výjimkami jsou **aplikační servery**, umožňující ovládání a sledování BMS, které samozřejmě musí být dostupné ze stanic uživatelů,

které nejsou součástí TeNe MU. Případná další omezení (např. pouze pro přístup z počítačů v síti MU, nikoliv odkudkoliv z internetu) jsou řešena pomocí firewallu v akademické síti. Vyčlenění BMS MU do samostatné sítě jednak zjednodušuje správu a konfiguraci zařízení zajišťujících provoz budovy, a jednak zvyšuje odolnost vůči bezpečnostním rizikům.

Přestože jsou všechna zařízení zapojena do sítě, jsou zároveň v co největší míře **autonomní**. BMS MU slouží ke vzdálenému sledování stavu zařízení a vzdálenému vydávání povelů, neslouží ale k zajištění základních funkcí technologie budov. Jednotlivá zařízení budově musí být v co největší míře schopna autonomního fungování i při výpadku komunikace s ostatními částmi systému (např. je požadováno, aby byl regulátor byl schopný řídit běh systému HVAC samostatně i po odpojení ze sítě – nedochází k přenosu nutných dat mezi zařízeními BMS MU. Stejně tak bezpečnostní systémy musí zůstat plně funkční i při výpadku komunikace ústředny s ostatními prvky v BMS MU).

2.1 Softwarové standardy aplikací v prostředí BMS MU

Veškeré současné aplikace splňují určité funkční a nefunkční[1] požadavky. V případě **náhrady stávajícího řešení nebo dodávky nové aplikace** pro ovládání a správu BMS MU je nutné tyto požadavky také dodržet. Jedná se o následující požadavky:

- **Údržbu, úpravu a rozšiřovaní** aplikací (např. vývojové prostředí pro vytváření vizualizačních obrazovek) **bez omezení** počtem datových bodů, času nebo uživatelů aplikace, a to včetně všech potřebných knihoven a potřebného počtu a verzí licencí;
- **Provoz** aplikací (BMS) **bez omezení** počtem datových bodů, času nebo uživatelů aplikace. Aplikace musí být dostupná jak v prostředí pracovní stanice, tak i jako web aplikace provozována na webserveru;
- **Uživatelský přístup** k aplikacím **bez licenčního omezení** počtu současných uživatelů
- Aplikace musí umožňovat **směrování alarmů** dle zadání (dle typu alarmu, role, uživatele, času, na žádost. . .);
- **Ukládání provozních dat** dle zadání do databáze;
- **Českou** lokalizaci;
- **Logování** událostí (uživatelských akcí);
- **Autentizaci a autorizaci** s napojením na centrální **systém MU** (s použitím identit používaných na MU);
- Výhradně **šifrovanou komunikaci** mezi webovým rozhraním BMS MU a klientskými stanicemi uživatelů;
- Zobrazení sledovaných a řízených prvků technologií v **půdorysech** skutečného stavu;

[1] Jedná se např. o výkon, škálovatelnost, spolehlivost, rozšiřitelnost, udržitelnost, spravovatelnost, nebo bezpečnost.

- Výhradně **šifrovanou komunikaci** pro případný vzdálený přístup do interního prostředí technologické sítě;
- Připojení do **domény** BMS MU v případě, že je řešení postaveno na MS Windows.

2.2 Hardwarové standardy aplikačních serverů v prostředí BMS MU

V síti BMS MU fungují různé aplikační servery. Aplikační server definujeme jako zařízení, které splňuje všechny následující podmínky:

- Zajišťuje běh některé ze **služeb BMS MU**;
- Jedná se o **samostatné zařízení** (vlastní napájecí zdroj, skříň, možnost připojení periferií pro ovládání);
- Komunikuje prostřednictvím počítačové sítě;
- Obsahuje procesor s architekturou **x86-64** (příp. x86);
- Umožňuje instalaci standardního operačního systému **Windows/Linux**.

Každý nově dodaný aplikační server musí splňovat následující parametry:

- Montáž do **rozvaděče** (rack mount);
- **Serverový OS** v aktuální stabilní verzi (Windows Server, Debian);
- Redundantní **napájecí zdroj**;
- Redundantní úložiště zapojené v **RAID1**;
- Karta pro **vzdálenou správu**;
- Komponenty se sníženou spotřebou (**TDP** na jeden procesor max. **90W**).

Konkrétní specifikace (např. na počty procesorů, velikost operační paměti apod.) budou upřesněny v projektové dokumentaci dle požadavků Investora a po schválení Garantem.

V případě, že dodavatel zajišťuje i montáž aplikačního serveru, je povinen zajistit připojení obou jeho napájecích zdrojů dle kapitoly 5.2.2. Pokud takové připojení není možné, je povinnen informovat o této skutečnosti Garanta.

2.3 Redundance v BMS MU

U komponent, kde je takové řešení možné, je Investorem vyžadovováno takové řešení, které je proti výpadku jedné z komponent chráneno redundancí. V BMS MU je využíváno několik typů redundance:

1. **Redundance napájení** – zařízení vybavena dvěma nezávislými zdroji, připojenými do dvou nezávislých okruhů dle kapitoly 5.2.2;

2. **Redundance síťového připojení** – zařízení jsou vybavena nezávislými síťovými kartami, připojenými do BMS MU přes dvě nezávislé síťové cesty;
3. **Redundance úložiště** – pevné disky jsou provozovány v režimu RAID 1;
4. **Redundance řadiče** – V případě diskových polí je nutné, aby byla vybavena dvěma nezávislými diskovými řadiči;
5. **Redundance zařízení** – Je připraveno identické záložní zařízení pro případ výpadku primárního. Pokud je tento typ redundance požadován, je to explicitně stanoveno v zadávací dokumentaci nebo v této metodice.

Požadavky na redundanci se týkají aplikačních serverů, diskových polí, softwarových převodníků, a dalších specializovaných komponent, které použití redundance typu 1 – 4 umožňují. Redundance typu 5 je vyžadována u obzvláště důležitých zařízení, jejichž správná funkce je kritická pro fungování BMS MU.

2.4 Komunikační protokoly

Masarykova univerzita využívá BMS integrovaný na úrovni komunikačního protokolu **BACnet (ČSN EN ISO 16484-5)**. V systému neexistuje jasně definovaný centrální prvek. Aplikace pro uživatele BMS MU (dispečink, archivní databáze – viz dále) podporují komunikaci pouze pomocí integračního protokolu BACnet a se všemi zařízeními BMS MU tedy komunikují stejným způsobem. Je tedy nutné, aby všechna zařízení BMS MU umožňovala komunikaci pomocí společného protokolu BACnet. Může se jednat buď o nativní podporu protokolu, nebo o využití příslušného překladače. Díky tomu při připojení nových zařízení není nutné zasahovat do existujících aplikací, změny probíhají pouze na úrovni konfigurace.

Nově připojovaná zařízení BMS MU musí podporovat komunikaci přes **BACnet/IP** nebo **BACnet/MS-TP (RS-485)** případně musí být dodána s příslušným převodníkem na jeden z těchto protokolů. Dodatečné požadavky na použité komunikační protokoly jsou u některých technologií dále specifikovány v příslušných částech Metodiky. Použité komunikační protokoly a adresace prvků musí být vyznačeny v topologickém schématu technologické sítě.

Každé zařízení, které ovládá či sleduje technologie budov skrze své vstupy a výstupy, musí být schopno komunikovat prostřednictvím protokolu **BACnet**, nebo musí být vybaveno **dedikovaným** převodníkem (k jednomu zařízení náleží jeden převodník).

2.5 Kompatibilita s existujícími aplikacemi v prostředí BMS MU

Aplikacemi v prostředí BMS MU jsou myšleny nástroje, které využívají koncoví uživatelé a administrátoři pro sledování, ovládání a analýzu provozu budovy a správu samotného BMS MU. Tím jsou myšleny zejména:

- Delta Controls **ORCAWeb** 3.40 R3 – Webové rozhraní BMS MU.
- Delta Controls **Historian** 3.40 R3 – Server pro ukládání dat do archivní databáze.
- Delta Controls **ORCAView** 3.40 R3 – Aplikace pro správu a konfiguraci systému.

Nově připojované zařízení BMS MU musí být kompatibilní s výše uvedenými aplikacemi v rozsahu popsaném **Metodikou Testování zařízení pro BMS MU** (Příloha A).

V případě, že pro ukládání dat bude použito jiné řešení než ukládání do stávající *archivní databáze* aplikace Historian, je dodavatel povinen zajistit:

- Zobrazení historických dat v prostředí aplikace ORCAWeb;
- Přístup k datům pro externí aplikace (např. SQL konektor, JSON, XML).

2.6 Distribuované integrační komponenty

Integračními zařízeními jsou myšlena taková zařízení, jejichž funkcí je provádět agregaci dat a podobné úlohy, které slouží pro účely vizualizace provozu BMS MU a pro pohodlné ovládání obsluhou. Jedná se zejména o:

- **Sumarizaci stavů** – algoritmus, který z množiny stavů určuje stav nadřazené komponenty (např. zkoumá, jestli je některé z čidel na daném podlaží v chybovém stavu a pokud ano, vyhlásí chybu pro celé podlaží). Sumarizace je používána pro propagaci chybových stavů (viz část 3.7);
- **Ukládání historických dat** – Některá zařízení nejsou schopna ukládat historická data do objektů typu TrendLog, v takovém případě jsou data ukládána na jiném zařízení, se kterým komunikuje po síti;
- **Konfigurace časových plánů a kalendářů** – Některá zařízení nejsou schopna časového plánování pomocí objektů typu Schedule a Calendar, v takovém případě jsou rozvrhy ukládány na jiném zařízení, se kterým komunikuje po síti;
- **Vizualizace dat** – vytváření objektů MultiTrend pro sledování více veličin současně.

Pokud jsou tyto nebo jiné úkoly realizovány pomocí objektů protokolu BACnet (Schedule, Calendar, MultiTrend, Analog/Binary/Multistate Variable), nemohou být tyto objekty vytvořeny na PC nebo serveru, je třeba využít **zařízení s nativní podporou protokolu BACnet**. **Standardem** pro integrační komponenty systému BMS MU je zařízení **Delta Controls eBCON**, případně **Delta Controls eBMGR**.

2.7 Testovací procedura

Vzhledem k tomu, že implementace protokolu BACnet se u různých výrobců může lišit (např. nemusí být úplná), dodavatel musí doložit možnost spolupráce zařízení různých výrobců, např. pomocí prohlášení výrobce **PICS** (Protocol Implementation Conformance Statement).

Zároveň je dodavatel povinen vyžádat si pro každé zařízení BMS MU, které plánuje použít, stanovisko od Garanta. Garant v tomto stanovisku sdělí, jestli je vyžadováno, aby prošlo **testováním** v laboratoři BMS MU s **kladným výsledkem** podle **Metodiky Testování zařízení pro BMS MU** (Příloha A). Zařízením je pro účely Testování myšlena konkrétní kombinace hardware a jeho programového vybavení (firmware, software). Ja u HW, tak u SW je nutné rozlišovat různé verze či revize. Garant si vyhrazuje

právo požadovat nové testování pro zařízení, u kterého došlo ke změně HW revize nebo ke změně verze SW vybavení.

Smyslem testování je ověřit jednak tvrzení výrobce v PICS, vhodnost pro daný účel, a jednak důkladně ověřit kompatibilitu s existujícími aplikacemi a prostředím BMS MU.

Testovací procedura ověřuje zejména následující vlastnosti a funkce:

- Směrování, filtrování a konfigurace **alarmů** a notifikací;
- Možnosti **přenosu dat** v síti (COV Subscription atd.);
- Schopnost **ukládání dat** (Trendlog), možnosti konfigurace (COV/Polling) a spolupráce se serverem Historian (Notifikace o nutnosti stáhnout data);
- Korektní práce s tzv. Status flags a správná indikace **manuálního režimu**;
- Dostačující **odezva** na změny stavů (konkrétní požadovaná reakční doba je závislá na konkrétním použití – je tím myšlena taková odezva, která nezpůsobuje komplikace při provozu).

V případě, že zařízení nesplní požadavky testování a neobdrží od Garanta souhlas, je možné podstoupit nejvýše **dvě** další **opravná** testování.

2.8 Požadavky na fyzickou instalaci prvků BMS

Zařízení a další komponenty v BMS MU musejí být nainstalovány způsobem, který umožňuje jejich dlouhodobý spolehlivý provoz, efektivní údržbu a další rozšiřování systému BMS.

Servery (počítače, u kterých není fyzicky přítomna po celou dobu používání lidská obsluha) musejí být dodány v provedení **rack mount** a nainstalovány v rozvaděči („racku“).

Zařízení určená k montáži **na zeď** (ústředny, převodníky…) musí být umístěny ve **slaboproudých rozvodnách**, pokud není zadavatelem stanoveno jinak.

Regulátory, PLC a další zařízení určená k montáži do rozvaděčových skříní musejí být instalována podle požadavků stanovených v části 6.3.2.

2.9 Připojování nových zařízení do BMS

Připojování nových zařízení do BMS musí probíhat s vědomím a ve spolupráci s Garantem. Pokud Garant požaduje testování, musí zařízení projít testováním podle **Metodiky Testování zařízení pro BMS MU** (Příloha A) před připojením do BMS MU. Při samotném připojování zařízení do BMS MU je třeba dodržet **Metodiku Připojování nových zařízení do BMS MU** (Příloha B). Dodavatel je povinen nejdříve instalaci provozovat v tzv. **ostrovním režimu**, kdy je nejdříve plně otestována funkčnost celé instalace. Po otestování funkčnosti si dodavatel vyžádá písemný souhlas Garanta s připojením a následně je celá instalace najednou připojena k BMS MU za přítomnosti zástupců dodavatele i Garanta.

2.10 Použití převodníků na protokol BACnet

Pro připojování podsystémů do BMS MU lze použít převodník (překladač, bránu, gateway) v případech, že daný podsystém nepodporuje nativně komunikaci přes BACnet. Poměrně běžná jsou zařízení, u kterých je funkce převodníku pouze jednou ze služeb, kterou poskytují. Příklady takových zařízení:

- Regulátor systému MaR na BACnet/IP, který sice plní i svou roli v systému MaR, zároveň jsou přes něj ale připojena zařízení podporující protokol Modbus;
- Ústředna systému PZTS, která obsahuje převodník na BACnet buď jako součást programové výbavy, nebo jako rozšiřující modul (i přes to, že samotný rozšiřující modul nepřijímá zprávy fyzicky přes síť, ale přes rozšiřující rozhraní ústředny, stále překládá na BACnet zprávy od čidel/linkových modulů/koncentrátorů a dalších prvků, které jsou distribuovány po budově).

Maximální přípustná **odezva** převodníku na přijetí signálu musí garantovat požadovanou funkčnost připojovaných technologií. Přednostně je požadován převodník hardwarového provedení od stejného výrobce jako technologie připojovaná do nadřazeného systému BMS MU (viz dále).

Pokud převodník umožňuje **vzdálený přístup** (SSH, RDP…), musí být funkční a přístupové údaje musí být součástí dokumentace díla.

2.10.1 Softwarový převodník

Za softwarový převodník považujeme zařízení, které splňuje **všechny** následující charakteristiky:

- Zařízení se skládá z **oddělitelné** softwarové a hardwarové části.
- Hardwarová část je složena z uživatelsky **vyměnitelných komponent** jako např. procesor v patici, grafická karta nebo operační paměti ve standardizovaných slotech.[2]
- Převodník využívá veřejně dostupný **operační systém** (jedná se zejména o neupravované verze OS Windows nebo OS založené na Linuxu).
- Softwarová část je schopná **běhu na libovolném HW** různých výrobců, splňujícím určité požadavky (zejména na typ I/O portů), není tedy pevně svázána s dodaným HW řešením a nemusí s ním být dodávána společně.
- Převodník umožňuje instalaci dalšího softwaru.
- Převodník není fyzickou součástí jiného zařízení (např. ústředny, regulátoru).

Volněji řečeno, za SW převodník považujeme takové řešení, které se skládá z aplikace, běžící na běžném operačním systému, který je **nainstalovaný na PC** standardu ATX/microATX nebo serveru s procesorovou architekturou x86-64 nebo x86.

Softwarové převodníky **nelze použít** mezi různými protokoly pro **měření a regulaci** (BACnet/M-Bus, BACnet/Modbus…). Jsou akceptovatelné jako integrační prvky dalších technologií (PZTS, EKV, EPS). Použití softwarového převodníku podléhá písemnému schválení ze strany Garanta.

Požadavky na softwarový převodník:

[2] Rozhodující je technologické kritérium. I když záruční podmínky daného zařízení uživatelské zásahy zakazují, stále se jedná o uživatelsky vyměnitelné komponenty.

- Musí splňovat požadavky na **aplikační server** v BMS MU (viz část 2.2).
- **Záložní převodník** s identickou konfigurací (SW i HW) připravený k nasazení v případě výpadku primárního převodníku.
- Převodníky postavené na Windows musí být připojeny do **domény**.
- SW část převodníku musí fungovat bez nutnosti stále přihlášeného uživatele (tzn. jako **služba**/démon).
- SW část musí být schopna **automatického startu** např. po restartu z důvodu aktualizací.
- K SW části musí být součástí dodávky **dokumentace**, obsahující:
  - Instalační soubory;
  - Instalační postup + licenční klíče apod.;
  - Zálohu konfiguračních souborů;
  - Popis možností konfigurace.

Alternativně je možné místo aplikačního serveru použít **průmyslové PC** (odolnost proti prachu a vibracím, nejlépe pasivní chlazení). V takovém případě není požadována karta pro vzdálenou správu, RAID 1 a redundantní napájení. Konkrétní dodaný HW podléhá schválení Garanta v okamžiku podání nabídky.

Dále je možné realizovat SW převodník jako **virtuální server**. V takovém případě je však nutné zajistit vysokou dostupnost GW při provozování v rámci loadbalancing clusteru tak, aby byla GW funkční bez ohledu na to, na kterém uzlu clusteru je právě spuštěna, a aby byla schopna automatické obnovy po výpadku nebo po migraci mezi uzly. Realizace virtuální GW podléhá schválení ve chvíli podání nabídky a podmínkou tohoto řešení je to, že jsou k dispozici kapacity pro umístění dalších virtuálních serverů.

2.10.2 Hardwarový převodník

Za hardwarový převodník je považován každý převodník, který nespadá do kategorie softwarových převodníků.

Součástí dodávky hardwarového převodníku musí být **servisní příslušenství** (např. propojovací kabely, konfigurační software, nestandardní redukce) a kompletní **dokumentace** včetně popisu konfigurace a zapojení.

2.11 Časová synchronizace v BMS MU

Časová synchronizace v distribuovaném systému je klíčová pro sledování provozu budovy a zejména pro zpětné dohledávání času výskytu důležitých událostí. Časové značky jsou součástí alarmových zpráv a notifikací i historických dat. Proto je nezbytné, aby každé zařízení, které nějakým způsobem pracuje s časovými razítky (zejména se jedná o regulátory s objekty TrendLog, Schedule, Calendar, Event Enrollment a dalšími podobnými, převodníky a aplikační servery), podporovalo **časovou synchronizaci** buď pomocí protokolu **NTP**, nebo protokolu **BACnet** (musí být schopno přijímat pokyny k časové synchronizaci od dalších zařízení v BMS MU a korigovat na jejich základě své hodiny).

2.12 Jmenná konvence datových bodů

Veškeré objekty, viditelné prostřednictvím protokolu BACnet, musejí mít **názvy** (BACnet property Name) ve tvaru, který splňuje tzv. Jmennou konvenci BMS MU.

Název objektu se skládá z následujících položek (v tomto pořadí):

1. Poloha;
2. Technologie;
3. Typ objektu;
4. Zařízení;
5. Upřesnění.

Platí tato pravidla:

- Název se skládá z povinné Polohy a minimálně jedné další položky z výše uvedeného seznamu;
- Pořadí položek je neměnné, tedy první musí být uvedena Poloha, dále Technologie (je-li použito), Typ objektu, Zařízení a Upřesnění;
- Pro oddělení položek v rámci názvu se používá znak podtržítko (_), který lze použít pouze k tomuto účelu a pro potřeby indexování (viz níže);
- Prvky položek Technologie, Typ objektu, Zařízení a Upřesnění jsou dány číselníkem, který poskytuje Garant, a jsou zcela unikátní v rámci prvků všech položek;
- Položky Poloha, Technologie, Typ objektu a Zařízení se v rámci jednoho názvu mohou vyskytovat pouze jednou;
- Položka Upřesnění se může vyskytovat opakovaně;
- Za položkami Technologie, Zařízení a Upřesnění se může vyskytovat alfanumerický index oddělený podtržítkem, který označuje konkrétní věc – místnost (102, 1S05), podlaží (2NP, 4NP), rozvaděč (17RDC001), větev vzduchotechniky (A, B, C…). Index následuje bezprostředně za položkou, kterou popisuje (Pro VZT s číslem 1 a jedním odtahovým ventilátorem takto: VZT_1_Odtah, ne VZT_Odtah_1).

Význam jednotlivých položek je následující:

- **Poloha** – Tvoří unikátní identifikaci budovy. Je tvořena částí polohového kódu popisující lokalitu a budovu – tedy např. pro budovu ESF na Lipové je to `BPA11`.
- **Technologie** – Popisuje začlenění objektu do významných technologických celků z hlediska provozu budovy. Tvoří podrobnější rozčlenění než MaR/silnoproud/slaboproud – např. `BVS`, `Zaluzie`, `ZCH`….
- **Typ objektu** – Vychází z typování objektů podle protokolu BACnet, jde o zkratku anglického označení – např. `AV` znamená Analog Variable, tedy analogová proměnná, `TL` znamená TrendLog atp.

- **Zařízení** – Upřesňuje druh zařízení, ke kterému se objekt vztahuje – `Cerp` čerpadlo, `Dig` digestoř, `Mix` ventil. . . .
- **Upřesnění** – Používá se v případě, že je třeba dále specifikovat účel daného objektu - typicky `Chod`, `Porucha`, `Rychlost`, `Vykon`.

2.12.1 Rozsah působnosti konvence

Jmenná konvence se týká následujících druhů objektů:

- Objekty vstupů a výstupů: AI, BI, MI, AO, BO, MO;
- Proměnné: AV, BV, MV;
- Trendlogy: TL;
- Události: EV;
- Rozvrhy: SCH;
- Kalendáře: CAL;
- Totalizéry: AT, BT;
- Kontrolní smyčky: CO.

Další druhy objektů budou pojmenovány po koordinaci s Garantem. Rovněž případné nedodržení této konvence je třeba schválit Garantem (může jít např. o případy systémových objektů, jejichž názvy nelze změnit). Aktuální Číselník jednotlivých položek je udržován Garantem a je poskytnut na vyžádání. Garant rovněž shromažďuje návrhy na úpravy/doplnění Číselníku.

2.12.2 Příklady

Pro názornost je zde uvedeno několik příkladů názvů dle jmenné konvence:

- `BHA06_BVS_TL_Tlak_Primar_Privod` – Trendlog na tlaku páry na přívodu primárního okruhu systému BVS v budově UKB-A5.
- `BHA12_UT_AI_T_Vetev_Zapad` – Měření teploty ÚT západní větve objektu UKB-A11.
- `BHA42_VZT_1_AO_Mix_Teplo` – Ovládání ventilu na topné části první (VZT_1) vzduchotechniky objektu UKB-Z.
- `BHA20_ZCH_BV_Cerp_Sekundar_Zapni` – Proměnná sloužící k zapnutí čerpadla na sekundárním okruhu zdroje chladu objektu UKB-A19.

2.13 Ukládání archivních dat (Trendování)

Všechna zařízení zapojená v BMS MU musí být schopna ukládat **historii** svých provozních stavů a hodnot veličin. Ukládání těchto historických dat označujeme jako trendování.

Pro trendování jsou vytvořeny speciální objekty označované jako **trendlogy** (TL). Ty jsou obvykle vytvořeny přímo na zařízení, kde se provádí sledování příslušných veličin. Každý trendlog je schopen sbírat a ukládat data z jednoho datového bodu.

V BMS MU je nutné ukládat historii **všech měřených veličin (vstupů) a výstupů**. U objektů typu proměnná specifikuje požadavky na trendování Garant a Investor. Výjimky z tohoto pravidla podléhají schválení Garanta.

K ukládání dat pomocí trendlogů je možné přistupovat dvěma způsoby. První možností, jak ukládat data, je v **pravidelných časových intervalech**, kdy se záznam vytvoří např. každou hodinu. Pro tento způsob trendování se používá název **polling**. Polling umožňuje jednoduché nastavení počtu záznamů za časový úsek a snadné stanovení velikosti paměti trendlogu. Výhodou této metody je pravidelný sběr dat, který probíhá podle předem daného nastavení. Pokud dojde na zařízení k problémům s komunikací, je snadné rozpoznat výpadek trendování. Nevýhodou trendování pomocí metody polling jsou chybějící extrémní hodnoty. Pokud se tyto hodnoty nebudou vyskytovat právě v době měření, tak nebudou zaznamenány a uloženy pro pozdější analýzu. Metoda polling je výhodná v situaci, kdy je třeba zaznamenat hodnoty po určitých časových úsecích. Metoda polling se v BMS MU používá pouze v odůvodněných případech kvůli vysoké náročnosti na komunikaci. Je možné ji použít po písemném schválení Garantem.

Druhou možností ukládaní dat je metoda **COV** (Change of value). Tato metoda se preferuje z důvodu nižší náročnosti na regulátory, komunikaci a menší množství uložených dat. Data se ukládají vždy po změně hodnoty o předem nastavený krok. Touto metodou se snadno zaznamenají extrémní hodnoty, čímž je odstraněna nevýhoda metody polling. Nevýhodou COV je nemožnost kontroly pravidelného nárůstu dat a tím pádem není možné rozpoznat výpadek v trendování.

Objekt TL má omezenou kapacitu záznamů, pokud je vytvořen např. v regulátoru. Proto BMS MU obsahuje **archivní databázi**, která umožňuje uchovávat historii provozních stavů bez omezení kapacitou paměti. Obecně platí, že veškeré objekty Trendlog, definované na zařízeních BMS MU, musí být zároveň ukládány i do archivní databáze. Výjimky z tohoto pravidla jsou možné pouze po schválení Garantem.

2.14 Události v BMS MU

BMS MU rozlišuje dva základní typy událostí podle definice v protokolu BACnet – `Alarm` a `Notification` (dále Notifikace). Alarmy a notifikace v BMS MU slouží k upozornění obsluhy na nežádoucí nebo jinak významné stavy zařízení a technologií v BMS MU. Zatímco Alarm značí nežádoucí stav, notifikace označuje stav nějak významný. Pro události v BMS MU obecně platí několik zásad (splnění některých z nich je ověřováno testovací procedurou podle **Metodiky Testování zařízení pro BMS MU**):

- Události musí být korektně zobrazovány v seznamu alarmů v aplikaci OrcaWeb (název objektu, název alarmu, alarmový text, čas události);
- Události musí být možné **deaktivovat a měnit typ** (Notification/Alarm – zejména u PTZS a EPS);
- Události musí být možné přiřadit do libovolné **Notification class**;

- V případě potvrzovaných událostí musí být možné ji **potvrdit** z aplikace Orcaweb.

Další požadavky na alarmy (které hodnoty na sebe mají mít navázány alarmy atd.) jsou uvedeny v částech Metodiky věnovaných jednotlivým technologiím. Další požadované alarmy definují uživatelé budov a místností před zahájením realizace.

2.15 Vizualizační obrazovky

Při připojení nových zařízení komunikujících protokolem BACnet do BMS MU je vždy nutné vytvořit nové (a/nebo upravit stávající) **vizualizační obrazovky** pro software **ORCAView** a **ORCAWeb**. Obecné požadavky na funkci a strukturu vizualizačních obrazovek jsou uvedeny v části 3 (Uživatelské prostředí BMS MU). Konkrétní standardy pro vizualizační obrazovky různých technologií jsou popsány v příslušných částech Metodiky.

2.15.1 Úpravy obrazovek

Nové obrazovky (stejně jako úpravy existujících) jsou předávány Garantovi ve formě **zdrojových souborů GPC**. Soubory jsou předány nahráním do systému **SVN** a vytvořením požadavku na překlad v systému Trac. Přesný postup je popsán v **Metodice Správa vizualizačních obrazovek BMS MU** (Příloha C).

Předáním obrazovek zároveň dodavatel souhlasí s tím, že Garant může v obrazovkách provádět samostatně úpravy (v době záruky pouze po předchozím nahlášení a schválení úprav dodavatelem).

2.16 Software a data pro správu systému

Investor si vyhrazuje právo provádět vlastními silami kompletní správu systému po skončení záruky na dílo. V době trvající záruky jsou povolené servisní zásahy ze strany Investora předmětem domluvy s dodavatelem.

Správou systému jsou myšleny zejména následující úkony:

- Obnovení SW vybavení ze zálohy;
- Náhrada nefunkčního zařízení;
- Změna konfigurovatelných parametrů;
- Změna adresace (IP, BACnet);
- Rozšíření systému (např. přidání dalších vstupů a výstupů, modulů . . .);
- Oprava chyb ve specifickém SW;
- Doplnění funkcionality nebo rozšíření specifického SW.

Pokud jsou k výše zmíněným zásahům třeba **přístupové údaje**, musejí být součástí dokumentace. Zadavatel musí mít k dispozici přístup s **nejvyššími** možnými oprávněními (Administrator, root, technik...). Faktické využívání těchto údajů pro zásahy do konfigurace bude upraveno záručními podmínkami díla.

Pokud je k výše zmíněným úkonů potřeba **specializovaný software**, musí tento být součástí dodávky také, a to **včetně instalačních souborů** nebo médií a včetně časově neomezené **licence** pro používání.

Musí být dodány takové licence, které umožní z technického i právního hlediska instalaci SW na záložní hardware, připravený k nasazení v případě výpadku. Zejména je nepřípustné dodat pouze licence, které jsou vázány na konkrétní hardware, takže SW nelze v případě výpadku na záložním HW zprovoznit.

Součástí dodávky musí být i tzv. *specifický SW*. Zejména jsou tím myšleny programy v regulátorech. Toto programové vybavení musí být dodáno ve zdrojovém tvaru tak, aby zadavatel byl schopný provádět úpravy těchto programů a mohl použít programové vybavení i v jiných zařízeních (např. při výměně vadného kusu).

Dodavatel zároveň předáním díla souhlasí s budoucími **opravami, úpravami a opětovným použitím** v rámci BMS MU.

Dodavatel je povinnen při každé úpravě nebo opravě, kterou provádí, dodat Garantovi aktuální zdrojové soubory *specifického SW*.

Rovněž musí být dodány podrobné návody, jak postupovat v případě údržby, změny konfigurace a opětovného uvedení systému do provozu.

Po dobu záruky na dílo je dodavatel povinen zajistit **funkčnost dodaného software na nejnovější verzi operačního systému** MS Windows nebo některé z rozšířených distribucí OS Linux (Debian, Ubuntu, Fedora).

2.17 Dokumentace

Z pohledu dokumentace skutečného provedení BMS MU jsou důležité následující dokumenty, které musí být součástí dokumentace předávaného díla:

- **Technická zpráva**;
- **Připojení prvků BMS MU do Technologické sítě** – pro každý aktivní prvek BMS MU (server, regulátor, převodník...) komunikující prostřednictvím protokolů IP a/nebo Ethernet je nutné uvést:
  - Číslo zásuvky;
  - Číslo portu na Switchi;
  - BACnet ID, pokud existuje;
  - IP adresu, pokud existuje.
- **Schémata rozvaděčů** – zahrnující podrobně rozkreslené zapojení zařízení na napájení a do regulátoru/kontroleru, včetně jističů, svorek atp., v souladu a propojené s dokumentací ostatních systémů.
- **Napojení na podřízené technologie** – pro každý vstup nebo výstup regulátoru nebo jiného zařízení se vstupy a výstupy je třeba dodat mapování vstupů a výstupů na signály v podřízeném systému.

- **Topologické schéma zapojení** – schéma zachycuje zapojení na sběrnicích BACnet MS/TP, Modbus, M-Bus a podobných. Schéma musí zachycovat pořadí zařízení na sběrnici spolu s jejich adresami.
- **Uživatelská dokumentace** – Popisuje práci se systémem z pohledu uživatele BMS.
- **Administrátorská dokumentace** – popisuje postupy pro změnu všech konfigurovatelných nastavení instalovaných zařízení, obnovu softwaru zařízení ze zálohy a zprovoznění nového zařízení. Dále obsahuje popis fungování systému, konkrétní použité zapojení a síťovou adresaci a seznam hodnot konfigurovatelných parametrů.
- **Přístupové údaje** – Veškeré přístupové údaje umožňující používání a správu systému. Podrobně viz část 2.16 (Software a data pro správu systému).

Dokumenty **Připojení prvků BMS** a **Napojení na podřízené technologie** musejí být dodány v **editovatelném tabulkovém formátu** (Excel, CSV). Topologická schémata musejí být dodána ve formě CAD výkresu (DWG) a ve formě barevného PDF. Jako formát PDF **není akceptovatelný** naskenovaný výkres uložený ve formátu PDF. PDF musí obsahovat vektorovou grafiku a texty. PDF musí být v rozlišení dostačujícím pro tisk na formát A3.

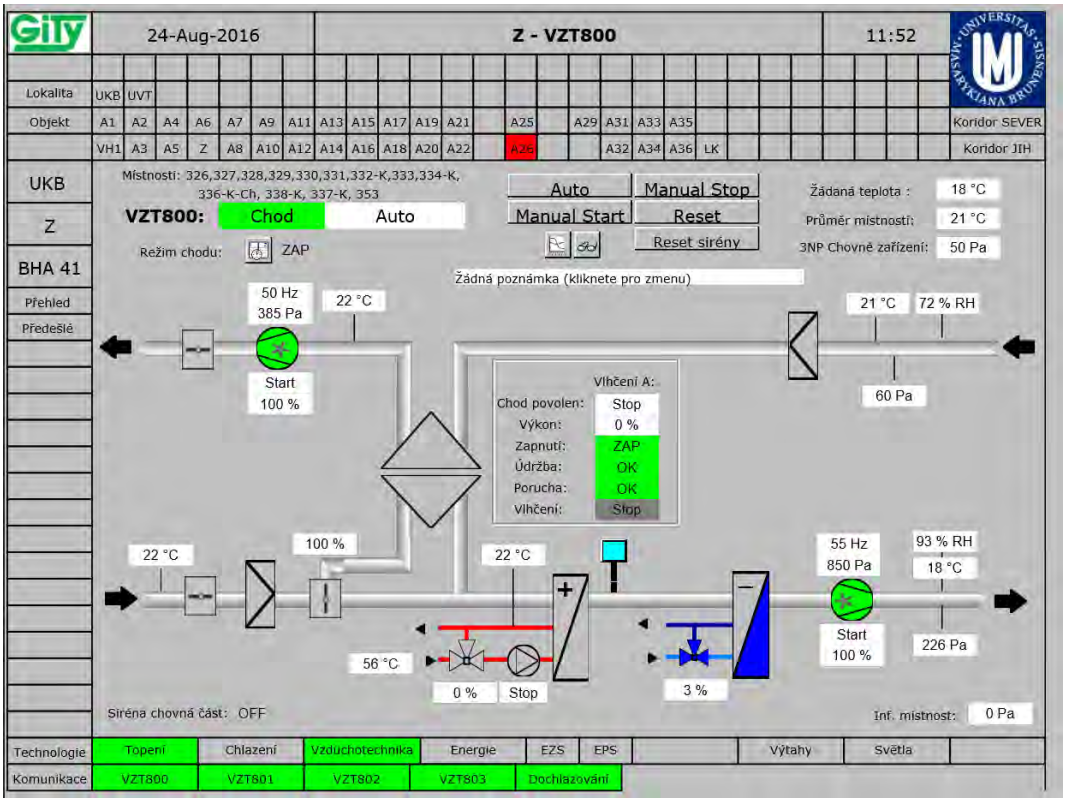
Případné další doplňující požadavky na dokumentaci jsou uvedeny v částech věnovaných jednotlivým technologiím.

3 Uživatelské prostředí

Při připojení nových zařízení komunikujících protokolem BACnet do BMS MU je vždy nutné vytvořit nové (a/nebo upravit stávající) **vizualizační obrazovky** pro software **ORCAView** a **ORCAWeb**. Obecné požadavky na funkci a strukturu vizualizačních obrazovek jsou uvedeny v této kapitole. Konkrétní standardy pro vizualizační obrazovky různých technologií jsou popsány v příslušných částech Metodiky.

3.1 Obecné standardy vizualizačních obrazovek

Vizualizační obrazovky jsou výhradním prostředkem pro ovládání BMS MU v běžném provozu. Jejich správná funkce je proto klíčová pro provoz technologií budov.



Obrázek 3.1: Obrazovka technologie

Obecné požadavky, platné pro všechny vizualizační obrazovky v BMS MU jsou následující:

- S obrazovkami musí být dodány veškeré použité **rastrové obrázky**, které nejsou součástí standardní knihovny Delta Controls;

- Obrazovky **nesmí** obsahovat odkazy na **objekty, které neexistují** v BMS MU;
- V obrazovkách je třeba přímo **vizualizovat fyzické vstupy a výstupy** regulátorů (objekty AI, BI, MI...) a nikoliv objekty typu proměnná (Variable – AV, MV, BV), do kterých jsou hodnoty ze vstupů kopírovány. Výjimka je možná pouze u objektů, které nemají fyzickou reprezentaci (žádané hodnoty, stavové proměnné, proměnné pro nastavení režimu, sumární objekty apod.), případně v dalších případech po schválení ze strany Garanta;
- Obrazovky **nesmí** obsahovat odkazy na **obrazovky** nebo jiné dokumenty (HTML, PDF, apod.), které **neexistují** v BMS MU;
- U každé hodnoty, jejíž historie je ukládána (tzn. existuje objekt Trendlog) musí být v obrazovce **odkaz na** tento **Trendlog**. Pokud se Trendlog ukládá i do archivní databáze, musí na obrazovce přítomen i odkaz na archivní Trendlog.
- Obrazovky musí obsahovat **prostor pro umístění tzv. poznámky**. Garantovi musí být doplnění poznámek umožněno bez porušení záruky, případně musí být provedeno dodavatelem po domluvě s Garantem. Standardní velikost poznámky zobrazuje 3.1 (poznámka je umístěna pod tlačítky ovládání technologie);
- Obrazovky musí obsahovat všechny **povinné komponenty** (viz dále) a celkově respektovat zvyklosti uživatelského rozhraní BMS MU (viz dále). V odůvodněných případech lze učinit výjimku po schválení Garantem (např. specializované obrazovky pro dotykové panely);
- Obrazovky musí korektně **signalizovat manuální režim** (viz dále);
- Obrazovky musí korektně **signalizovat ztrátu komunikace** (viz dále);
- Obrazovky musí korektně implementovat zobrazení a **propagaci událostí a významných stavů** (viz dále).

3.2 Povinné komponenty vizualizačních obrazovek

Každá vizualizační obrazovka obsahuje určité komponenty, které slouží k navigaci v uživatelském prostředí BMS MU. V následujících částech jsou popsány tyto povinné části obrazovek v závislosti na jejich typu.

3.2.1 Společné komponenty vizualizačních obrazovek

Každá obrazovka obsahuje tyto základní komponenty:

- Titulek obrazovky (Název technologie / Budovy / Areálu – viz specifikace v části metodiky věnované příslušné technologii);
- Datum – vlevo od titulku;
- Čas – vpravo od titulku;
- Logo MU;

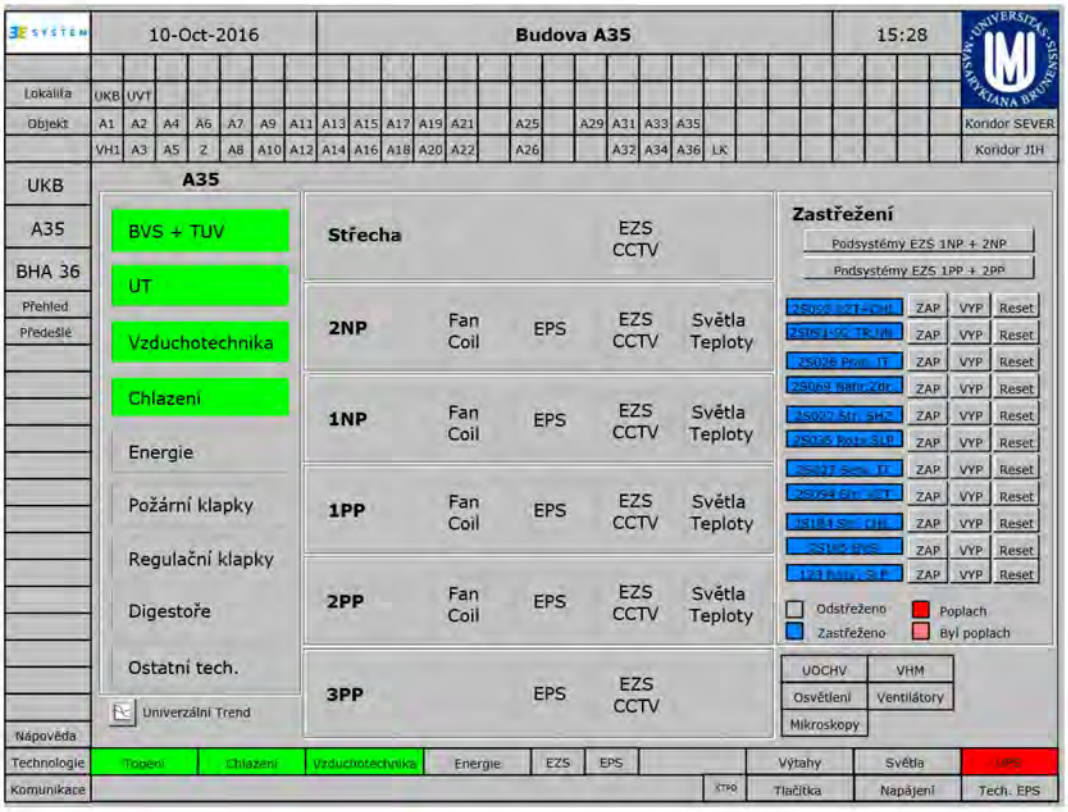
- Horní navigační menu – obsahuje následující odkazy:
  - Ostatní lokality;
  - Ostatní budovy v rámci lokality - V této části navigační lišty jsou odkazy na budovy obarvovány na základě pravidel pro propagaci alarmů a chybových stavů (viz A26 na Obrázku 3.1).
- Levé navigační menu – obsahuje:
  - Odkaz na přehledovou obrazovku areálu (např. `UKB` na Obrázku 3.1);
  - Odkaz na přehledovou obrazovku budovy (např. `Z` na Obrázku 3.1);
  - Polohový kód budovy (např. BHA36);
  - V případě obrazovek, které obsahují půdorys podlaží: odkazy na obrazovky stejné technologie v jiných podlažích téže budovy;
  - Odkaz `Přehled` – Odkaz na přehledovou obrazovku areálu;
  - Odkaz `Předešlé` – Odkaz na předchozí navštívenou obrazovku;
  - Odkaz `Komunikace` – Odkaz na obrazovku s přehledem funkčnosti vybraných zařízení v areálu.
- Dolní navigační menu – odkazy v menu jsou obarvovány podle pravidel propagace chybových stavů. Menu obsahuje:
  - Odkazy na další technologie společné pro areál (v případě přehledové obrazovky); nebo společné pro budovu (v případě obrazovek technologií a přehledových obrazovek budovy);
  - Odkazy na další obrazovky technologie stejného typu v rámci budovy/areálu (např. ostatní jednotky VZT v budově);
  - Zvláštním případem jsou přehledové obrazovky technologií společných pro celý areál – ty nemusejí obsahovat odkazy na další technologie, pouze na další obrazovky stejné technologie.

3.2.2 Přehledová obrazovka budovy

Přehledová obrazovka budovy slouží jako hlavní navigační rozcestník ke všem technologiím, které jsou v budově ovládány prostřednictvím BMS. Musí z ní vést odkazy na všechny obrazovky, které se týkají technologií dané budovy. Hlavní části obrazovky jsou následující:

- Tlačítka **hromadných** technologií budovy v levé části – tlačítka jsou obarvována podle pravidel propagace alarmů;
- Odkazy na plány podlaží pro **distribuované** technologie;
- Přehled zón PZTS – přehled obsahuje názvy zón, jejich stavy a ovládací prvky;
- Odkazy na další speciální technologie.

Zařazení obrazovek příslušných technologií do kategorií (**Distribuované**/**Hromadné**) je součástí příslušných částí Metodiky věnujících se předmětným technologiím.



Obrázek 3.2: Přehledová obrazovka budovy

3.2.3 Přehledová obrazovka areálu

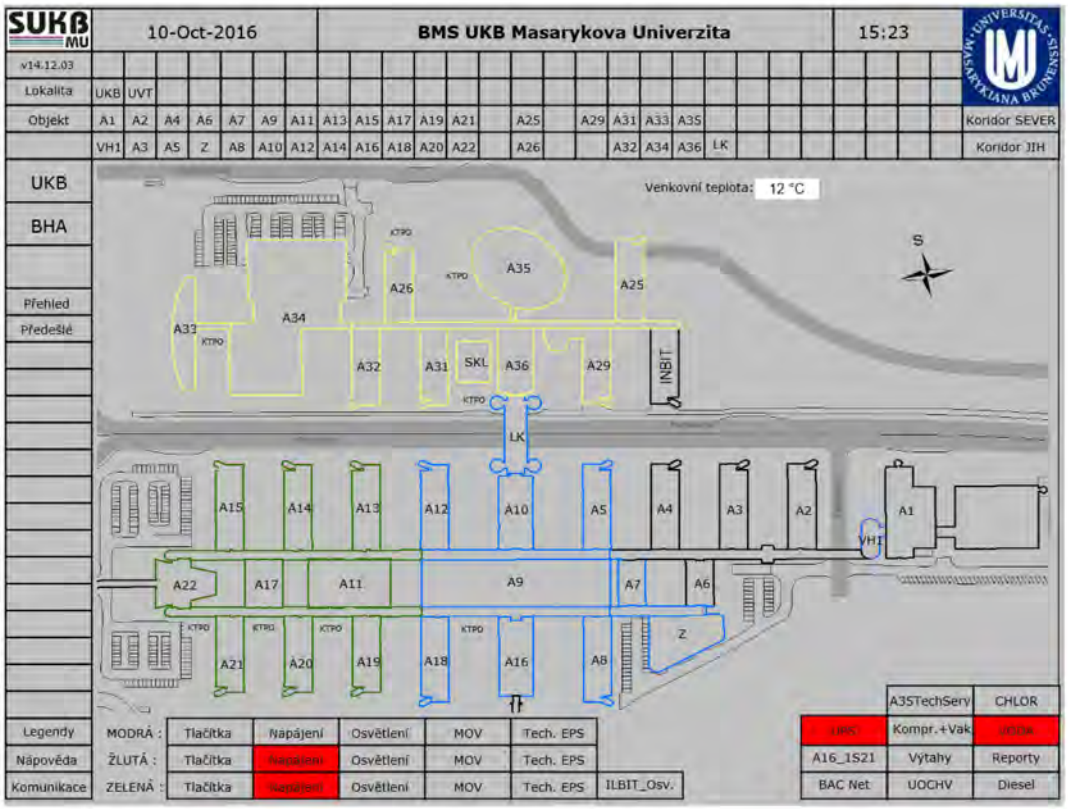
Přehledová obrazovka v areálu obsahuje navíc kromě prvků, které jsou společné pro všechny obrazovky, a navíc:

- V titulku uvedený název areálu;
- Mapa areálu – na mapě areálu jsou vyznačeny půdorysy budov, které jsou obarvovány podle pravidel pro propagaci alarmů a chybových stavů (viz dále).

3.2.4 Obrazovka s půdorysem/mapou

Některé obrazovky obsahují půdorys podlaží (obrazovky hromadných technologií) nebo mapu (přehledová obrazovka areálu). Pro tyto obrazovky navíc platí další požadavky:

- Veškeré půdorysné obrazovky musí obsahovat směrovou růžici;
- Nesmí se překrývat prvky obrazovky;
- Musí být čitelná čísla místností;
- Musí být zobrazeny pouze nutné vrstvy stavebních konstrukcí (stěny, dveře, okna, schodiště);



Obrázek 3.3: Přehledová obrazovka budovy

- A další nutná opatření, aby obrazovka byla přehledná.

3.3 Použití barev BMS MU

Výchozí podkladová barva obrazovek je stříbrná (RGB [192, 192, 192]), jinou barvu je možné použít pouze ve výjimečných případech a po schválení Garantem.

Barvy pro signalizaci stavu technologií a zařízení musí respektovat normu **ČSN EN 60073 - Základní a bezpečnostní zásady pro rozhraní člověk-stroj, značení a identifikaci – Zásady kódování sdělovačů a ovládačů** a zvyklosti BMS MU.

Základní barevné schéma BMS MU:

- Šedá – Výchozí stav – Vypnuto/Neaktivní/V pořádku/Bez signalizace;
- Zelená – Chod (V případě, kdy je tento stav vizualizován podbarvením);
- Žlutá – Servis;
- Červená – Porucha/Chyba;
- Fialová/Růžová – Ztráta komunikace.

Zvyklosti ohledně používání barev jsou dále specifikovány v částech Metodiky, věnujících se příslušným technologiím.

3.4 Fyzikální jednotky

Pro zajištění přehlednosti a přesnosti zobrazení měřených a žádaných hodnot je nutné dodržet zobrazení hodnot v následujícím tvaru:

- Teplota vzduchu – jedno desetinné místo (např. 21.3 °C);
- Teplota topné vody – bez desetinných míst (např. 55 °C);
- Teplota chladicí vody – jedno desetinné místo (např. 7.3 °C);
- Otevření ventilu – bez desetinných míst (např. 75 %);
- Tlak vzduchu – bez desetinných míst (např. 310 Pa);
- Tlak vody – bez desetinných míst (např. 354 kPa);
- Tlak [bar] – dvě desetinná místa (např. 3.54 bar);
- Vlhkost vzduchu – bez desetinných míst (např. 36 % RH);
- Spotřeby energií – počet desetinných míst podle typu používaných jednotek a přesnosti měřidla, obvykle však na jedno desetinné místo (např. 2510.2 kWh, 118.3 m^3, 514.6 GJ).

Jednotky u zobrazených hodnot v obrazovkách musí být dynamicky načítány ze stejného datového bodu, ze kterého je načítána hodnota. Výjimky jsou možné v případě neobvyklých jednotek nebo za zvláštních okolností; v obou případech toto podléhá schválení Garanta.

3.5 Signalizace manuálního režimu

U každé zobrazované hodnoty (i když je vizualizována formou animace/vizualizace barvou) je třeba indikovat, pokud je daný objekt v **manuálním režimu** (hodnota nastavena operátorem). To je v BMS MU signalizováno symbolem ruky.

Výjimky jsou možné v následujících případech:

- Vizualizovaný datový bod není možné manuálně ovládat (tedy při pokusu o manuální ovládání dané zařízení toto nedovolí);
- Jedná se o žádanou hodnotu, která je nastavována pouze uživatelem (neplatí např. pro žádané hodnoty vypočtené z ekvitermy apod.);
- Objekt je v obrazovce, která bude do Webového rozhraní BMS MU přeložena bez kontextových menu (např. přehledová obrazovka pavilonu, PZTS, EPS) a zároveň bude tato obrazovka používána pouze ve Webovém rozhraní BMS MU.

Ve sporných případech rozhoduje o nutnosti signalizace ručního režimu Garant.

3.6 Signalizace ztráty komunikace

Ztráta komunikace s některým zařízením poskytujícím data pro obrazovku se signalizuje zobrazením otazníků místo hodnoty. U prvků, které neobsahují dynamický text, se **změní barva** (na růžovou pro MaR, na bílou pro PZTS, EPS).

Ztráta komunikace musí být **zjevná při pohledu na obrazovku**, z toho důvodu je zakázáno používání dvojice obrázků pro signalizaci stavu (např. obrázky OK/Porucha).

U všech datových bodů, které jsou přenášeny pomocí převodníku (jedná se např. o Modbus převodník pro elektroměry, M-Bus pro vodoměry a měřiče tepla, převodník pro splity, zdroje chladu) musí být zajištěna signalizace věrohodnosti zobrazovaných dat (např. růžové podbarvení). Důvodem je možný výpadek zařízení (či jeho komunikace) za převodníkem (elektroměr, vodoměr) – v tom případě se nesignalizuje výpadek standardně (pomocí otazníků v textovém poli), proto je nutné signalizovat jiným způsobem. Tento požadavek platí i pro jakékoliv datové body v obrazovkách, které nejsou vizualizovány odkazem na zařízení, ze kterého původně pocházejí (např. takzvané **proxy objekty** pro doplnění chybějící funkcionality apod.).

3.7 Vizualizace a propagace událostí významných stavů

Základním mechanismem pro upozorňování o významných událostech v BMS MU jsou tzv. Události (viz 2.14). K událostem musí být doplněny odkazy do vizualizačních obrazovek. Při výskytu události nebo při jejím prohlížení zpětně musí být možné dostat se v jednom kroku („jedním klikem“) na příslušnou obrazovku, kde je hodnota vizualizována) – technický postup je popsán v **Metodice Správa vizualizačních obrazovek BMS MU** (Příloha C).

Kromě samotného mechanismu Událostí je vyžadováno, aby chybové a další stavy hodné pozornosti (typicky `Alarm`/`Servis`/`Chod`) byly vizualizovány přímo ve **vizualizačních obrazovkách**, dokud významný stav stále trvá. Chybové stavy jsou propagovány na přehledové obrazovky (budovy, areálu). Vždy, když je některá z technologií budovy v takovém významném stavu, je třeba tento stav vizualizovat jak v obrazovce příslušné technologie, tak na přehledových obrazovkách a navigační liště. Stavy vyžadující propagaci jsou rozděleny do tří tříd:

- Stav s nižší závažností — Alespoň jeden z možných stavů technologie obarvuje tlačítko příslušné technologie v přehledové obrazovce pavilonu a zároveň obarvuje půdorys budovy na přehledové obrazovce;
- Stav s vyšší závažností — Alespoň jeden z možných stavů technologie obarvuje tlačítko příslušné technologie v přehledové obrazovce pavilonu a zároveň obarvuje jak půdorys budovy na přehledové obrazovce areálu, tak odkaz na budovu v **navigační liště na všech obrazovkách areálu**.
- Stav bezpečnostní technologie (PZTS, EPS) – Alespoň jeden z možných stavů technologie obarvuje tlačítko příslušné technologie v přehledové obrazovce pavilonu a zároveň obarvuje odkaz na budovu v **navigační liště na všech obrazovkách areálu**.

K propagaci významných stavů se dále váží následující pravidla:

- Pokud některá technologie v budově je ve stavu, který by měl být zpropagován na přehledové obrazovky a navigační lišty, musí k propagaci dojít – chybový stav má nejvyšší prioritu;

- Stav `V pořádku`/`Chod` apod. může být indikován na přehledové obrazovce pavilonu (typicky zeleným podbarvením tlačítka), nepropaguje se ale na přehledovou obrazovku areálu. To samé se může týkat i některých jiných stavů – tato pravidla jsou stanovena u každé technologie;
- V horní navigační liště jsou zobrazovány pouze stavy `Porucha/Chyba` (tzn. tlačítko má pouze dva stavy – `Porucha` a `Výchozí/OK`);
- Původ stavu, který byl propagován do přehledových obrazovek, musí být vizualizovaný i na obrazovce technologie tak, aby bylo možné jasně určit, co je příčinou problému;
- Pokud je na přehledové obrazovce areálu vizualizována porucha, musí být vizualizována i na přehledové obrazovce budovy;
- Každá událost typu Alarm musí být zároveň vizualizována v obrazovkách BMS MU – Události, které neoznačují chybový stav (např. otevření dveří pomocí karty, zastřežení zóny, záloha paměti regulátoru) nejsou vizualizovány a ani se nepropagují na přehledové obrazovky a navigační lišty, nesmí ale zároveň využívat typ zprávy `Alarm` dle normy protokolu BACnet;
- Konkrétní popis přiřazení událostí do tříd a způsobu propagace na přehledové obrazovky se nachází v částech Metodiky věnovaných jednotlivým technologiím;
- Jakékoliv jiné chování propagace alarmů je zakázáno bez schválení Garantem.

4 Komunikační prostředí

Technologická síť MU (TeNe) je základním komunikačním prostředím pro veškeré technologie, které jsou monitorovány a řízeny systémem BMS MU. Jedná se o strukturovanou kabeláž a související aktivní prvky. Tato infrastruktura je **oddělená** od standardní (tzv. akademické) datové sítě, která je součástí internetu. Technologická síť využívá fyzické infrastruktury (rozvodny, kabelové trasy) budované v rámci akademické sítě MU, **aktivní prvky** (přepínače, směrovače) však používá **vlastní**. Zařízení, umístěná v technologické síti, jsou tedy od internetového provozu **oddělena** – neexistuje síťová cesta umožňující zařízením komunikovat vně technologické sítě. Vyjímky jsou možné pouze po schválení Garantem - v takovém případě je potom komunikace vedena před firewall.

Technologická síť v prostředí MU sestává z **podsítí lokalit** (LAN TeNe) a **páteřní komunikační sítě** (páteřní TeNe). Páteřní TeNe propojuje jednotlivé podsítě směrovacím protokolem OSPF tak, aby byla zajištěna konektivita k centralizovaným službám BMS MU, které jsou provozovány na UKB.

Jediná možná konektivita (mimo aplikační servery BMS MU) z tzv. akademické sítě MU je řízena firewallem, kde jsou definována **jednoznačná** přístupová pravidla. Firewall Juniper SRX240 směruje veškerý povolený provoz z datové sítě MU do technologické sítě, navíc integrované služby (AV, IPS) zvyšují on-line bezpečnost, což eliminuje možné hrozby a bezpečnostní rizika. Firewall spravuje oddělení ODS ÚVT.

4.1 Lokální technologická síť

Technologická síť musí zajistit spolehlivou a bezpečnou komunikaci jednotlivých komponent BMS MU. Komunikační infrastruktura je vytvořena samostatnými vyhrazenými aktivními a pasivními síťovými prostředky. Způsob komunikace jednotlivých komponent BMS MU v tomto prostředí je definován komunikačním protokolem dle ČSN EN ISO 16484-5. Jednotlivé technologické sítě stavebních objektů nebo areálů musí být možné propojit se vzdáleným dohledovým a řídícím pracovištěm pomocí uvedeného protokolu s využitím aktivních síťových prostředků a páteřních IP sítí, intranetu a internetu.

Je nutné upřesnit, co v této kapitole představuje pojem aktivní prvek, případně aktivní síťový prvek či prostředek: v tomto případě se jedná vždy o ethernetový přepínač (switch), který musí splňovat níže uvedené vlastnosti.

4.1.1 Pasivní síťové prostředky technologické sítě

Projekt a realizace strukturované kabeláže v objektu musí zohlednit potřeby napojení jednotlivých komponent BMS MU na aktivní prvek technologické sítě. Požadavky musí být definovány v projektech jednotlivých komponent BMS MU. Minimální požadovaný **standard** je kabeláž kategorie 5e v nestíněném provedení. Měřícím protokolem musí být doloženo dodržení předepsaných parametrů pro strukturovanou kabeláž. Kabeláž musí obsahovat dostatečný počet servisních zásuvek na vhodných místech; ve všech místech napojení zařízení BMS MU na strukturovanou kabeláž musí být nejméně **dva volné vývody zakončené zásuvkou** strukturované kabeláže pro servisní účely.

Kabeláž je ukončována v zásuvkách co nejblíže k připojovanému zařízení. Pokud je připojované zařízení v rozvaděči MaR, zásuvka se umístí do rozvaděče včetně servisního vývodu. Druhý konec je na propojovacím panelu v datovém rozvaděči. Datové rozvaděče jsou umístěny ve vyhrazených místnostech – tzv. slaboproudých rozvodnách. Ve vzdálenosti 2-3 m od propojovacího panelu strukturované kabeláže musí být v datovém rozvaděči umístěny aktivní síťové prvky.

Kabeláž nižší úrovně propojující jednotlivé regulátory a případně polní instrumentaci je ve sběrnicové technologii dle standardu pro sběrnici RS-485.

Případné **páteřní spoje** mimo dosah metalické kabeláže jsou provedeny pomocí jednovidové optiky 9/125 µm. V odůvodněných případech, a pokud délka kabeláže umožní gigabitové přenosy, je možno použít mnohavidová vlákna, nicméně v tomto případě je nutný souhlas Garanta.

4.1.2 Aktivní síťové prostředky technologické sítě

Každá lokalita, která je připojována do páteřní technologické sítě, **musí být** osazena **minimálně jedním** centrálním L3 přepínačem. U některých lokalit je nutná redundance centrálního uzlu (např. UKB), nutnost redundance bude posouzena Garantem při zahájení projekčních prací. L3 přepínač zprostředkovává konektivitu k přístupovým L2 přepínačům lokality a k páteřní technologické síti. Přístupové L2 přepínače zajišťují připojení jednotlivých technologií.

Páteřní technologický přepínač, který tvoří hranici mezi tzv. lokální TeNe a tzv. páteřní TeNe, je vždy připojen **dvěma směry** k páteřní technologické síti (viz 4.2 odstavec 2.). Tato redundantní konektivita zajistí trvalou nepřerušenou komunikaci i v případě výpadku jednoho ze tří uzlů páteřní TeNe.

Stručně shrnuto, každá lokalita předpokládá minimálně jeden L3 přepínač, který slouží k připojení do páteřní sítě, a jeden nebo více L2 přepínačů pro napojení jednotlivých technologií (shodně je provozována i technologická síť v rámci UKB, kde L2 přepínače jednotlivých pavilonů připojují provozované technologie, zatímco L3 přepínače datových center ve věžích LK zajišťují vazbu na systém BMS MU a páteřní komunikaci). V odůvodněných případech lze pro připojení technologií využít přímo porty L3 přepínače, odpadá tedy nutnost osadit přístupový L2 přepínač. Tato výjimka však podléhá schválení Garantem.

Aktivní síťové prostředky - přepínače musí umožňovat definování virtuálních sítí tak, aby bylo možné v rámci komunikačního prostředí oddělit komunikaci jednotlivých technologických komponent systému BMS MU. Všechny komunikační uzly musí být napájeny ze zdroje **zálohovaného** napájení 1. kategorie (VDO). Více v kapitole 5.

Minimální HW požadavky na aktivní síťový prostředek:

L2 (příp. L3 přepínač), 24(48) 10/100 RJ45 metalických portů, 2x RJ45 metalické porty 10/100/1000 a 2 porty pro osazení SFP (případně jen 4x SFP porty — centrální L3 přepínač vždy). Pomocí uplinkových portů (SFP) je napojen na centrální switch (router) technologické sítě. Centrální L3 přepínač se v některých případech může hardwarovou konfigurací odchylovat od uvedených parametrů (například větší počet SFP portů); bude uvedeno v zadání. U každého přepínače je vyžadována rezerva minimálně 4 porty RJ45, výjimky jsou možné po schválení Garantem. Přepínač musí být možné namontovat do 19“ datového rozvaděče (v případě jiných rozměrů je nutná odpovídající montážní sada). Aktivní síťový prostředek (přepínač, směrovač) dále musí splňovat následující parametry:

- L2 vrstva:
  - IEEE 802.1D-1998 (ISO/IEC 15802-3:1998)
  - IEEE 802.1Q-2003

  - počet aktivních VLAN: min. 255
  - IEEE 802.1X – Port Based Network Access Control
  - 802.1s – Multiple Spanning Tree Protocol
  - 802.1w – Rapid Tree Spanning Protocol
  - 802.1p - Minimálně 4 vnitřní fronty
  - detekce protilehlého zařízení (CDP, LLDP)
  - detekce jednosměrné linky (UDLD)
  - IGMP snooping v2, v3
- Fyzická vrstva IEEE 802.3-2000
  - 802.3ad – minimálně dvě skupiny sdružených portů
  - 802.3z
  - jumbo frames
  - standardní optické adaptéry (GBIC, SFP) – podle nasazení, minimálně však 2 ks,
  - musí spolupracovat s optickými adaptéry třetího výrobce
- Management
  - SNMP (min. v2)
  - SNMP trap, inform
  - RMON
  - ladicí (debugovací) informace (včetně posílání přes vzdálený syslog)
  - portmirroring
- Ovládání
  - CLI (příkazová řádka)
  - SSH server
  - konzola na sériové lince
  - třídy příkazů (privilegovaný/neprivilegovaný)
  - textové konfigurační soubory
  - popisy portů
  - možnost zálohování konfigurace v txt
  - možnost upgrade software/firmware
- Autentizace, autorizace, accounting:
  - přes vzdálenou službu (TACACS+, RADIUS)
- Zobrazení aktuálního stavu

  - ARP tabulky (VLAN, port…)
  - MAC address tabulky
  - zobrazení stavu interface:
    * popis interface
    * in/out bajty pakety
    * počty chyb (CRC, runt, late-coll)
  - system:
    * zatížení procesoru
    * obsazení paměti
    * procesy
- Logování
  - vzdálený SYSLOG
  - lokální buffer
- Omezení přístupu k lokálním službám pomocí firewallových pravidel
- Místní klienti:
  - NTP klient
  - DNS klient
  - SSH klient
  - telnet klient

Rozšíření požadavků pro centrální L3 přepínač — podpora rozšířených IP služeb (IP services)

- IP Helper Address;
- RFC 2328 – OSPF version 2;
- RFC 2338 – IP Redundancy VRRP;
- RFC 2453 – RIP v2;
- RFC 3046 – DHCP/BootP Relay;
- RFC 3768 – VRRP - Virtual Router Redundancy Protocol;
- Static Routes;
- routovací tabulka o velikosti min 24 000 záznamů.

4.1.3 Adresace na úrovni protokolu BACnet

Základní komunikační protokol pro technologickou síť a řídicí systém je definován normou **ČSN EN ISO 16484-5**, dále označované jako BACnet. U každého zařízení, které komunikuje v TeNe tímto protokolem, musí být možné nastavit adresu BACnet (Device Object Identifier) libovolně z rozsahu dle normy BACnet.

Pokud jsou použita v dané lokalitě jak BACnet/IP zařízení, tak i BACnet MS/TP zařízení, vždy zařízení na IP/Ethernet bude mít adresu dělitelnou 100 (např. 30900) a k němu připojená zařízení MS/TP budou adresována v daném rozsahu (např. 30900 – 30999).

Pokud jsou použita pouze BACnet/IP zařízení, v daném rozsahu budou adresována v řadě za sebou (např. 30800, 30801...).

Konkrétní **adresní rozsah pro nově připojovanou lokalitu** stanoví Garant.

4.1.4 IP adresace

IP adresace UKB MU

Adresovací plán pro UKB MU je definován podle vzoru:

adresní rozsah	10.**V**.**O**.**X**
maska	255.255.0.0
gateway	10.**V**.0.1

V je číslo virtuální sítě 10,11,12,13... Vytvořeny jsou tyto virtuální sítě:

- 10: MNG pro management zařízení UKB
- 11: BACnet pro připojení zařízení z MaR, PZTS, EPS z AVVA Modrá, Zelená
  BACnet pro připojení zařízení z EPS, PZTS z AVVA Žlutá
- 12: PZTS EPS AVVA Modrá, Zelená, ILBIT
- 13: CCTV pro kamerové systémy UKB
- 31: BACnet pro připojení zařízení z MaR na protokolu BACnet UKB Žlutá D
- 32: PZTS EPS AVVA UKB Žlutá D
- 33: PCO pro připojení pracoviště PCO
- 41: BACnet pro připojení zařízení z MaR na protokolu BACnet CETOCOEN
- 61: BACnet pro připojení zařízení Šumavská 15

O je číslo objektu 1,2,3...99...101... Čísla jsou objektům přiřazena dle jednotlivých pavilonů

X je nahrazeno unikátním číslem prvku v povoleném rozsahu 2-254, z toho 2-9 vyhrazeno pro diagnostiku

Konkrétní **adresní rozsah pro nově připojovanou lokalitu v rámci UKB** stanoví Garant.

IP adresace MU (mimo UKB)

Adresovací plán je definován podle vzoru:

adresní rozsah:	10.**O**.**T**.**X**
maska:	255.255.255.0
gateway:	10.**O**.**T**.1

O je unikátní identifikátor **objektu**, například:

101: ICS Botanická 68a
102: CPS Komenského nám. 2
103: ECON ESF Lipová 41a

T slouží k identifikaci **technologie**, např.:
10: MNG pro management zařízení
11: BACnet pro připojení zařízení technologií MaR
12: PZTS EPS
13: CCTV

X je nahrazeno **unikátním číslem prvku** v povoleném rozsahu 2-254, z toho 2-9 je vyhrazeno pro diagnostiku a servisní účely.

Identifikátory nových lokalit a technologií **stanoví Garant**.

4.1.5 Směrování na úrovni protokolu BACnet

Technologická síť je na základě výše uvedených adresních pravidel rozdělena do IP podsítí (LAN lokalit, případně VLAN), které spolu komunikují prostřednictvím páteřní technologické sítě. Pro zajištění komunikace řídicího systému se servery je nutné v každé IP podsíti **MaR** (tj. VLAN 11) instalovat zařízení podporující **BBMD** dle standardu ANSI/ASHRAE Standard 135-2004, ANNEX J. Zařízení musí podporovat zákaz směrování broadcastových zpráv na protokolu BACnet.

Standard zařízení, podporujícího **BBMD**: Delta Controls eBCON.

Standard zařízení, podporujícího **filtrování broadcast zpráv**: Delta Controls eBMGR.

4.2 Páteřní technologická síť

Je plně ve správě Oddělení datových sítí (ODS) ÚVT. Je tvořena třemi hlavními přístupovými uzly — x-ics, x-cps a x-econ, které tvoří fyzický trojúhelník. Toto redundantní zapojení zabezpečí trvalou komunikaci i v případě poruchy jednoho z páteřních uzlů — dojde pouze k výpadku komunikace technologií, které jsou do TeNe připojeny v rámci tohoto uzlu. Podmínkou je, aby páteřní L3 přepínač lokality byl připojen současně ke dvěma těmto páteřním uzlům tak, aby výpadek jednoho z nich nepřerušil komunikaci mezi připojenou lokalitou a UKB, kde se nachází centrum služeb TeNe.

5 Napájení a jeho sledování

5.1 Obecné požadavky

Cílem napájecí strategie je zajistit provoz a funkcionalitu BMS (po dobu minimálně jedné hodiny) i v situacích, kdy je omezeno napájení budovy nebo dílčích částí z veřejné sítě. Budova musí být vybavena náhradními zdroji napájení - dieselagregátem (DA) a zároveň akumulátorovým nepřerušitelným zdrojem (UPS). Jiné řešení je podmíněno schválením Garanta a Investora.

5.2 Kategorie důležitosti

Rozvody napájení jsou rozlišeny podle kategorií důležitosti. Rozvody musí být naprojektovány tak, aby obsahovaly rozvody pro všechny tři kategorie důležitosti již od hlavních rozváděčů objektu a sekce pro jednotlivé stupně důležitosti musí být v rozvaděčích zřetelně označeny a viditelně odděleny. Jednotlivé kategorie napájí tato zařízení:

1. kategorie (**VDO**, zálohované UPS)
    - všechny aktivní prvky technologické sítě (kap. 4)
    - prvky insfrastruktury BMS (servery, gatewaye)
    - regulátory MaR
    - chladící jednotky v rozvodnách SLP (včetně typu SPLIT)
    - prvky CCTV (viz kapitola 5.2.1)
    - požární výtahy (pokud není řešeno samostatně)
2. kategorie (**DO**, zálohované DA) - systémy PZTS, EKV a případně další zařízení určené Investorem
3. kategorie (**MDO**, nezálohované)

5.2.1 Napájení prvků CCTV

Celá komunikační síťová infrastruktura CCTV systému včetně klientů dohledového centra (i s monitory) je **napájena z obvodů 1. kategorie (VDO).**

Kamery jsou **napájeny z portů přepínačů (VDO)** (podpora funkce PoE – 802.3af, případně PoE+ - 802.3at). Externí kamery, které jsou připojeny optickým kabelem, mají samostatné napájení - rovněž zálohované. Výjimky určuje Investor a nebo Garant.

5.2.2 Redundanantí napájení

Je-li jakýkoliv server, instalovaný prvek TeNe nebo jiné zařízení vybaveno dvěma napájecími zdroji, musí být jeden zdroj připojen na obvody VDO a druhý na obvody MDO. Zároveň je požadováno, aby byly tyto obvody (zásuvky) řádně označeny.

5.3 Požadavky na náhradní zdroje

Při výpadku hlavního přívodu napájení musí ihned nastartovat DA. Pro překlenutí okamžiku startování, jsou obvody VDO a případné požární rozvody zálohovány UPS. Po nastartování, DA zajistí napájení obvodů DO a UPS. Přepínání náhradních zdrojů při výpadku i obnově napájení musí být **plně automatické**.

5.3.1 UPS

Na UPS jsou kladeny tyto požadavky:

- její stav musí být monitorován v BMS dle požadavků uvedných v kapitole 5.4.1
- musí být napájena z DA
- výkon musí být nadimenzován tak, aby byla schopna poskytnout alespoň **20 minut** provozu při instalované zátěži (s rezervou +30 %; soudobost se nebere v úvahu), pro pokrytí času do doby startu DA
- musí být umístěna v prostředí vybaveném klimatizací, aby byla zajištěna konstantní teplota prostředí $20 \pm 2°C$ z důvodu životnosti baterií
- v místě umístění UPS musí být umístěny dva vývody slaboproudé kabeláže pro připojení komunikačního rozhraní

5.3.2 Dieselagregát

- stav DA musí být možno nepřetržitě sledovat v BMS pomocí některého z komunikačních protokolů 6.4, a to i během výpadku. Více viz 5.4.2
- zařízení (gatewaye apod.) určená pro komunikaci s DA musí být napájena z UPS
- vybaven automatikou startu
- K obnově napájení z DA musí dojít nejpozději do jedné minuty po výpadku hlavního přívodu napájení

5.4 Sledování stavu náhradních zdrojů

5.4.1 Sledování UPS

Všechny UPS musí být dodány s rozhraním SNMP pro vzdálený dohled a správu, a proto v blízkosti instalované UPS je nezbytné umístit minimálně dva datové vývody. Součástí dodávky SNMP modulu je i MIB tabulka SNMP objektů od výrobce, přiložená k dokumentaci. Dodaný SNMP modul musí být schopen vyhovět standardu stávajícího monitoringu UPS na MU, který zahrnuje SNMP podporu a měření okamžitých hodnot těchto objektů (veličin):

- Okamžitý stav systému (síť, běh na akumulátor, vypnuto, přemostěno . . .)

- Kapacita akumulátorů `[% celkové kapacity akumulátorů]`
- Teplota akumulátorů `[°C]`
- Vstupní síťový kmitočet `[Hz]`
- Vstupní síťové napětí `[V]`
- Výstupní zatížení `[% kapacity systému]`
- Výstupní činný výkon `[W]`
- Odhadovaný zbývající čas běhu na akumulátor
- Dosavadní čas běhu od posledního transferu (síť - akumulátor)

V případě 3fázové UPS, musí obsahovat separátní SNMP objekty (nikoliv SNMP tabulky) pro jednotlivé fáze u veličin: napětí, kmitočtu, zatížení a činného výkonu.

5.4.2 Sledování DA

Řídící jednotka DA musí být vybavena komunikací s BMS pomocí některého z povolených protokolů uvedených v kapitole 6.4. Je požadováno sledování těchto stavů nebo veličin:

- informace o chodu
- informace o poruše
- nedostatek paliva
- výpadek napájení
- jistič generátoru
- jistič sítě
- hladina paliva `[l]` + trendlog
- napětí startovací baterie `[V]` + trendlog

5.5 Sledování stavu prvků SLN

Napájení všech silových a MaR rozvaděčů je nutné sledovat a přenášet do řídícího systému tak, aby byla zajištěna dostatečná spolehlivost této informace (relé pro hlídání fází, není přijatelné odvozovat od stavu jističe). Výjimky jsou možné pouze pro rozváděče MaR které jsou kompletně napájeny z jednoho okruhu (např. fan-coilové rozvaděče ...), nebo pro rozváděče, u kterých Garant písemně schválí výjimku.

Během přípravy projektu může Investor nebo Garant určit další jističe, u kterých musí být **pomocným kontaktem sledován stav** a přenášen do BMS.

Vzdáleně pomocí BMS musí být také sledován stav přepěťových ochran v rozvaděčích.

Je také požadováno sledování napájení klimatizačních jednotek (vnitřních i venkovních) pomocí pomocného kontaktu jističe.

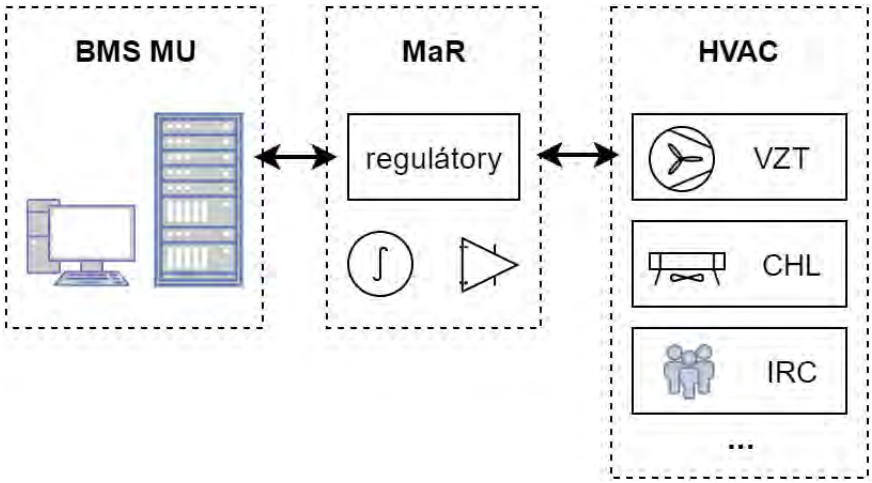
Sledování napájení čerpadel a motorů viz 7.6.9

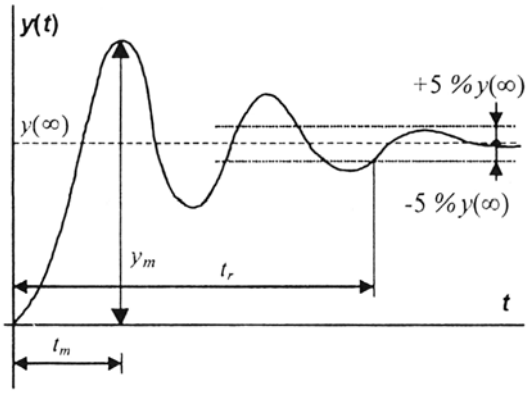
6 Měření a regulace

6.1 Úvod

Profese MaR (Měření a Regulace) zajišťuje řízení, sledování a integraci technologického zařízení budov, včetně potřebných snímačů a akčních členů. Prvky technologie MaR (řídicí systém) jsou tedy prostředkem pro řízení a regulaci technologií budov (HVAC, měření energií a další) a zároveň poskytují vybrané měřené veličiny pro vizualizaci (BMS MU).

Technologie **MaR je tedy zároveň rozhraním mezi BMS MU a technologiemi budovy**. V hardwarové rovině jde o aktivní prvky technologické sítě, v softwarové potom relevantní BACnet objekty (povolení chodu, nastavení ŽH, měřené hodnoty...). Použité prvky MaR musí splňovat požadavky uvedené v této kapitole i ostatních částech metodiky.





Obrázek 6.1: Regulační děj s vyznačenými veličinami

6.2 Obecné požadavky na regulaci

Úkolem regulace je nastavení technických veličin (regulovaná veličina y - teplota, tlak, otáčky ...) na žádanou hodnotu w a udržovat je na této hodnotě i při působení poruch (vnějších vlivů). Regulační odchylka e je rozdílem těchto hodnot $e = w - y$. Úkolem regulačního procesu je udržovat tuto odchylku minimální, nejlépe nulovou. Z hlediska automatizace budov a níže zmíněných technologií je zásadní především kvalita regulace v časové oblasti. Pro jednoduché posuzování kvality regulace můžeme definovat pojmy (viz obrázek 6.1):

κ **relativní překmit** „přeregulování“ reg. veličiny: $\kappa = \frac{y_m - y(\infty)}{y(\infty)}$ kde
y_m je maximální hodnota regulované veličiny
t_m je čas, kdy je tato hodnota dosažena
$y(\infty)$ je žádaná hodnota

t_r **doba regulace** doba za kterou trvale klesne odchylka regulované veličiny y pod pod 5%

Teoretickým cílem je dosáhnout žádané hodnoty $y(\infty)$ v co nejkratším čase t_r s nulovým překmitem $\kappa = 0$.

U pomalých dějů, jako je regulace teploty a vlhkosti prostředí je vyžadována regulace s nulovým překmitem $\kappa = 0$ a dobou regulace $t_r < 15min$. **Jsou vyloučeny veškeré kmitavé nebo pilovité průběhy** regulované veličiny.

U dějů, kde nedochází k přímému styku regulovaného děje s uživateli budovy (tedy především technologické povahy, například regulace polohy pohonů a ventilů), můžou být průběhy rychlejší s překmitem do 10 % ($\kappa < 0,1$), ovšem tak, aby nedošlo k poškození akčního členu nebo technologie překmitem mimo povolený rozsah.

Je nezbytné, aby byly **vytvořeny vždy dva trendlogy**, jeden s žádanou hodnotou a druhý s regulovanou veličinou, aby bylo možné Investorem, Garantem a samotným zhotovitelem zhodnotit kvalitu regulačního děje.

6.3 Řídicí systém

Řídicí systém ovládaných technologií je tvořen soustavou HW zařízení - např. regulátory, gatewaye a aplikačním (řídícím) programem (v rámci této Metodiky jsou řídicí programy považovány za tzv. Specifický software). Řídící systém udržuje chování dotčených technologií v předem definovaných provozních podmínkách (ať již pevně daných, tak i obsluhou definovaných). Řízení a ovládání jednotlivých technologií je úzce svázáno s údaji poskytovanými prvky polní instrumentace (7.6), které jsou do systému integrovány dle projektu MaR.

Regulátory jsou umístěny v rozvaděčích, které jsou poblíž ovládaných zařízení a vybaveny odpovídajícím množstvím potřebných vstupů a výstupů.

Propojení systémových regulátorů a vazby řídících prvků na systém BMS MU se provádí vyhrazenou technologickou sítí (4). Aplikační regulátory jsou propojeny se systémovými regulátory sběrnicí dle standardu `RS-485` odpovídající kabeláží (6.4). Do jednotlivých vstupů a výstupů kontrolérů je napojená polní instrumentace. Polní instrumentace musí komunikovat na úrovni signálů (dle kap. 7.6) nebo pomocí komunikačního protokolu (dle kap. 6.4).

Komunikační **protokol řídicího systému je BACnet** (dle kap. 2.4). Pro připojení řídicího systému jako celku do BMS MU **není možné** použít gateway (překlad z jiného protokolu).

Dodavatel musí před zahájením prací sestavit typový seznam prvků řídicího systému a **předložit jej ke schválení Garantovi**. Garant si může vyžádat otestování každého typu zařízení, aby se vyloučily problémy se zařízením při připojování do BMS MU a TeNe. Dodavatel je povinen předat zařízení korektně nakonfigurované a v takovém zapojení s ostatními zařízeními, aby byly co nejvěrněji simulovány podmínky plánovaného nasazení zařízení. Zároveň s každým zařízením dodavatel Garantovi předá „Protocol Implementation Conformance Statement“ (PICS) a popis účelu zařízení. Testování probíhá dle **Metodiky Testování zařízení pro BMS MU**, která bude na žádost předána dodavateli.

Řídicí systém musí být napájen ze zálohovaného zdroje (obvodů VDO), aby veškeré technologie bylo možné ovládat a monitorovat i v případě výpadku napájení. Více viz v kap. 5.

6.3.1 Požadavky na regulátory

Pro plynulý a bezproblémový chod regulátorů je třeba zajistit minimální volné místo ve statické a dynamické paměti regulátoru a minimální scan rate. Dále je třeba zajistit minimální počet resetů regulátoru a aktuálnost jeho firmwaru. V rámci jednoho regulátoru je nutné mít **minimálně 20% rezervu z celkové statické a 20% rezervu z celkové dynamické paměti** pro plynulý chod regulátorů. Dále je třeba zajistit, aby se hodnota scan rate nedostala pod hodnotu 5 scan za sekundu. Při instalaci regulátoru je nutné držet počet resetů v jednotkách na jednom zařízení. Nedodržení tohoto předpisu je možné pouze v odůvodněných případech se souhlasem Garanta. Dále je nutné vždy dodávat regulátor s nevyšší možnou verzí firmwaru, pokud Garant nestanoví jinak.
Standard:

- Systémové regulátory:
  - eBCON (Delta Controls);
  - DSC 1616E (Delta Controls);
  - DSC 1280E (Delta Controls);
  - DSM RTR (Delta Controls).
- Aplikační regulátory:
  - DAC 1146 (Delta Controls);
  - DAC 633 (Delta Controls);
  - DFC 304R3-240 (Delta Controls).

6.3.2 Požadavky na rozváděče

Rozváděč musí vyhovovat požadavkům normy **ČSN EN 61439** (nebo aktuálně platné novelizace) včetně dodané dokumentace. Všechny rozváděče musí být přístupné nejvýše s použitím „kličky“ bez nutnosti demontáže nebo použití zámků, ale v případě, kdy je rozváděč umístěn na veřejně přístupném místě (chodba, posluchárna), musí být navíc umístěn za uzamykatelnými dveřmi. Rozváděče musí být zároveň umístěny tak, aby byla **minimalizována rizika poškození jejich vybavení** - zejména nesmí být umístěny pod vedením kapalných médií (rozvody pitné nebo odpadní vody, TUV, kondenzátu, chladiva

apod.) nebo pod zařízeními u kterých hrozí úniky těchto látek (potrubí, split, fan-coil, atd.). V rozváděčích musí být dostatečná rezerva (v momentě dokončení díla) pro další rozšiřování v budoucnu nebo úpravy systému:

- prostorová rezerva v rámci jednoho rozváděče musí být **minimálně 20% z celkové využité plochy** - to například odpovídá ekvivalentu jedné prázdné přístrojové řady ve skříni, která by obsahovala další 4 obsazené.
- Vstupně/výstupní rezerva u instalovaných regulátorů nebo V/V modulů musí být **minimálně 20%** z celkového počtu **vstupů** a 20% z celkového počtu **výstupů**.

Zařízení, připojená pomocí `Cat5e` kabeláže, musí být připojena prostřednictvím síťové zásuvky s konektorem `RJ45`, vhodně umístěné v prostoru rozváděče. V každém rozváděči vybaveném síťovými zásuvkami `RJ45` musí být k dispozici minimálně navíc dvě další zásuvky nad rámec instalovaných zařízení: jedna navíc jako rezerva pro další rozšiřování systému a jedna servisní zásuvka `RJ45` pro připojení notebooku nebo jiných servisních zařízení.

Regulátory, PLC a další zařízení určená k montáži do rozváděčových skříní musí být instalována výhradně do skříní k tomu určených. V rozváděčích, kde je připojené silové napájení, je nutné zajistit dostatečnou ochranu před dotykem živých částí. Při instalaci nových silových rozváděčů je nutné realizovat dostatek místa mezi kabely a zařízeními, aby bylo možné bezpečně připojit klešťové měřicí přístroje.

6.3.3 Ovládání a sledování zařízení

Provozní stav zařízení je definován souborem následujících stavů:

1. Stav běhu:
   - Binární proměnná (BI/BV/BO);
   - Možné stavy:
     - 0 - stop;
     - 1 - chod.
2. Alarmové stavy:
   - Více stavová proměnná (MI/MV;)
   - Možné stavy:
     - 1 - OK;
     - 2 - alarm tlaku(ů);
     - 3 - alarm komunikace;
     - 4 - alarm napájení;
     - 5 - alarm teploty (termokontakt).
3. Řídící zdroj:
   - Více stavová proměnná (MI/MV);

- Možné stavy:
  - 1 - Automatické;
  - 2 - Ruční z BMS;
  - 3 - Ruční lokální.

Pro potřeby vizualizace je nutné pro každé zařízení vytvořit sumární objekt (sumář), který poskytuje rychlé a přehledné informace o zařízení, je vhodný k obarvení symbolu zařízení:

- Více stavová proměnná (MI/MV);
- Možné stavy:
  - 1 - stop;
  - 2 - chod;
  - 3 - alarm;
  - 4 - servis.

Do provozního stavu zařízení také patří veškeré další údaje o stavu zařízení (např. otáčky motoru, frekvence napájení, teplota, tlak ...).

Pro snímače a měřidla energií a médií je provozní stav definován jako soubor všech veličin, které snímač či měřidlo poskytuje řídicímu systému. Tyto veličiny je možné doplnit o stav běhu, alarmové stavy a řídící zdroj.

Pro binární proměnné je vyžadována konfigurace, kdy stav 0 (`OFF`) odpovídá stavu stop, normál, vypnuto ... a stav 1 (`ON`) odpovídá stavu chod, alarm, zapnuto ...

Sledování zařízení

Sledováním zařízení rozumíme odečítání a vizualizaci provozního stavu, který je pro dané zařízení k dispozici. Pro bezproblémovou obsluhu systému BMS MU je nutné, aby sledování bylo co nejvíce důvěryhodné, k čemuž je nutné splnit podmínky z kapitoly 7.6.

Více o sledování čerpadel v kapitole 7.6.9, ventilátorů (7.6.10), přesných klimatizací (7.5.2).

Ovládání zařízení

Ovládáním zařízení rozumíme určování stavu určitého zařízení, případně nastavování jeho provozních parametrů (výkon, ŽH, míra otevření ventilu, reset ...)

Řídící zdroj je zdroj ovládání určitého zařízení.

Všechna zařízení jsou ve výchozím stavu ovládána automaticky (tzn. programem v regulátoru). V určitých situacích je nutné tato zařízení ovládat manuálně. Ruční režim může být

- z BMS: ovládání zařízení z BMS MU přepnutím odpovídající proměnné do požadovaného stavu.
- lokální: ovládání zařízení pomocí SLN vybavení rozvaděče.

V případě různých povelů z různých řídících zdrojů má vždy nejvyšší prioritu lokální ruční ovládání, následně ruční ovládání z BMS MU a nakonec automatické. Ruční ovládání lokální se realizuje pomocí přepínače na dveřích rozvaděče nebo případně v rozvaděči (přepínač na VV modulu). Zapojení ručního ovládání musí být realizováno tak, aby bylo možné ve všech případech spolehlivě zařízení ovládat (nezávisle na regulátoru, stykači . . .). Další možnost ručního ovládání lokálního je přímo pomocí součástí daného zařízení (např. u pohonů klapek kličkou . . .).

6.3.4 Ukládání provozního stavu

U všech zařízení musí být možnost ukládat provozní stav do archivní databáze pro další zpracování (ve formě trendlogů a alarmů). Rozsah ukládání dat specifikuje uživatel a v čase může být proměnný.

Ke sledování zařízení rovněž patří i odečítání doby běhu zařízení. U zařízení s konstantním příkonem se realizuje pomocí objektu `Binary Totalizer`. U zařízení s proměnným příkonem se realizuje pomocí objektu `Analog Totalizer`, případně může být nahrazeno určenými objekty od výrobce (např. v případě frekvenčních měničů, zdrojů chladu. . .). I tyto objekty musí být možné ukládat do SQL databáze, rozsah ukládání specifikuje uživatel a v čase může být proměnný. Totalizéry jsou vyžadovány u všech zařízení, které mají roční spotřebu elektrické energie vyšší než 2500 kWh.

6.3.5 Měřidla energií a médií

U měřidel musí být možné sledovat a ukládat jejich provozní stav. Odečty nesmí být narušeny výpadkem napájení. Měřidla musí být **vybavena komunikačním rozhraním** podporujícím protokoly uvedené v kapitole 6.4. Dodána musí být měřidla schváleného typu. Měřidla s impulsním výstupem bez matematického členu nejsou pro nasazení v systému BMS MU vhodná a dostačující.

Standard:

- Elektrická energie
  - BACnet MS/TP
  - Veris E50
  - Modbus RTU
  - Schneider electric PM 710
  - Merlin Gerin PM9C
- Teplo
  - M-Bus
  - Pollutherm
  - Census
- Voda
  - M-Bus
  - ENBRA

6.4 Komunikační protokoly

Základní komunikační protokol pro technologie HVAC je BACnet, který je maximálně upřednostněn. Více viz kapitola 2.4. Možné jsou jeho následující implementace:

- IP – UDP/IP;
- Ethernet;
- MS/TP (485).

Volba konkrétní implementace závisí na možnostech řešení přenosových cest, požadované latenci (řízení vs. monitoring) a složitosti sítě. Vždy je preferován BACnet IP, BACnet MS/TP lze použít pro koncové prvky nebo tam, kde by bylo použití IP nehospodárné. Pro napojení měřidel, polní instrumentace a rozšíření vstupů a výstupů lze použít doplňkové protokoly:

- LINKnet (nástěnné ovladače pro uživatelský vstup);
- Modbus RTU (integrace přídavných V/V modulů příp. jiných technolgií – zdroje CHL, FM);
- M-Bus (měřiče energií);
- MP-Bus;
- enteliBUS.

Pro vedení komunikačních linek je nutno použít odpovídající kabeláž:

- BACnet IP/Ethernet – Cat5e.
- BACnet MS/TP + LINKnet – Belden 9842.
- Modbus – FTP twisted pair.
- M-Bus – UTP twisted pair.

Použití doplňkového protokolu je podmíněno **obousměrným funkčním převodem** na základní protokol a souhlasem Garanta. Pro řízení osvětlení (rozsvícení, zhasnutí, řízení intenzity) hlavně tam, kde je požadováno ovládání různých skupin osvětlení, je vyžadováno použití protokolu DALI. Použití těchto protokolů a jimi používané instrumentace je podmíněno zajištěním převodníku (více viz 2.10.2) pro propojení se základním protokolem BACnet a souhlasem Investora. Použití některého z protokolů musí být **koordinováno s řešením napájení osvětlení**. Použité komunikační protokoly a adresace prvků musí být vyznačeny v topologickém schématu technologické sítě.

6.5 Dokumentace MaR

Dokumentace MaR obsahuje:

- Seznam výkresové dokumentace;
- Technická zpráva;
- Půdorysné plány všech dotčených podlaží s vyznačenou polohou, označením a propojením prvků ve formátu `.dwg` a `.pdf` (viz výše);
- Technologická schémata jednotlivých systémů zahrnutých v MaR (BVS, ÚT, VZT, ZCH...);
- Schéma zapojení (topologie) - zapojení regulátorů s vyznačením druhů komunikace a zapojení do síťových prvků včetně použitých adres (IP, BACnet, případně dalších protokolů) a dotčených portů. Dále musí být jednoznačně identifikováno umístění jednotlivých zařízení (polohovým kódem, nebo označením lokality, budovy, podlaží a místnosti);
- Schémata zapojení rozváděčů zahrnující podrobně rozkreslené zapojení zařízení na napájení a do regulátorů, včetně jističů, svorek atp., v souladu a propojené s dokumentací ostatních systémů (VZT, ÚT, silnoproud...);
- Pro každý regulátor seznam jeho portů (komunikačních, vstupů, výstupů...), u obsazených s popisem připojeného zařízení, označení signálu (v souladu s ostatní dokumentací MaR) a označení připojeného zařízení v dokumentaci dalších technologií (např. VZT);
- Specifikaci zařízení, tedy seznam veškerých použitých zařízení v minimálním rozsahu: [výrobce; typ; název; popis; označení; poznámka], kde název je např. „Snímač teploty“, popis je stručný seznam parametrů zařízení (příkon, rozsah, typ signálu, napájení...), označení je označení zařízení a/nebo signálu (v souladu se zbytkem dokumentace), poznámka je umístění nebo logická vazba na jiné zařízení (např. ÚT větev západ, Napájení 12RH...);
- Okomentované zdrojové kódy konfiguračních programů MaR (strukturovaný text, ladder diagram, funkční bloky a další) v editovatelné podobě (záloha regulátorů, projekty atd.). Pokud Garant nemá SW nástroje k úpravě zdrojových kódů (nebo má pouze nedostatečný počet licencí), je povinností zhotovitele tyto SW nástroje (či licence v dostatečném počtu a bez jejich časového omezení) objednateli předat (viz také část 2.17).

7 HVAC

7.1 Úvod

Technologie **HVAC (Heating, Ventilation and Air Conditioning)** je technologie, jejímž cílem je dosažení **tepelného komfortu a kvality vzduchu** v jednotlivých prostorách budov **při zachování efektivity provozních a pořizovacích nákladů**. Tyto standardy jsou definovány v tabulce přílohy D. HVAC využívá prostředků dílčích technologií jako je chlazení (CHL), vzduchotechnika (VZT), vlhčení (VLH), příprava teplé vody (TV) nebo ústředního vytápění (ÚT).

7.2 Zásady návrhu

Dokumentace **již od stupně DVD** musí obsahovat **výpočet předpokládaných tepelných zisků**, potřebný chladící výkon jednotlivých místností a celé budovy. Návrh a výpočet musí zohlednit:

1. vnější vlivy
   (a) tepelné vlastnosti stavební konstrukce budovy
   (b) přenos tepla vedením konstrukcí budovy
   (c) místní klimatické poměry (tepelné špičky)
   (d) orientaci a umístění budovy v terénu
   (e) přenos okny (solar heat gain factor)
2. vnitřní vlivy
   (a) obsazenost a vybavení místnosti
   (b) množství instalované výpočetní techniky
   (c) zisky z osvětlení
   (d) požadavky na současné i potenciální využití řešené části budovy
3. vliv samotného technologického zařízení
   (a) výpočet tepelného zisku z hnacích ventilátorů
   (b) tepelného zisku v přepravním potrubí
   (c) tepelné ztráty v regulačních klapkách
4. legislativní požadavky a aktuálně platné technické normy, zejména

   Nařízení vlády č. 93/2012 Sb. kterým se stanoví podmínky ochrany zdraví při práci
   ČSN EN ISO 11855 Navrhování prostředí budov

ČSN EN 13779 Větrání nebytových budov - Základní požadavky na větrací a klimatizační systémy

ČSN 12 7010 Vzduchotechnická zařízení - Navrhování větracích a klimatizačních zařízení - Obecná ustanovení

ČSN EN 15423 Větrání budov - Protipožární opatření vzduchotechnických systémů

ČSN EN 15243 Větrání budov - Výpočet teplot v místnostech, tepelné zátěže a energie pro budovy s klimatizačními systémy

ČSN EN 15251 Vstupní parametry vnitřního prostředí pro návrh a posouzení energetické náročnosti budov s ohledem na kvalitu vnitřního vzduchu, tepelného prostředí, osvětlení a akustiky

ČSN EN 15241 Větrání budov - Výpočtové metody pro stanovení energetických ztrát způsobených větráním a infiltrací v budovách

ČSN EN 12098 Regulace otopných soustav

7.3 Vytápění a výroba TV

BMS MU snímá provozní parametry systému topení a výroby TV a řídí výrobu a distribuci tepla dle stanovených pravidel. Je vyžadováno, aby montáže čidel teploty pro řídicí systém a kontrolní lokální měření teplot byly totožně umístěny (čidlo v jímce), tedy co nejblíže vedle sebe a bez jiného ovlivnění, aby byla možná co nejpřesnější kontrola správnosti naměřených hodnot. Systém musí být možné lokálně ovládat manuálně bez BMS MU a vzdáleně pomocí systému BMS MU. Z hlediska řízení je nutné věnovat velkou pozornost správnému návrhu ventilů a vyvážení tlakových poměrů. Nevhodná charakteristika ventilů může způsobit rozkmitání systému a prakticky nemožnost dosáhnout uspokojivého řízení.

Jako smluvní požadavek je nutné doložit výpočtem ověřený a měřením s měřícím protokolem potvrzený skutečný stav zaregulování soustavy TV, včetně hodnot požadovaného nastavení regulačních a by-passových ventilů a čerpadel.

7.4 Vzduchotechnika

Technologie musí umožňovat instalaci teplotních čidel dle příslušných norem, jedná se hlavně o vzdálenosti mezi ohřívákem a chladičem a přístupnost tohoto prostoru pro servis protimrazové ochrany. Nasávací a odtahové potrubí musí být osazeno uzavíratelnou klapkou. Pokud je technologie v objektu, klapka musí být umístěna co nejblíže vnějšího pláště objektu. Pokud jsou použity ve VZT zvlhčovací jednotky, musí mít **komunikační rozhraní** dle kapitoly 6.4. Pokud jsou použity ve VZT frekvenční měniče, musí mít **komunikační rozhraní BACnet** dle kapitoly 6.4 . Při použití protimrazové ochrany (PMO) je nutné ji osadit ve VZT jednotce tak, aby správně plnila svoji funkci (tzn. spínala při reálné hrozbě zamrznutí ohřívače). PMO musí umožňovat funkci automatické deblokace po odeznění podmínek pro aktivaci. PMO nesmí být programově blokována a nesmí být možnost ručně zakázat její funkci či signalizaci (kromě poruchových stavů, zásah provede osoba zodpovědná za provoz MaR). Zapojení ostatních prvků polní instrumentace je řešeno projektem MaR dle požadavku Investora. Standardně používaným zvlhčovačem je **Defensor Mk5 s rozhraním Modbus**.

7.5 Zdroje chladu

Zdroje chladu musí zajistit výrobu chladícího média pro fan-coily a VZT jednotky v potřebném množství. Jsou dodávány jako kompaktní autonomní jednotky, u kterých systém BMS MU povoluje chod a sleduje poruchy. Přestože se jedná o autonomní jednotky, je požadováno, aby tyto jednotky měly komunikační rozhraní protokolem dle kap 6.4. Je požadován přístup ke všem provozním parametrům jednotky z BMS MU, aby bylo možné identifikovat případné poruchové stavy bez nutnosti fyzicky dojít k dané jednotce a odečítat stavy z provozního displeje jednotky zdroje chladu.

7.5.1 Lokální zdroje chladu, klimatizace typu split

Pokud v době provozu objektu vznikne požadavek na doplnění lokálního chlazení (ať už z důvodu nedostatečného výkonu stávajícího, rozšíření chlazených prostor nebo kvůli nutnosti chladit i v zimním období), je nutné zabezpečit integraci nových komponent se stávajícími systémy (především topení, chlazení, vzduchotechnika), aby **stávající a nové komponenty spolupracovaly, tzn. aby jeden systém netopil a druhý nechladil.**

Pro integraci splitového systému do BMS MU je nutné splnit následující podmínky:

1. Komunikace s BMS MU: (nutné splnit jeden z bodů)
   (a) musí být v souladu s kapitolou (6.3) a zároveň splňovat podmínky uvedené v 7.4.
   (b) Systém může mít jako nativní komunikační protokol i jiný protokol než BACnet, avšak musí být beze zbytku splněny podmínky dané kapitolou 2.10.2, zároveň splňovat podmínky uvedené v kapitole 7.4 a celkové navrhnuté řešení musí být před realizací **schváleno Garantem**.
2. Systém musí umožňovat sledování, ovládání a ukládání provozních stavů dle kapitoly 6.3.3 v minimálním rozsahu:
   (a) Kalendář (pro nastavení pracovních dnů)
   (b) Časový rozvrh (pro nastavení den/noc)
   (c) Žádané hodnoty (pro den i noc)
   (d) Celý systém HVAC pro místnost (sledování a ovládání zap/vyp, auto/man apod.)
   (e) Jednotlivá zařízení (okenní kontakt, aktuální teplota, ventily, ventilátory apod.)
3. Propojení se stávajícím (nebo novým) systémem topení/chlazení/VZT
   (a) Zvolí se jeden ze systémů (chlazení, topení) jako hlavní (master), a tento bude ovládat druhý (slave) pomocí komunikačního protokolu
   (b) Je možné, aby systémy pracovaly v rovnocenném režimu, ale musí být zajištěna jejich plná spolupráce
   (c) Jednotný provozní režim (zap/vyp, noc/den...)
   (d) Jednotné nastavení kalendářů a rozvrhů
   (e) Jednotné nastavení žádaných hodnot

(f) Jednotná regulace (buď je regulátor pouze v jednom systému nebo musí být regulátory vhodně sladěny - stejný typ regulátoru, stejný deadband apod.)

(g) Jednotné uživatelské rozhraní (jeden ovládací panel, jedna sada ovládacích a vizualizačních datových bodů ve vizualizaci BMS MU)

4. V místnostech, kde je plánována instalace dodatečného chlazení (splitů), je nutné zajistit automatické ovládání ventilů na otopných tělesech. Pokud je již v místnosti instalován fan-coil (včetně ovládání topení), není nutné tento systém měnit. Pokud je v místnosti topení ovládáno pouze lokálně (termostatické ventily…), je nutné toto ovládání nahradit automatickým (termoelektrická hlavice napájena `24 V`) a řídicí systém podle požadavků 6.3. Automatickým ovládáním ventilů je myšlena autonomní regulace teploty v místnosti na žádanou hodnotu.

5. V projektu musí být **zdůvodněno**, zda je vzhledem k rozsahu a životnosti hopodárnější použití klasické jednotky **split nebo systému VRV / VRF**.

7.5.2 Konkrétní požadavky na přesnou klimatizaci

Sledování provozních hodnot

Zejména je vyžadováno sledování následujících hodnot (stavů):

- Stav komunikace (má význam pro gateway – komunikace s vlastní jednotkou klimatizace);
- Chybový stav (binárně a s kódem chyby);
- Žádané hodnoty (teplota, vlhkost a další);
- Aktuální režim (vypnuto, chlazení, topení, větrání…);
- Rychlost ventilátorů;
- Povolení lokálního ovládání;
- Aktuální hodnoty (teplota, vlhkost a další určené Garantem);
- Stavy filtrů;
- Stav jednotky (zapnuto, vypnuto).

Ovládání jednotky

- Žádané hodnoty (teplota, vlhkost a další);
- Rychlost ventilátorů;
- Povolení lokálního ovládání;
- Aktuální režim (vypnuto, chlazení, topení, větrání…);
- Stav jednotky (zapnuto, vypnuto).

7.6 Polní instrumentace a prvky systémů HVAC

Všechny instalované prvky systému HVAC a MaR musí být řádně a viditelně označeny dle projektové dokumentace. Také musí být umístěny v takovém místě a s dostatkem okolního prostoru, aby byla možná jejich snadná pravidelná i nepravidelná údržba, výměna, čištění a revize.

7.6.1 Požární klapky

Stav požárních klapek musí být možné sledovat v BMS MU. Obvykle je realizováno připojením bezpotenciálových kontaktů z požárních klapek do regulátorů MaR. Jsou vyžadovány signály `NC (normally closed)`. Stav požárních klapek každé budovy je vizualizován na obrazovce v tabulkovém zobrazení a zároveň v půdorysných plánech EPS.

Jsou vyžadovány klapky se servopohonem napájené napětím **230 V** a dobou natočení **do 200 sekund**. Pouze se souhlasem Garanta je možné instalovat požární klapky jiného typu, než je uvedeno.

7.6.2 Regulační klapky

Pro klapku určené pro plynulé řízení průtoku je doporučeno používat klapky se střídavou orientací listů `[/ \ / \ / \]` z důvodu rovnoměrnějšího výstupu vzduchu (menší dyn. ztráty). Pro regulaci typu `ZAP/VYP` je výhodnější použití klapek se stejným směrem listů `[ / / / / ]` (nižší cena). Pouze se souhlasem Garanta je možné instalovat regulační klapky jiného typu, než je uvedeno.

Příklad zobrazení v BMS MU:

zavřená klapka

otevřená klapka

7.6.3 Nasávání a výdechy

Nasávací otvory musí být vzdáleny od zdrojů znečištění (odpadky, odpadní vzduch, emise atp.), ale zároveň přístupné pro čištění a údržbu. Také je třeba aby byly odstíněny, aby nedocházelo v létních měsících k nadměrnému zahřívání vstupního vzduchu.

Přívod vzduchu do vnitřního prostoru musí být dostatečně vzdálen od odtahu, aby se čerstvý vzduch dostatečně promíchal se stávajícím a nedošlo ke „zkratu“, kdy je nově přiváděný vzduch rovnou odtahován.

Výfuk odpadního vzduchu musí být proveden do venkovního prostředí, dostatečně vzdálen od nasávacích otvorů a nesmí být vystaven riziku ucpání (listí, sníh atp.)

7.6.4 Vzduchová potrubí

V závislosti na délce a tvaru potrubí dochází k významným ztrátám tlaku přepravovaného vzduchu (dynamické ztráty). Z tohoto důvodu je doporučena **minimalizace vzdálenosti, kolen, rozdělení a přechodů mezi průměry**. Zvýšení nebo snížení průměru potrubí musí být provedeno graduálně (vzájemný úhel stěn maximálně 15 °), aby bylo zamezeno vírům v ostrých hranách.

7.6.5 Snímače

U snímačů musí být možné sledovat a ukládat jejich provozní stav. Pro případ poruchy je nutné mít možnost snímač i ovládat (tedy nastavit řídící zdroj na `Ruční` z BMS MU a nastavit pevnou hodnotu veličiny) Pro analogové veličiny jsou vyžadovány snímače `0-5 V, 0-10 V, NTC 10 kΩ, 4-20 mA`. Pouze se souhlasem Garanta je možné instalovat snímače jiného typu, než je uvedeno.

Snímače prostorové teploty

Veškeré snímače teploty musí být instalovány tak, aby měřená hodnota nebyla ovlivňována nežádoucími vlivy okolí (např. sálání teplých povrchů, ochlazování proudícím vzduchem, oslunění, radiátor ...). Snímání teploty je třeba realizovat minimálně v následujících typech (účelech) místností:

- Slaboproudé rozvodny, serverovny;
- Silnoproudé rozvodny, rozvodny NN;
- Výměníkové stanice, kotelny, místnosti s rozvodem ústředního topení;
- Veškeré místnosti, jejichž teplota je ovlivňována technologickými prostředky budov. Výjimkou je místnost pouze s radiátorem a termostatickým ventilem nebo místnost, kde se VZT používá pouze k nucené výměně vzduchu (ne k vytápění či chlazení);
- Jakékoliv další místnosti, kde je měření teplot vyžadováno Investorem nebo Garantem.

Pokud je v místnosti instalováno zařízení, které je integrováno do BMS MU a toto zařízení měří prostorovou teplotu, není nutné instalovat další snímače teploty (jedná se např. o splity, ovladače fan-coilů apod.), musí však být zajištěna možnost sledovat a ukládat hodnotu teploty.

Snímače zaplavení

Snímače zaplavení musí být instalovány do **nejnižšího místa místnosti**. Pokud však celá místnost není vyspádovaná do jednoho místa, musí být snímač zaplavení v každém **lokálním minimu**. Snímače zaplavení musí být instalovány minimálně v následujících typech (účelech) místností:

- Slaboproudé rozvodny, serverovny;
- Silnoproudé rozvodny, rozvodny NN;
- Výměníkové stanice, kotelny, místnosti s rozvodem ústředního topení;
- Světlíky pro stupačky;
- Jakékoliv další místnosti, kde je detekce zaplavení vyžadována Investorem a/nebo Garantem.

Není nutné používat pouze plovákové snímače, u některých aplikací může být vhodnější detekční lano (nasákavý drát) či další typy snímačů.

7.6.6 Frekvenční měniče

Frekvenční měniče musí obsahovat **komunikační rozhraní BACnet** pro monitoring provozních hodnot. Řízení je nutno provádět analogovými signály z důvodu vyšší rychlosti a spolehlivosti oproti síťové komunikaci. Standardně používaným frekvenčním měničem je **ABB ACH 580/550** s rozhraním BACnet. Pouze se souhlasem Garanta je možné instalovat frekvenční měniče jiného typu, než je uvedeno.

7.6.7 Pohony

U pohonů musí být možné **sledovat a ukládat jejich provozní stav**. Ovládání pohonů musí být možné v plném rozsahu. Jsou vyžadovány analogové pohony řízené signálem `0-10 V`.

7.6.8 Ventily

U ventilů musí být možné sledovat a ukládat jejich provozní stav. Ovládání ventilů musí být možné v plném rozsahu. Parametry ventilu musí umožňovat snadnou ovladatelnost řízeného procesu. Rozsah otevření ventilu při běžné spojité regulaci se musí pohybovat v mezích 10-90 %. Jsou vyžadovány analogové pohony řízené signálem `0-10 V`. V případě nižších požadavků na kvalitu regulace je možné použít dvoustavové se souhlasem Garanta.

Příklad zobrazení v BMS MU

škrtící ventil 

třícestný ventil 

7.6.9 Čerpadla a motory

Čerpadla musí být nastavena dle příslušných norem, nastavení zdokumentováno protokolem.

Sledování zařízení

- Chod motoru se sleduje pomocí relé zapojeného paralelně s motorem, kombinací stavu stykače a hlídání napájení před stykačem nebo případně pomocí bezpotenciálového kontaktu u elektronických čerpadel. **Není přijatelné odvozovat stav chodchod pouze od stavu výstupu na ŘJ**, stavu stykače apod.
- Alarmy na motoru se sledují pomocí bezpotenciálových kontaktů u elektronických čerpadel (případně SSM – soubor poruchových hlášení) a u neelektronických motorů se sleduje termokontakt a napájení motoru.
- Řídící zdroj se určuje sledováním ručního ovladače nebo porovnáváním očekávaného a skutečného stavu (napájení v pořádku, stykač sepnut, motor neběží) v kombinaci s informací o ručním režimu z BMS MU.

Ovládání zařízení a ukládání provozního stavu musí být možné v plném rozsahu.

Grafické zobrazení v BMS MU pro čerpadlo

7.6.10 Ventilátory

Ovládání zařízení a ukládání provozního stavu musí být možné v plném rozsahu dle 6.3.3. Výjimkou ve sledování a ovládání mohou být odtahové ventilátory pro hygienická zařízení, kuchyňky, denní místnosti apod., kde může být dostačující sledovat stav jističe a ovládání realizovat automaticky či lokálně ručně.

Sledování zařízení

- Chod ventilátorů se sleduje pomocí **diferenčních tlakových snímačů** nebo případně stejně jako u čerpadel (7.6.9).
- Alarmy ventilátoru se vyhodnocují pomocí diferenčních tlakových snímačů, sledováním napájení a stykače nebo pomocí objektů BACnet na frekvenčním měniči.
- Řídící zdroj se určuje jako u motorů nebo pomocí objektů BACnet na frekvenčním měniči.

7.7 Popis UI BMS MU

Vizualizační obrazovky jsou výhradním prostředkem pro ovládání BMS MU v běžném provozu. Stav zařízení v objektu je prezentován zabarvením na obrazovce. Jednotlivé barvy jsou přiřazeny hodnotě vizualizační proměnné. Tato hodnota nesmí být nastavena manuálně. Níže uvedená barevná zobrazení jsou jednotně použita pro celou technologii MaR, HVAC a všechna její zařízení. Dále je nutné zachovat vizuální styl obrazovek, jak je popsán v kapitole 3.

- Zelená - na zařízení není signalizována porucha, zařízení je v chodu.
- Žlutá – zařízení je ve stavu servis.
- Červená - na zařízení je signalizována havárie.
- Šedá - zařízení je ve stavu stop.
- Růžová - zařízení přestalo komunikovat s BMS MU.

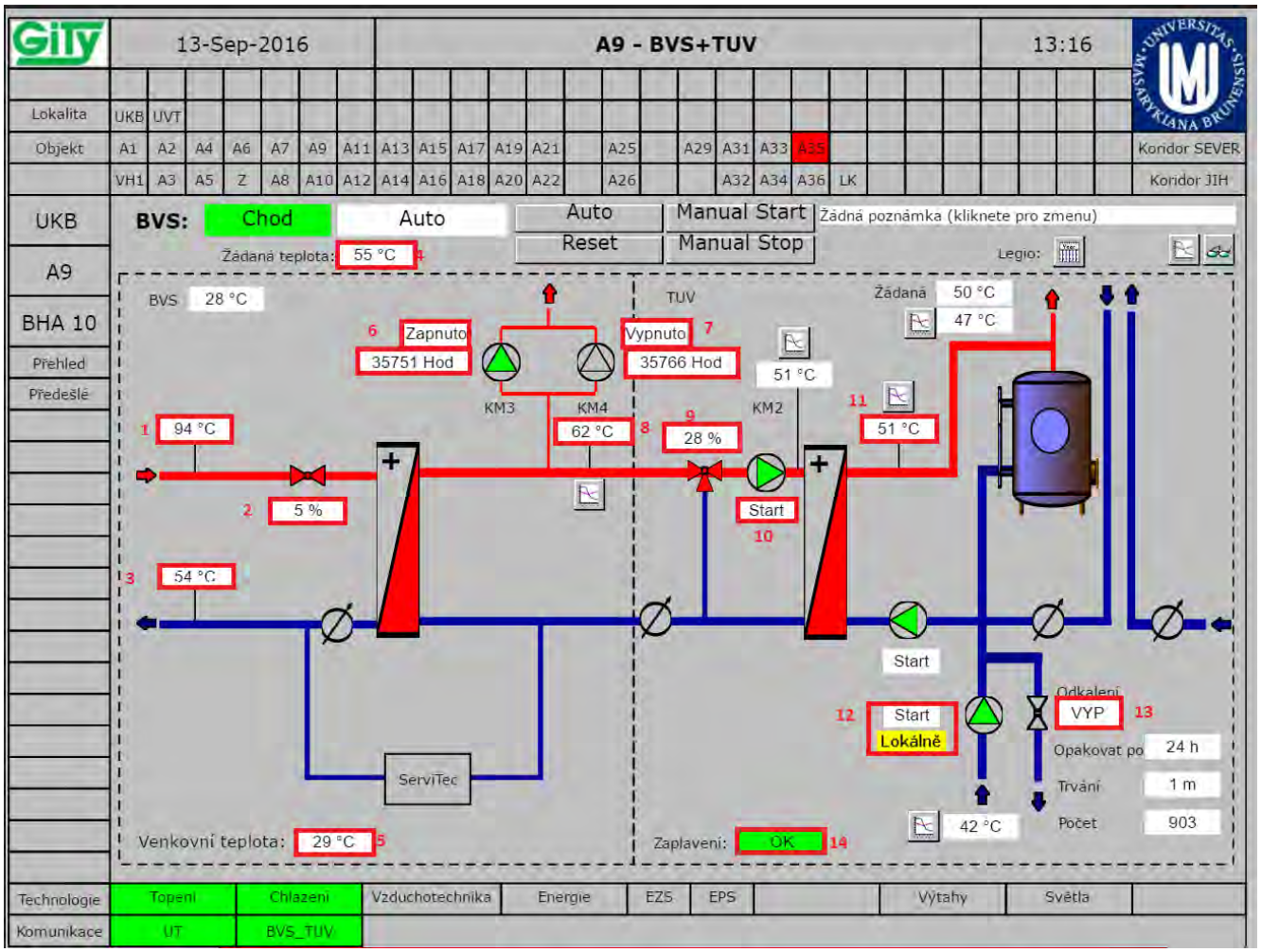
7.7.1 Symbolika zařízení

V obrazovkách HVAC (topení, vzduchotechnika, klimatizace. . .) se používají symboly definované v normě **ANSI/ASHRAE Standard 134-2005: Graphic Symbols for Heating, Ventilating, Air-Conditioning, and Refrigerating Systems** a/nebo symboly dle zvyklostí BMS MU. Pro označení potrubí lze alternativně (ke značení dle normy ANSI/ASHRAE Standard 134-2005) použít barevné rozlišení. Přívodní potrubí se značí zásadně plnou čarou, vratné potrubí se značí čárkovanou čarou.

7.7.2 Příklady obrazovek pro jednotlivé technologie

Přiložené obrazovky jsou příkladem obrazovek v systému ORCAweb (BMS MU). Je vyžadováno dodržení jednotného vizuálního stylu pro přehlednost a snadné ovládání obrazovek.

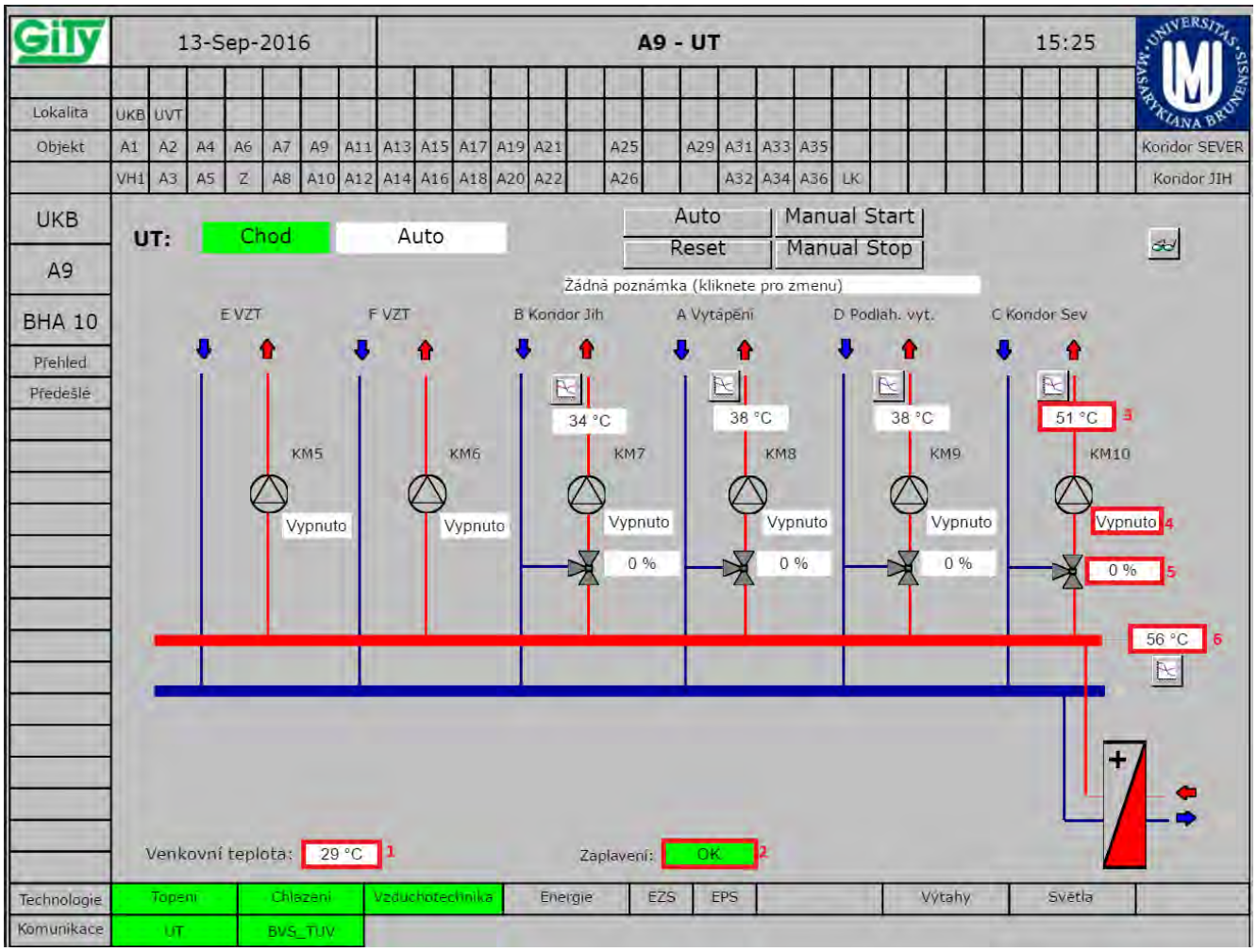
Příklad obrazovky Blokové výměníkové stanice



1. Teplota primární topné vody přivedené z horkovodu. Horkovod je veden z kotelny UKB do výměníkové stanice v suterénu objektu.
2. Procentuální vyjádření polohy kohoutu na horkovodu.
3. Teplota vratné vody z výměníkové stanice objektu do horkovodu.
4. Žádaná teplota sekundární topné vody pro účely vytápění.
5. Teplota z venkovního teploměru.
6. Informace o provozu čerpadla KM3 topné vody ÚT a VZT.
7. Informace o provozu čerpadla KM4 topné vody ÚT a VZT.
8. Teplota sekundární topné vody pro vytápění ÚT, TV a VZT.

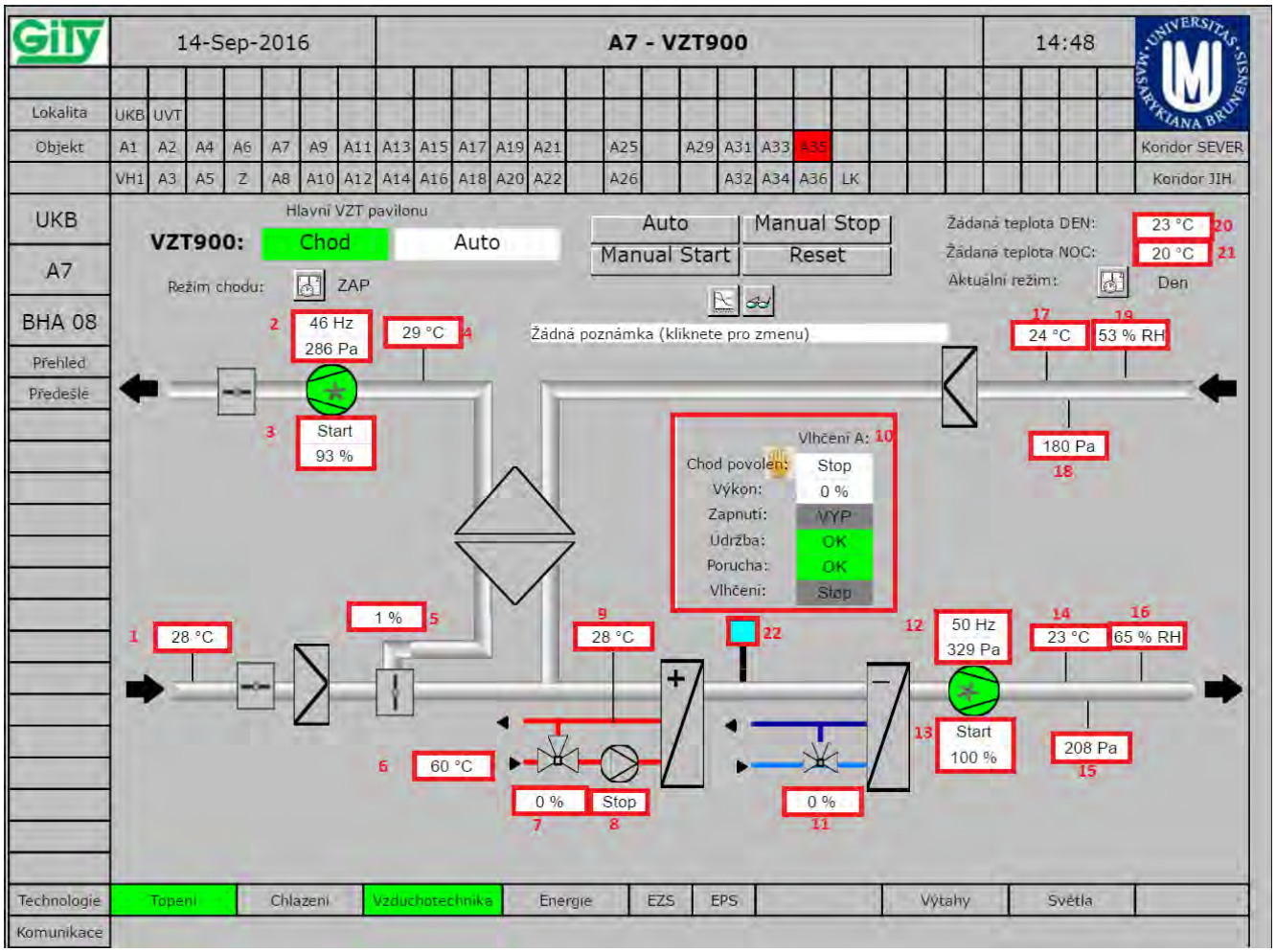
9. Procentuální vyjádření polohy směšovacího ventilu regulačního uzlu pro přípravu topné vody pro ohřev TV.
10. Informace o provozu oběhového čerpadla regulačního uzlu ohřevu TV.
11. Teplota ohřáté TV.
12. Informace o provozu oběhového čerpadla TV.
13. Procentuální vyjádření polohy ventilu odkalení.
14. Informace o stavu čidla zaplavení.

Příklad obrazovky Ústředního topení



1. Teplota z venkovního teploměru.
2. Informace o stavu čidla zaplavení.
3. Teplota topné vody směřující do topné větve.
4. Informace o provozu oběhového čerpadla regulačního uzlu.
5. Procentuální vyjádření polohy směšovacího ventilu na regulačním uzlu.
6. Teplota topné vody pro vytápění ÚT a VZT.

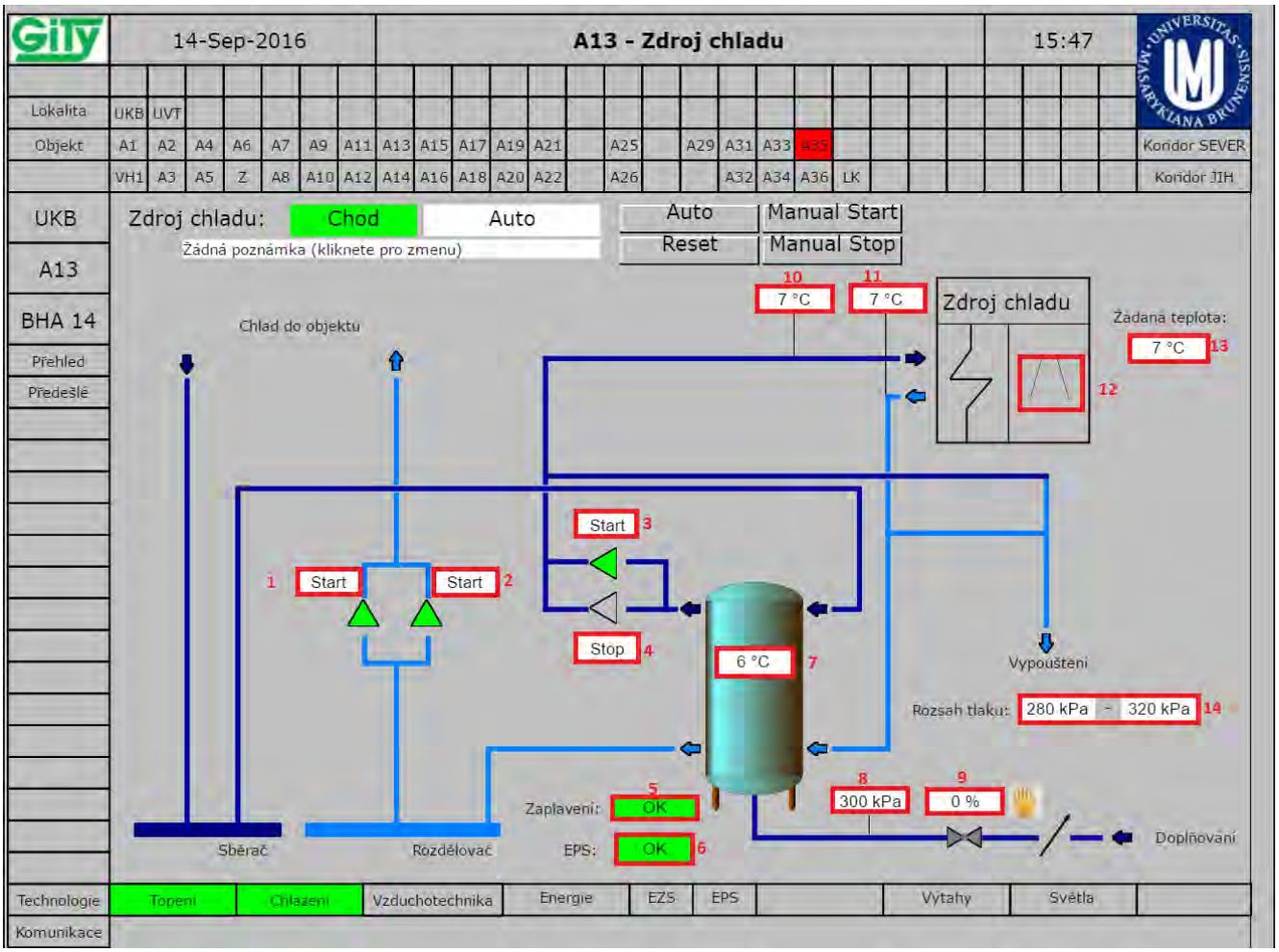
Příklad obrazovky Vzduchotechnické jednotky



1. Teplota přiváděného vzduchu do vzduchotechnické jednotky.
2. Pracovní frekvence motoru ventilátoru.
3. Procentuální vyjádření výkonu ventilátoru. Rozsah od 0% (minimum) do 100% (maximum). Informace o odtahovém ventilátoru. Ve stavu Start je ventilátor v chodu. Ve stavu Stop je ventilátor vypnut.
4. Teplota vzduchu po rekuperaci.
5. Procentuální vyjádření polohy ventilu přivádějícího vzduch do rekuperátoru.
6. Teplota vody přivedené do regulačního uzlu vzduchotechnické jednotky k ohřevu vzduchu.
7. Procentuální vyjádření polohy směšovacího ventilu na regulačním uzlu ohříváku.
8. Informace o provozu oběhového čerpadla na regulačním uzlu.

9. Teplota vratné vody za ohřívákem.
10. Informace o stavu a provozu zvlhčovacích jednotek.
11. Procentuální vyjádření polohy směšovacího ventilu na chladné vodě.
12. Pracovní frekvence motoru ventilátoru.
13. Procentuální vyjádření výkonu ventilátoru. Rozsah od 0% (minimum) do 100% (maximum). Informace o odtahovém ventilátoru. Ve stavu Start je ventilátor v chodu. Ve stavu Stop je ventilátor vypnut.
14. Teplota výstupního vzduchu ze vzduchotechnické jednotky.
15. Přetlak přiváděného vzduchu oproti tlaku vzduchu ve větraném prostoru.
16. Hodnota relativní vlhkosti vzduchu ze vzduchotechnické jednotky.
17. Teplota vzduchu na odtahu z větraného prostoru.
18. Podtlak odtahovaného vzduchu oproti tlaku vzduchu ve větraném prostoru.
19. Hodnota relativní vlhkosti na odtahu z větraného prostoru.
20. Požadovaná denní teplota výstupního vzduchu do větraného prostoru.
21. Požadovaná noční teplota výstupního vzduchu do větraného prostoru.
22. Informace o stavu čidla protimrazové ochrany.

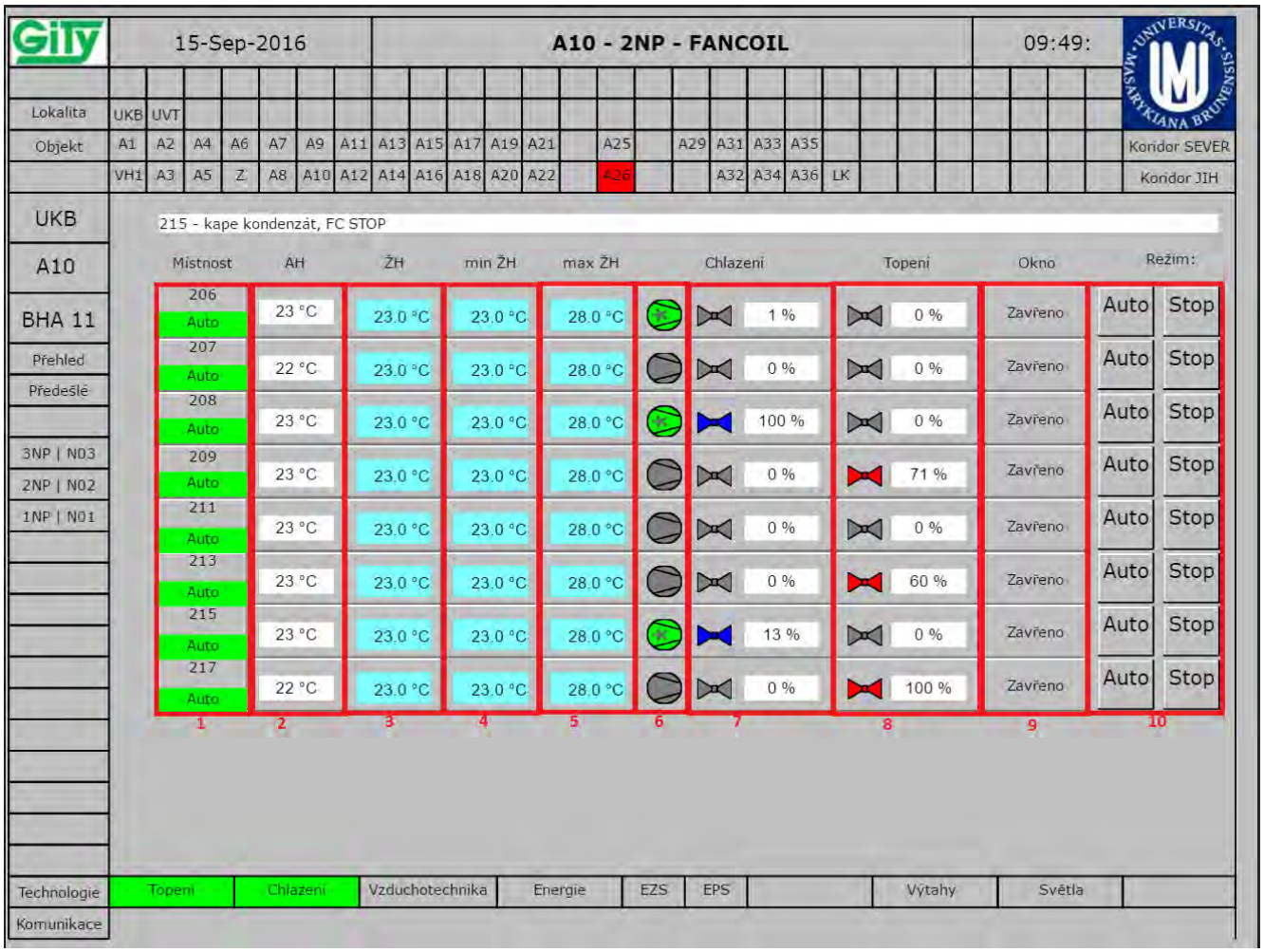
Příklad obrazovky Chladící jednotky



1. Informace o provozu sekundárního oběhového čerpadla chladné vody.
2. Informace o provozu sekundárního oběhového čerpadla chladné vody.
3. Informace o provozu primárního oběhového čerpadla chladné vody.
4. Informace o provozu primárního oběhového čerpadla chladné vody.
5. Informace o stavu čidla zaplavení.
6. Informace o stavu čidla EPS.
7. Teplota chladné vody v zásobníku.
8. Tlak vody.
9. Procentuální vyjádření polohy ventilu na vstupu vody pro doplňování do systému chlazení.

10. Teplota chladné vody na vstupu do zdroje chladu.
11. Teplota chladné vody na výstupu do zdroje chladu.
12. Informace o stavu zdroje chladu.
13. Požadovaná teplota zdroje chladu.
14. Informace o povoleném rozsahu tlaku v chladící soustavě.

Příklad obrazovky fan-coilových jednotek



1. Informace o režimu v jednotlivých místnostech.
2. Aktuální teplota v místnosti.
3. Žádaná hodnota v místnosti.
4. Minimální povolená hodnota teploty. Na ovladači v místnosti není možné nastavit nižší než minimální povolenou teplotu.
5. Maximální povolená hodnota teploty. Na ovladači v místnosti není možné nastavit vyšší než maximální povolenou teplotu.
6. Informace o provozu ventilátoru fan-coilové jednotky.
7. Informace o provozu systému chlazení. Modré podbarvení indikuje chod systému a šedé vypnutí systému. Dále je zde uvedeno procentuální vyjádření polohy ventilu chladící jednotky.

8. Informace o provozu systému topení. Červené podbarvení indikuje chod systému a šedé vypnutí systému. Dále je zde uvedeno procentuální vyjádření polohy radiátorové hlavice.
9. Informace o poloze okna. Při otevřeném okně je fan-coilové jednotce a systému topení blokován chod.
10. Ovládání fan-coilové jednotky je možné dvěma tlačítky. Tlačítko Auto nastaví fan-coil do automatického režimu. Tlačítko Stop vypne fan-coil.

7.8 Integrace s ostatními technologiemi

7.8.1 Přístupové systémy

V případech, kdy je dopředu známo obsazení prostor, je výhodné použít možnosti spuštění technologií v předstihu tak, aby při příchodu uživatele byla teplota prostředí již na ŽH. Čas předstihu musí být nastaven dostatečně dlouhý tak, aby bylo ŽH dosaženo včas, zároveň ale tak, aby nedocházelo k nehospodárnému zbytečně dlouhému chodu technologie. Nastavení délky tohoto předstihu by mělo být nejlépe dosaženo adaptivně na základě dat (trendů) z předchozích období.

8 Bezpečnostní systémy

Tato kapitola 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 používán 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 této kapitoly je stanovit jednotné požadavky na zabezpečovací a přístupové systémy (souhrnně zde nazvané jako bezpečnostní systémy) a rovněž definovat koncepci jejich provozu. Pro elektrickou požární signalizaci jsou doplněny požadavky na integraci do BMS MU.

8.1 Komunikační protokoly

Tato kapitola se zabývá popisem prostředků protokolu BACnet, které jsou použity při implementaci požadované funkcionality uvedené v části 8.2.

8.1.1 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;
- 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.

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

8.1.2 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.

8.1.3 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.

8.1.4 Vzdálené ovládání systémů

Bezepčnostní systémy mohou být ovládány v následujících režimech:

- 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`;

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

- 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 dále) 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.

8.1.5 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);
- 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 část 8.3.1.

8.2 Definice rozhraní s BMS

Následující část 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 kapitole „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.

8.2.1 Předávaná data a funkce systému

V následujících částech jsou popsány data a funkce, které musí bezpečnostní systémy PZTS a EKV 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 vybavit vhodným integračním zařízením (např. **Delta Controls eBMGR**, **Delta Controls eBCON**, integrační zařízení musí projít testováním kompatibility v laboratoři BMS), které schopnosti systémů rozšíří o požadované funkce.

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];
- 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] Může být nahrazen tzv. stavem „dveří“, pokud je čidlo nebo zámek součástí takového celku (viz dále)
[4] Může být nahrazeno stavem integrovaného přístupového bodu, pokud je zóna nebo zámek součástí takového celku (viz dále)

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].

Společné (Integrovaný PZTS + EKV)

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).

EPS

Data:

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

8.3 Trendování

Vytvoření trendlogů je realizováno v prostředí BMS MU dle požadavku na konkrétní realizaci a řídí se běžnými požadavky na trendování (viz část 2.13), standardně trendování provozních stavů neprobíhá. Vzhledem k výčtu prvků, jejichž stavy mají být předávány do BMS MU (viz část 8.2), je možné trendovat libovolný fyzický či virtuální prvek systému.

8.3.1 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 části 8.1.5.

Pro potřeby zabezpečovacích a přístupových systémů rozeznáváme tři 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.).

8.4 Popis uživatelského rozhraní v BMS MU

Systémy PZTS, EKV i EPS je třeba integrovat do BMS MU včetně vytvoření příslušných obrazovek. Pro EPS pak platí požadavek na jednosměrnou integraci, ostatní zůstává část 8.11. 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, apod., 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:

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

Pro prvky PZTS a EKV jsou stanovené barevné kódy jednotlivých stavů znárorněny v následující tabulce:

ID	stav	barva		RGB
1	(stav neznámý)	bílá		255,255,255
2	neaktivní	šedá		128,128,128
3	aktivní	zelená		0,128,0
4	zastřeženo	světle modrá		0,128,255
5	přemostěno	purpurová		255,0,255
6	sabotáž/porucha	žlutá		255,255,0
7	poplach	červená		255,0,0
8	byl poplach	růžová		255,128,128
9	zavřeno + zamčeno	fialová		128,0,255
10	zavřeno + odemčeno	azurová		0,255,255

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:
    - Má právo prohlížet objekty (obrazovky) na jemu příslušné skupině obrazovek/zařízení;
    - Má právo prohlížet alarmy na jemu příslušné skupině obrazovek/zařízení.
2. Ostraha:
    - Má právo zastřežovat a odstřežovat zóny na jí příslušné skupině obrazovek/zařízení;
    - Má právo potvrzovat alarmy na jí příslušné skupině obrazovek/zařízení.
3. Správa budovy:
    - Má právo přemosťovat objekty a zóny na jí příslušné skupině obrazovek/zařízení;
    - Má právo nastavovat režim přístupových bodů na jí příslušné skupině obrazovek/zařízení.
4. Administrátor:
    - Má prohlížet a ovládat všechny objekty a zařízení;
    - Spravuje práva ostatních uživatelů.

8.5 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. Dodány budou akumulátory určené pro provoz s PZTS (EKV, EPS).

Napájení bude navrženo tak, že maximální odběr připojených zařízení bude činit nejvýše 60 % výkonu zdroje.

8.6 Integrace s univerzitní správou identit

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.

8.6.1 Pojmy

Následují definice základních používaných pojmů:

- **Lidé** – Jsou v systému evidováni se svým Univerzitním číslem osoby (UČO).
- **Karty** – Jeden člověk může mít nejvýše jednu aktivní (= nezrušenou) kartu.

- **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...).

8.6.2 Skupiny a EKV

Pro integraci skupin v ISu MU a systému EKV platí následující:

- 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.

8.6.3 Komunikace se serverem

Pro komunikaci systému EKV a IS MU platí následující:

- Server na straně IS MU se jmenuje 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.

8.6.4 Export osob a externistů k dané skupině osob

Pro export osob z ISu MU platí následující:

- 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 používá jako oddělovač 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:

```
1337;;08084554c0;"RNDr. Hugo Kokoška"
27380;;08065f0de1;"Adolf Havlík"
;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.

8.6.5 Import údajů o průchodech

Pro import údajů o průchodech platí následující:

- 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>
```

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.

8.6.6 Kontakt

Vývojový tým Informačního Systému MU: iscor@fi.muni.cz

8.7 Provozní (funkční) požadavky

Provozní požadavky se vztahují na fungování systému při běžném provozu. Vymezují potřebnou funkcionalitu ve vztahu k uživateli systému.

8.7.1 EKV

Pro systém EKV se jedná o následující:

- Integrace s BMS MU -– 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 2s;
- 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 s tisknutým tlačítkem/zastřežení místnosti (viz část 8.10 – 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).

8.7.2 PZTS

Pro systém PZTS se jedná o následující:

- Integrace s BMS MU – sledování stavu periferií a sledování a ovládání stavu systému (viz část 8.2);
- Integrace se systémem EKV (viz část 8.10).

8.7.3 EPS

Pro systém EPS se jedná o následující:

- Integrace s BMS MU – sledování stavu periferií a sledování a ovládání stavu systému (viz část 8.2).

8.8 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...).

8.8.1 Struktura a správa práv

Zabezpečovací a přístupové systémy (či spíše jejich provoz) jsou ovlivněny množstvím různých vstupních bodů, prostřednictvím kterých může být ovlivněno jejich chování. Následuje výčet možných vstupních bodů:

1. IS:
   - Práva na správu skupin osob;
   - Práva na zavádění/přidělování karet (externistům);
   - Další práva v ISu (definice skupin osob...).
2. Převodník, softwarové nástroje:
   - Přístup do převodník pro synchronizaci s IS (OS, aplikace);
   - Přístup do ústředny přes konzoli (technik);
   - Přístup do převodník BACnet (OS, aplikace).
3. Technologická síť MU:
   - Přístup přes nástroj pro přímý přístup do sítě (typicky ORCAview);
   - Přístup přes Webové Rozhraní BMS MU;

- Jiný přístup přes technologickou síť (SW dalších výrobců, vlastní SW).

4. Fyzický přístup:
   - Lokální kódy (uživatelské, Master a Technik);
   - 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):
   - Změna veškerých přístupových údajů ve všech uvedených bodech;
   - Uchování těchto údajů ve vyčleněném, zabezpečeném dokumentu – administrátorská dokumentace;
   - Tyto účty nebudou nadále určeny pro běžný provoz, pouze pro řešení havarijních situací;
   - 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:
   - Pokud nebyly dosud vytvořeny, provést nyní a provádět nadále potřebné operace (včetně provozu služeb apod.) pod těmito účty;
   - Uchování těchto údajů v administrátorské dokumentaci.

Skupina oprávnění 3 je v kompetenci Garanta, dodavatel do technologické sítě nemá přístup. Platí pravidla pro provoz TeNe MU.

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, 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.

8.8.2 EKV

Dodatečné požadavky pro správu systému EKV jsou následující:

- 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.

8.8.3 PZTS

Dodatečné požadavky pro správu systému PZTS jsou následující:

- 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.

8.8.4 EPS

Dodatečné požadavky pro správu systému EPS jsou následující:

- 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.

8.9 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.

8.9.1 Veřejné prostory

Charakteristika:

- 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.

8.9.2 Společné prostory MU

Charakteristika:

- 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.

8.9.3 Knihovny

Charakteristika:

- sleduje se příchod i odchod;
- může jít o prostory s větší kapacitou osob, ale zároveň 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 v případě narušení dveří pro okamžitou detekci).

8.9.4 Auly, velké posluchárny

Charakteristika:

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

8.9.5 Uzavřené chodby

Charakteristika:

- 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.

8.9.6 Učebny

Charakteristika:

- 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.

8.9.7 Laboratoře, specializované učebny

Charakteristika:

- 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.

8.9.8 Technické místnosti mimo SLP rozvodny

Charakteristika:

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

8.9.9 SLP rozvodny

Charakteristika:

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

8.9.10 Prostory s auty – parkoviště, garáže, koridory

Charakteristika:

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

8.9.11 Další

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.

8.10 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:

8.10.1 Chodba

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.

8.10.2 Laboratoř/počítačová učebna

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.

8.10.3 Učebna

Prostor je odstřežován a zastřežován vzdáleně nebo automaticky (obsluhou BMS, časovým plánem). 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 k odchodové čtečce/přiložení karty se současným stiskem tlačítka;
  - Změně režimu na **Mimo výuku**;
  - Zastřežení místnosti.

8.10.4 Zastřežovaná učebna

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 k odchodové čtečce/přiložením karty a stisknutím odchodového tlačítka dojde k uzamčení zámku.

8.10.5 Uzavřená chodba s laboratořemi

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.

8.11 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 MU je výhradně jednosměrná, z EPS jsou přenášeny a dále zpracovány informace prostřednictvím převodníku. Ústředna EPS je umístěna v rozvodně SLP.

8.12 Dokumentace

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

8.12.1 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.

8.12.2 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.).

8.12.3 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.

9 Kamerový systém - CCTV

Hlavním důvodem pro nasazení kamerového systému je kontinuální monitorováním vstupů objektů a uzlových komunikačních bodů, sledování určených místností, případně zajištění ostrahy objektů za účelem ochrany investic a bezpečnosti osob. Systém zajišťuje předávání aktuální obrazové informace na centrální dispečink a/nebo případná další vyhrazená pracoviště; současně se uchovává záznam obrazu pro případ vyhodnocení možné mimořádné události. Shrnuto - kamerový systém zajišťuje centrální jednotný dohled nad důležitými prostorami a archivaci obrazových dat.

Kamerový systém je postaven na **čistém IP řešení**, komunikační prostředí je strukturovaná kabeláž. Pouze v případě nahrazení analogové CCTV technologie, kdy je obtížná instalace nového UTP kabelu, lze využít stávající koaxiální rozvody za použití vhodného převodníku. Toto řešení však musí být odsouhlaseno Garantem.

Pokud je již v lokalitě provozován kamerový systém, dodávka a instalace znamená jeho rozšíření, pokud není v zadávacích podmínkách uvedeno jinak (např. nahrazení technicky a morálně zastaralého analogového systému).

9.1 Definování systému CCTV

Obecné požadavky na technologii kamerového systému:

- Celý systém je postaven na čistém IP řešení. Výjimkou mohou být rekonstrukce stávajících analogových systémů, kdy je v některých případech možné využít instalované analogové kamery za použití vhodného encoderu (není doporučeno).
- Navržený systém nabízí flexibilní licenční strukturu, podporující růst systému dle potřeb uživatele.
- Systém dovoluje souběžný provoz připojených klientských stanic v počtu dle zadání uživatele.
- Systém podporuje multi-klientové a multi-serverové řešení.
- Podpora systémové integrace s ostatními bezpečnostními systémy.
- Kompatibilita s IP video produkty nejrozšířenějších jiných výrobců.
- Systém je založen na otevřených standardech (případně tyto standardy podporuje, i když má pro homogenní systém vlastní proprietární řešení); primární je podpora standardu ONVIF.
- CCTV systém nabízí spolehlivost, robustnost a stabilní výkon.
- Flexibilní vzdálený přístup klientů.
- Možnost centrální jednotné správy systému.
- Centralizované řešení.

- Navržený CCTV systém umožňuje postupné rozšiřování dle rostoucích potřeb uživatele.
- Nutná podpora multicastového provozu - i když nebude implementována při prvotní instalaci kamerového systému. Toto řešení souvisí s podporou v celém systému, proto je nutná funkcionalita i na straně síťových zařízení.

9.2 Podrobnější systémové požadavky

- V případě nově instalovaných CCTV systémů vzít v úvahu i budoucí rozvoj areálu a nabídnout nadčasové řešení, tj. aby v další etapě výstavby nebylo nutné přecházet na vyšší SW verzi CCTV systému. Z tohoto pohledu hned z počátku škálovat i server. Tento požadavek bude konzultován s Garantem.
- Server clustering, pro ukládání záznamu podpora SAN, NAS, DAS, RAID úložiště.
- Podpora multicastové komunikace, QoS.
- Licencování i po jednotlivých kamerách.
- Nelicencovaní klienti.
- Podpora kompresních formátů videa MJPEG, MPEG4, H.264 (primárně).
- Plná podpora megapixelových a HD kamer.
- Možnost uživatelského exportu videa/obrázků jednotlivých kamer z historických dat.
- Možnost nastavovat dobu záznamu, kvalitu, typ komprese pro každou kameru zvlášť.
- Uživatelská práva pro přístup k obrazu jednotlivých kamer, a to z hlediska reálného obrazu, záznamu a nastavení.
- Možnost předdefinování pohledů (multiscreenů) pro jednotlivé uživatele/skupiny uživatelů, možnost individuálních a sdílených pohledů.
- Neomezené (míněno softwarově) klientské více obrazovkové zobrazení nebo virtualní matice.
- VMD zónová analýza v záznamu.
- Podpora objektové analýzy obrazu - minimálně VMD (detekce pohybu), záznam řízen kamerami.
- Definice pre/post alarm záznamu s možností zvýšení kvality obrazu a snímkové frekvence.
- Podpora PTZ kamer.
- Podpora ovládání vstupů/výstupů na kamerách/enkodérech.
- Hlášení poruch kamer (odpojení od komunikační sítě, napájení) – mail, SNMP.
- Možnost automatické archivace dat.
- Řízení uživatelských účtů pomocí AD, LDAP.

9.3 Požadavky na hardware

Pro HW systému CCTV jsou stanoveny následující požadavky:

9.3.1 CCTV server

Při návrhu hardwarové architektury serveru vzít do úvahy možné budoucí rozšiřování CCTV systému (např. v další etapě rekonstrukce areálu) a minimalizovat celkový počet serverů a tím nároky na prostor a chladící výkon ve SLP rozvodně - nutná konzultace s Garantem. Obecně viz 2.2.

- Provedení: RM 19";
- Výkon dle počtu kamer — počítat s možným rozšířením a nárůstem fps;
- Minimální počet současných klientů: 10;
- Redundantní napájecí zdroj;
- Konektivita: 4x Ethernetový interface 1000Base-T.

9.3.2 Datové úložiště

Redundantní úložiště zapojené v RAID 1, případně RAID 5 Velikost diskového prostoru je uvažována pro 7 denní záznam – 12fps, Full HD x počet kamer + nutná rezerva odsouhlasená Garantem

9.3.3 CCTV klient

Minimální požadavky na klientské PC vycházejí z následujícího:

- PC o výkonu potřebném pro provoz pro navržený počet kamer (vzít v úvahu fps a rozlišení), 3-4x monitor s digitálním rozhraním;
- Monitory: LCD monitor, úhlopříčka min. 19", rozlišení min. Full HD antireflexní, DVI/HDMI/DP, vč. potřebné montážní konstrukce;
- Konektivita: 1x 1000Base-T;
- Podpora multicastové komunikace.

9.3.4 Aktivní prvky

Přepínač zvolit dle 4.1.2, **navíc PoE (802.3af)**, případně PoE+ (802.3at), multicast IGMP snooping a prioritizace (QoS)

9.4 Kamery

Při realizaci kamerového systému je nutné řídit se následujícími zásadami:

- Umístění kamer se zřetelem k zvýšenému pohybu osob - sledování vchodů, křížení chodeb. Sledování přístupu do důležitých a vyhrazených místností.
- **Používat megapixelové a HD kamery s vhodnými objektivy.**
- V prostředí MU je vhodnější instalace dvou kamer „zády k sobě“, případně panoramatické kamery, než užití PTZ kamery - většinou kamera neustále sleduje stejné místo.
- **Používat kamery s IR přísvitem**, eliminuje se tím nepřetržitý noční záznam, kdy převládá v obraze šum, který je mylně vyhodnocen jako pohyb.

9.5 Napájení

Všechny prvky CCTV jsou napájeny z rozvodů 1. kategorie (VDO). Více viz kapitola 5.2.1.

9.6 Integrace systémů CCTV a BMS MU

Přenos okamžité obrazové informace (video streamu) z jednotlivých kamer (případně DVR serveru, pokud tuto funkcionalitu podporuje) do systému BMS MU je realizován překladem adres funkcí `PAT (Port Address Translation)`. Počítače z „akademické“ datové sítě MUNI tedy komunikují pouze s jednou veřejnou IP adresou, IP adresy kamer nejsou pro vnější uživatele dostupné. Překlad se v případě možnosti provádí přímo na DVR serveru, jinak je pro lokalitu nutné dodat zařízení s touto funkcionalitou.

Preferované je připojení kamer do technologické sítě MUNI (TeNe), kde je **pro CCTV systém rezervována VLAN 13**. Zde je bezpečnost řešena centrálně přístupem přes firewall, který je ve správě ODS ÚVT. V případě připojení CCTV systému do datové sítě MUNI je nutné **řešit bezpečnost samostatně v rámci lokality, nutný je souhlas Garanta**. Na příslušné obrazovce systému BMS MU s dispozicí podlaží budovy je umístěna ikona kamery, odkazovaný link adresuje příslušný (PAT) server, na kterém se překlad realizuje, spolu s číslem IP portu, který jednoznačně určuje konkrétní kameru. Pro zobrazení video streamu je nutné do prohlížeče instalovat vhodný plugin (např. VLC).

Jen vyhrazení uživatelé BMS MU mají oprávnění sledovat obraz z kamer. Např. v rámci UKB se uživatel autentizuje v doméně BMS, jejich oprávnění je dáno členstvím v příslušné skupině uživatelů domény. Dle skupiny získá uživatel právo sledovat obraz kamer v dané lokalitě, případně ovládat nastavení PTZ kamer. Do budoucna se předpokládá autentizace oprávněných uživatelů v centrálním systému MU (s použitím identit MU).

Celý CCTV systém (server i kamery) se časově synchronizuje na určeném NTP serveru (např. v rámci UKB na doménovém kontroléru BMS).

10 Výtahy a osvětlení

Tato kapitola se věnuje technologiím výtahů a osvětlení, které jsou integrovány v BMS MU.

10.1 Výtahy

Výtahy musí nadřazenému systému poskytovat potřebná data o poruše výtahu s detailnější informací o typu poruchy nebo provozním stavu výtahu. Informace může být ve formě diskrétních binárních signálů na výstupních portech řídicího systému výtahu. Informace o provozním stavu je možné předat nadřazenému systému i s využitím doporučených komunikačních protokolů a zajištění GW do BACnetu.

10.2 Osvětlení

Osvětlení společných prostor musí být možné ovládat vzdáleně časovým programem a musí být možné vzdáleně na povel obsluhy rozsvítit nadřazeným signálem. Pro řízení osvětlení platí příslušný odstavec v kap. 6.4

11 Seznam příloh

K této Metodice náležejí následující přílohy, nacházejícíc se v samostatných dokumentech:

- Příloha A – Metodika Testování zařízení pro BMS MU.
- Příloha B – Metodika Připojování nových zařízení do BMS MU.
- Příloha C – Metodika Správa vizualizačních obrazovek BMS MU.
- Příloha D – Tabulka Standardů místností.

SPRÁVA UNIVERZITNÍHO
KAMPUSU BOHUNICE
Masarykova univerzita

Metodika
Testování zařízení pro BMS MU

SUKB MU

12. července 2018

Obsah

Cíl metodiky

Cílem této metodiky je popsat testovací proceduru pro zařízení, které mají být připojeny do BMS MU a Technologické sítě MU (TeNe MU) a tím upřesňuje požadavky na testování kompatibility z [2]. Před připojením jakéhokoliv zařízení do BMS MU a TeNe musí být pro dané zařízení prokázáno pomocí „Protokol o testování zařízení pro BMS MU“, že toto zařízení je kompatibilní s BMS MU a TeNe a že jeho připojení by nemělo mít negativní vliv na dosavadní BMS MU a TeNe. Tím však není zodpovědnost za jakékoliv problémy způsobené tímto zařízením přenesena na MU, za všechny problémy související s tímto zařízením je zodpovědný zhotovitel.

1 Prerekvizity

Pro zahájení testování v Laboratoři BMS MU je nutné splnit následující podmínky:

1. Uvést přesnou identifikaci testovaného zařízení (výrobce, typ, firmware, revize HW, ...).
2. BTL Mark - je nutné doložit testování v BACnet® Testing Laboratory a zařízení musí dle protokolu splňovat požadavky dle této metodiky.
3. PICS - je nutné doložit dokument PICS a zařízení musí dle protokolu splňovat požadavky dle této metodiky.
4. Konfigurace zařízení - zařízení musí být předem dodavatelem nakonfigurováno tak, aby bylo možné bez zásahu do konfigurace zařízení otestovat všechny body této metodiky. Síťová nastavení, příjemce v EVC apod. na požádání dodavateli předá zástupce MU.
5. Účel zařízení - pro potřeby testování je nutné znát účel a způsob použití daného zařízení (např. kontrolér pro řízení fancoilu a radiátoru, volně programovatelný kontrolér, gateway pro překlad z jiného protokolu, měřič spotřeby, ...), v souvislosti s účelem použití bude dané zařízení testováno.

2 Podpora objektů

2.1 Seznam vyžadovaných objektů

Je nutné zkontrolovat, zda testované zařízení podporuje následující objekty:

1. AV
2. AI
3. AO
4. BV
5. BI
6. BO
7. CAL
8. SCH
9. MV
10. MI
11. BT
12. AT
13. TL
14. EV
15. EVC
16. DEV

U každého objektu je nutné zkontrolovat, zda je možné z něj číst data, zapisovat (minimálně) present-value, zda je objekt funkční (dle svého určení), zda nechybí některé důležité vlastnosti a zda implementace odpovídá [1].

Výjimky jsou přípustné pouze pokud je možné chybějící objekt plnohodnotně nahradit jiným z objektů nebo v případě specifického určení daného zařízení; v obou případech je nutný písemný souhlas zástupce investora.

2.2 Stavové texty objektů

U všech stavových objektů (BV, BI, BO, MV, MI, příp. MO) musí být možné nastavit vlastní stavové texty.

2.3 Inženýrské jednotky

U všech analogových objektů (AI, AV, AO) musí být možné nastavit vlastní inženýrské jednotky, nebo inženýrské jednotky implementované v zařízení musí odpovídat definici **BACnetEngineeringUnits** dle [1].

2.4 Vícestavové objekty

U objektů typu MV, MI, příp. MO je nutné otestovat, zda může `present-value` nabývat hodnoty mimo `state-text`. Často se může vyskytovat „0“ - například při výpadku komunikace. Toto chování je v rozporu s [1]. Zejména je nutné toto otestovat u zařízení, která se mohou chovat jako GW pro překlad jiných protokolů na BACnet (při výpadku komunikace nižšího protokolu může nastat problém).

2.5 Trendlogy

Trendlogy musí umožňovat ukládání dle předpisu COV (inkrement dle sledované proměnné, nastavitelný), POLL (nastavitelný minimálně v rozsahu 1s - 24h). Trendlogy typu POLL se musí ukládat tak, že počátek trendování je přesně půlnoc (0:00:00), tzn. 24h trendlog se ukládá vždy o půlnoci, 1h trendlog se ukládá vždy v celou hodinu, 15m trendlog se ukládá v časech [XY:00;XY:15;XY:30;XY:45] atd. Je nutné ověřit, zda trendlogy fungují korektně a přesně (jak POLL, tak i COV).

2.6 COV změny

Všechny objekty musí podporovat COV subscription dle [1].

2.7 Názvy objektů

Názvy všech objektů musí být volně konfigurovatelné s dostatečnými možnostmi délky textu pro danou aplikaci (např. minimálně 70 nebo nejlépe 255).

2.8 Ruční režim

Po přepnutí objektu na „Manual“ nebo „Manual Value“ se musí stav (Out of Service, Manual) zapsat do odpovídající property a musí být zpětně čitelný.

3 Podpora služeb

Je třeba ověřit, které služby zařízení podporuje (porovnat PICS, [1] a reálnou funkčnost). Nutnost podpory jednotlivých služeb závisí na účelu daného zařízení, na jeho profilu dle [1, Annex L] a zejména na požadavcích objednatele.

4 Časová synchronizace

1. Zařízení musí být schopno akceptovat nastavení času po BACnetu
2. V jednom okamžiku musí zařízení používat pouze jednu ze služeb BACnet pro časovou synchronizaci.
3. Záznamy o synchronizaci času se musí ukládat do trendlogů, avšak pouze pokud došlo k významnému posunu času. Naopak bezvýznamné časové posuny se do trendlogů nesmí ukládat.
4. Pokud je možné k danému zařízení připojit další zařízení po MSTP, musí zařízení umožňovat distribuci času pro připojená zařízení.

5 Síťové vlastnosti

5.1 BACnet ID

BACnet ID zařízení musí být volně konfigurovatelné v rozsahu dle [1].

5.2 BBMD device

Pokud je vyžadováno konfigurací sítě, musí dané zařízení podporovat BBMD device. Je nutné zkontrolovat, jestli nepropaguje BBMD devices tabulku po celé síti, což je v rámci BMS MU neakceptovatelné chování.

5.3 BACnet port

Pokud dané zařízení podporuje BACnet over IP, musí být možnost změnit port (z 47808 na libovolný jiný).

5.4 Podpora BACnet sítí

Číslo BACnet sítě (sítí) daného zařízení musí být konfigurovatelné. Pokud zařízení umožňuje překlad mezi různými typy sítí (BACnet IP, BACnet ethernet, BACnet MS/TP,...), je nutné tyto funkce ověřit (včetně alarmů,...). Dále je nutné ověřit, zda je možné tyto sítě (nebo překlad mezi nimi) deaktivovat.

5.5 Archivace dat

Ověřit ukládání do Historianu - v databázi musí být vyplněny alespoň nejdůležitější sloupce (identifikace sledovaného objektu ID, počty záznamů, log interval). Všechny trendlogy musí mít nadefinovanou EVC pro reporting (Buffer_ready) a ostatní nastavení funkce reporting musí být uvolněno pro zápis ze strany Historianu (zapnutí/vypnutí reportingu, Threshold,...).

6 Zálohování a obnovení

6.1 SW pro zálohu a obnovení

K zařízení musí být k dispozici SW pro zálohování a obnovení konfigurace a SW zařízení. SW musí umožňovat automatické zálohy nebo hromadné zálohování všech zařízení v síti.

6.2 Nový build SW

Po přehrání software v zařízení (rebuild,...) musí zůstat zachovány shodné ID BACnet objektů, nastavené archivování Historianem, příjemci v EVC a obsah provozních dat (AV, BV, MV, CAL, SCH,...).

6.3 Paměť zařízení

Zařízení musí být vybaveno nevolatilní pamětí, z které po výpadku napájení nastartuje s aktuální konfigurací a SW. Během výpadku napájení nesmí dojít k žádné ztrátě dat (kromě záznamů v trendech, které by se měly uložit po dobu výpadku).

7 Alarmy

7.1 Alarmové texty

Alarmové texty musí být volně konfigurovatelné, včetně diakritiky. Jsou vyžadovány alarmové texty pro přechody do stavů OffNormal, Fault, Normal, Low_limit, High_limit.

7.2 Event class

1. V Event classách (EVC) musí být možné nastavit příjemce (BROADCAST nebo jednotlivá BACnet zařízení). Je nutné mít možnost nastavit příjemce na IP, ethernetu i dle čísla BACnet sítě.
2. Číslo EVC (1600.EVC**25**) musí být volně nastavitelné.

8 Ostatní nalezené problémy

V průběhu testování se mohou objevit problémy, které tato metodika nepostihuje, avšak tyto problémy mohou být překážkou pro připojení a provozování testovaného zařízení v BMS MU. Může se jednat např. o fyzické provedení daného zařízení, problémy se SW dodaným k zařízení, jakékoliv skutečnosti neodpovídající [1] a jakékoliv nekompatibilní chování vůči ostatním zařízením BMS MU.

Literatura

[1] ČSN EN ISO 16484-5: *Automatizační a řídicí systémy budov - Část 5: Datový komunikační protokol.* Praha, 2012.

[2] Správa univerzitního kampusu Bohunice MU, Ústav výpočetní techniky MU, GiTy: *Metodika Nasazování a úpravy komponent BMS MU.* 2013.

SPRÁVA UNIVERZITNÍHO
KAMPUSU BOHUNICE
Masarykova univerzita

Metodika
Připojování nových zařízení do BMS MU

OFM SUKB MU

12. července 2018

Obsah

1 Cíl metodiky

Cílem této metodiky je popsat způsob připojování nových zařízení do BMS MU a do Technologické sítě MU (dále TeNe MU). Metodika definuje dokumenty a přílohy, kterými je nutné doložit, že připojované zařízení nebude mít negativní vliv na stávající části BMS MU a TeNe MU.

2 BACnet zařízení

BACnet zařízeními rozumíme všechna zařízení, která po síti komunikují tímto protokolem, typicky kontrolery (automaty, regulátory), převodníky pro převod z jiných protokolů, uživatelské stanice, servery a další.

2.1 Prerekvizity

Nutnými prerekvizitami jsou:

1. PICS (BACNET PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT)
2. Protokol o testování daného zařízení v Laboratoři BMS MU
3. Aktuální projektová dokumentace MaR a BMS (stupeň RD nebo DSPS)

Tyto dokumenty jsou nutnými předpoklady pro zahájení připojování daného zařízení, bez nich není možné zařízení do BMS MU a TeNe MU připojit.

2.1.1 Výchozí konfigurace

Před zahájením připojování jakýchkoliv zařízení do TeNe MU musí být splněny následující podmínky:

1. V lokalitě je vytvořena izolovaná síť (podsíť, VLAN), zařízení z této sítě nemají možnost komunikovat se zařízeními v TeNe MU (nejsou nastavené routy; fyzicky jiné switche apod.)
2. Všechna zařízení jsou připojena k izolované síti, zapnutá a komunikují

2.2 Kontroly před připojením

Při zahájení připojování daného zařízení je nutné postupovat dle postupu popsaného v této kapitole, výsledky jednotlivých testů a zkoušek je nutné zaznamenávat do protokolu a případné datové výstupy (reporty, tabulky apod.) připojit jako přílohu k tomuto protokolu.

Pro kontrolu některých nastavení jsou předpřipraveny reporty, je nutné je vložit do ORCAview (pravým tlačítkem na PC ve stromu zařízení, „Load. . . “) a následně spustit. Pro korektní uložení výsledku reportů je nutné vytvořit na disku C:\složku „tmp“ (aby bylo dostupné umístění „C:\tmp“). Pokud není možné pomocí těchto reportů požadovaná data vyčíst z připojovaných zařízení, je nutné toto zapsat do protokolu a doložit jiným způsobem správnost těchto nastavení.

2.2.1 Připojovaná zařízení

Spustit report „Kontrola_zarizeni“, jeho výsledek uložit jako přílohu 1 a zkontrolovat:

1. Zda počty a typy zařízení odpovídají projektové dokumentaci (zejména výkaz výměr a topologie MaR(BMS)), zároveň žádné zařízení nepřebývá, nechybí, nebude se připojovat „až někdy“ apod.
2. Zda pro všechny typy zařízení vypsaných reportem jsou doloženy povinné prerekvizity (PICS, protokol o Testování v Laboratoři BMS MU)
3. Zda jsou správně nastavena DEV_ID jednotlivých zařízení (dle **Metodiky Nasazování a úprav komponent BMS MU**)
4. Zda jsou všechna zařízení pojmenována dle Jmenné konvence nebo podle pokynů Garanta.
5. Zkontrolovat počet resetů - vysoký počet může znamenat poškozený kontroler nebo problém v SW
6. Zkontrolovat, zda zařízení mají vyplněno pole Location (mělo by obsahovat polohový kód, případně včetně upřesnění)

2.2.2 Síťová nastavení

Spustit report „Sitova_nastaveni“, jeho výsledek uložit jako přílohu 2 protokolu a zkontrolovat:

1. Zda jsou vypsána všechna připojovaná zařízení
2. Pokud se ve výpisu vyskytuje „0“ - zda je to port LINKnet
3. DSC/RTR: oba MSTP porty musí mít adresu sítě 20000 + (DEV_ID/100) nebo 50000 + (DEV_ID/100)
4. DAC (DFC,. . .): MSTP1 musí mít adresu shodnou s nadřazeným DSC, MSTP2 by měl být LINKnet
5. IP a Ethernet adaptér by měly být zároveň povoleny pouze na jednom zařízení (pokud se jedná o jednu lokalitu; výjimky jsou možné po schválení Garantem)
6. Zařízení s povoleným IP portem ručně zkontrolovat (adresu sítě, IP adresu, masku, gateway, typ zařízení (povolené pouze Regular Device), port)

2.2.3 Funkčnost komunikace

Spustit report „Funkcnost_komunikace“, jeho výsledek uložit jako přílohu 3 protokolu a zkontrolovat:

1. Zda komunikace nevykazuje problémy (subjektivní měřítko, ale každá hodnota nad 100 by měla být prověřena v ORCAview, zda chyby narůstají, zda jsou zanedbatelné oproti celkově přijatým apod.)

Pokud byly nalezeny jakékoliv problémy, uložit kontroler do FLASH, resetovat, zapsat do protokolu a na konci testů tento report zopakovat.

2.2.4 Výměna dat

Spustit report „Vymena_dat“, jeho výsledek uložit jako přílohu 4 protokolu a zkontrolovat:

1. Zda je DefaultExchangeType nastaven na „COV - Unconfirmed“, případně na „COV - Confirmed“ - pokud ne, je třeba vysvětlit. Naprosto nevyhovující je „Optimized Broadcast“, může narušit provoz některých zařízení.
2. Zda jsou časy posledních přenosů dat v normálních mezích (veškeré hodnoty nad 10 s mohou být problémem a je nutné je prověřit).

Spustit report „Vymena_dat_detail“, jeho výsledek uložit jako přílohu 5 protokolu a zkontrolovat:

3. Zda je report prázdný, pokud ne, tak: pro každé vypsané DER zkontrolovat, zda je zápis do vzdálené proměnné vhodně ošetřen (např. dle Delta Controls KbA1090)

2.2.5 Čas a jeho synchronizace

Spustit report „Cas_synch“, jeho výsledek uložit jako přílohu 6 protokolu a zkontrolovat:

1. Zda všechna zařízení mají po BACnetu čitelné aktuální datum a čas

Dále pomocí ORCAview (nebo jiného BACnet SW) nastavit výrazně odlišný čas a datum a znovu provést report „Cas_synch“, zkontrolovat:

2. Zda všechna zařízení mají shodný čas a datum (odpovídající nastavenému)

Následně pomocí ORCAview (nebo jiného BACnet SW) nastavit správný čas a datum, znovu provést report a zkontrolovat:

3. Zda všechna zařízení mají shodný čas a datum (odpovídající realitě)

2.2.6 Rychlost kontrolerů a volná paměť

Spustit report „Rychlost_pamet“, jeho výsledek uložit jako přílohu 7 protokolu a zkontrolovat:

1. Frekvenci průběhů programu (ScanRate) - pokud je pro některý kontroler pod 5, je nutné zmírnit jeho zátěž.
2. Frekvenci čtení/zapisování vstupů/výstupů (IOScanRate) - přijatelné jsou hodnoty vyšší jak 8
3. Volná dynamická paměť (DynamFree) - musí být minimálně 10% z celkové dynamické paměti, je nutné zkontrolovat všechny hodnoty pod 20
4. Volná statická paměť (StaticFree) - musí být minimálně 10% z celkové statické paměti, je nutné zkontrolovat všechny hodnoty pod 20

2.2.7 Datové body v obrazovkách

Je nutné zkontrolovat, zda jsou všechny objekty v obrazovkách správně nalinkovány.

1. Vizuální kontrola obrazovek, jestli fungují všechna zobrazovací pole
2. Kontrola mapování objektů ve webové verzi obrazovek

   Je nutné obrazovky přeložit pro ORCAweb, následně pro každou obrazovku otevřít soubor .asp v PSPadu. Následně kombinací Ctrl + F spustit hledání, do pole „Najít“ vložit „BAC.\d+“, v Možnostech zaškrtnout „Regulární výrazy“ a stisknout tlačítko „Kopírovat“. Ve vytvořeném souboru jsou DEV_ID kontrolerů, ze kterých jsou mapovány objekty do obrazovky. Tento seznam je nutné zkontrolovat, zda DEV_ID jsou podmnožinou reportu „Kontrola_zarizeni“ (jediná výjimka je aktuální čas a datum ze zařízení 91).

2.2.8 Trendlogy

Spustit report „Trendlogy“, jeho výsledek uložit jako přílohu 8 protokolu a zkontrolovat:

1. Zda jsou všechny trendlogy povolené (LogEn == true)
2. Zda mají trendlogy LogInt nastaven na 0 (tzn. COV), výjimka je možná pro trendování spotřeb nebo ve výjimečných případech, musí být odsouhlaseno ze strany objednatele.
3. Zda mají všechny trendlogy nastavenou EVC (Notification Class) pro oznamování plného bufferu, výchozí třída je EVC9 - „Archival“.
4. Zda mají všechny trendy nastavenou objekt trendování („InputRefEx“) a objekty trendování jsou na stejném zařízení, jako trendlog (výjimky jsou možné po odsouhlasení objednatelem).
5. Zkontrolovat velikost zásobníku na záznamy („BufferSize“). Nepřípustná hodnota je pod 100 záznamů, optimální je cca 500 záznamů (čím vyšší, tím lépe).
6. Zkontrolovat, zda jsou vytvořeny trendlogy pro všechny smysluplné objekty (zejména veškeré teploty, tlaky, spotřeby, žádané hodnoty, ventily, provoz zařízení (binárně nebo provozní hodiny), ...) - nutno konzultovat s Garantem.

2.2.9 Alarmy

Spustit report „Alarmy“, jeho výsledek uložit jako přílohu 9 protokolu a zkontrolovat:

1. Zda jsou všechny alarmy ve stavu Normal („Value“).
2. Zda mají všechny alarmy nastavenou korektní EVC (Notification Class), odpovídající zvyklostem.
3. Zda mají všechny alarmy nastaven objekt alarmu („InputRef“) a tomu odpovídající algoritmus alarmování.
4. Zda jsou vypnuté automatické texty (AutoText == false).
5. Zkontrolovat ručně alarmové texty - zda jsou vyplněny a obsahově i sémanticky správně.

2.2.10 EVC

Spustit report „EVC“, jeho výsledek uložit jako přílohu 10 protokolu a zkontrolovat:

1. Zda jsou na všech zařízeních vytvořeny EVC odpovídající zvyklostem BMS MU.
2. Správnost BACnet ID všech EVC (Notification Class) - musí bezpodmínečně odpovídat zvyklostem BMS MU.
3. Správnost názvů EVC - musí bezpodmínečně odpovídat zvyklostem BMS MU.
4. Funkčnost jednotlivých EVC (Value == true).
5. Ručně zkontrolovat příjemce jednotlivých EVC. Měly by být nastaveny příjemci dev91, dev92, dev93, dev94, případně operátorské stanice ORCAview. Nevyhovující nastavení je BROADCAST či některá jeho obdoba.

2.2.11 Časové plány

V ORCAview vyfiltrovat v každém zařízení objekty typu SCH a zkontrolovat, zda má každý rozvrh korektní „Value“ - povolenými stavy jsou české texty (nevhodné jsou ON, OFF, číselně vyjádřené stavy apod.). Výsledek kontroly je nutné zapsat do protokolu.

2.2.12 Ruční režim

Spustit report „Rucni_rezim“, jeho výsledek uložit jako přílohu 11 protokolu a zkontrolovat, zda je prázdný (povolené jsou konstanty a podobné objekty v ručním režimu). Výsledek zapsat do protokolu.

2.2.13 COV Increment

Spustit report „COV_Increment“, jeho výsledek uložit jako přílohu 12 protokolu a zkontrolovat nastavení velikosti COV Increment tak, aby byla nastavena smysluplně a vyhovovala požadavkům na trendování a komunikaci. Výchozí hodnoty jsou následující:

Teplota vzduchu	1°C nebo 0,5°C
Teplota topné vody	2°C nebo 5°C
Tlak vzduchu	10Pa
Tlak vody	0,5bar
Otevření ventilu	5%
Vlhkost vzduchu	5%

Popsané hodnoty jsou pouze doporučené, v případě potřeby je možné nastavit jinak, avšak s ohledem na trendování a přenos dat. Nejsou přípustné hodnoty výrazně nižší, než uvedené v tabulce výše.

2.2.14 Multistate objekty

Spustit report „Multistate_objekty“, jeho výsledek uložit jako přílohu 13 protokolu a zkontrolovat:

1. Zda všechny objekty mají vyhovující počet stavů (do 10).
2. Zda jsou hodnoty všech objektů v povoleném rozmezí (maximálně počet stavů).

2.2.15 Kontrola komunikace - Wireshark

Je nutné spustit na počítači připojeném do izolované sítě program Wireshark, spustit zachytávání komunikace a v průběhu sledování otevřít veškeré obrazovky a načíst data ze všech kontrolerů. Zároveň zachytávání provozu musí trvat alespoň půl hodiny. Následně zachytávání provozu ukončit, nachytaná data uložit do souboru .pcapng, tento přiložit jako přílohu 14 protokolu a zkontrolovat následující:

1. Zprávy broadcast - filtr „eth.dst == ff.ff.ff.ff.ff.ff“
   Povolené pakety pro tento filtr:

   - Who-Is 91
   - UnConfirmedEventNotification

   Pokud se vyskytují nějaké jiné pakety, je nutné toto zapsat do protokolu, prověřit a vyřešit. Zejména je nutné zkontrolovat, zda všechny pakety Who-Is jsou zasílány včetně limitů pro ID zařízení, v opačném případě může toto zahltit síť.

2. Fragmentace zpráv - filtr „bacapp.sequence_number“

   Fragmentace je vhodná pouze v určitých případech. Proto je nutné zjistit, zda fragmentace probíhá z důvodu čtení více objektů současně (ReadPropertyMultiple). Pokud má fragmentace jiný důvod, je třeba toto zapsat do protokolu a pokud je toto chybový stav, problém vyřešit. Naprosto nepřípustná je fragmentace zpráv při načítání jednotlivých objektů (např. pokud MV má 256 stavů).

Dále je možné ke kontrole komunikace použít Delta Network Analysis Tool - DNAT.

2.2.16 Kontrola dodržení Jmenné konvence

Je nutné zkontrolovat názvy objektů dle Jmenné konvence.

2.3 Vyhodnocení kontrol

Provedené kontroly je nutné vyhodnotit a výsledek zapsat do protokolu. Kladné stanovisko k připojení je možné vydat pouze v případě, že byly provedeny všechny kontroly uvedené v tomto dokumentu a při kontrolách nebyly nalezeny žádné chyby či nesrovnalosti. Provedení kontrol musí být kromě protokolu doloženo i reporty (které je možné nahradit jinými výpisy z konfigurace).

Následně je report podepsán ze strany Garanta a zhotovitele. Podpisem tohoto protokolu se pouze potvrzuje správnost údajů zaznamenaných v tomto dokumentu a v jeho přílohách. Není možné od podpisu dokumentu vyvozovat jakékoliv další skutečnosti. Pokud by bylo zjištěno, že skutečný stav neodpovídá situaci popsané v tomto protokolu a přiložených reportech, MU si vyhrazuje právo daná zařízení odpojit a zhotovitel je následně povinen doložit novým protokolem bezproblémové nastavení zařízení, až poté je možné zařízení opětovně připojit.

2.4 Příprava na připojení

K tomuto kroku je možné přistoupit pouze za předpokladu, že veškeré problémy, nesrovnalosti a nejasnosti z kapitoly 2.2 byly vyřešeny.

1. Vytvořit již finální podsíť (VLAN) a přidat volný port do této podsítě. Následně zapojit notebook s programem Wireshark a zkontrolovat, zda v této síti není žádný provoz (pouze některé typy broadcastů, ale pouze na IP, rozhodně nesmí nic komunikovat na ethernetu).
2. Nastavit na notebooku správné IP adresy a vyzkoušet dostupnost výchozí brány a některých zařízení v centru TeNe MU (orcaweby, BBMD zařízení apod.).
3. Portům switchů změnit podsíť (VLAN) na finální a opět pomocí programu Wireshark zkontrolovat síťový provoz v podsíti. Zároveň s tím pomocí programu ORCAview kontrolovat, zda v síti nenastávají problémy (jak na straně připojované lokality, tak na straně stávajícího BMS MU).

2.5 Vlastní připojení

V průběhu připojování je nutné sledovat komunikaci v síti (jak pomocí Wiresharku, tak i pomocí ORCAview). Je nutné mít přístup k ORCAview jak v lokální síti, tak i v stávající BMS MU.

1. Povolit IP adaptér na kontroleru, který bude zajišťovat BBMD (se správnou IP adresou, maskou, bránou a adresami sítí). Kontroler by měl být prozatím Regular Device.
2. Zkontrolovat provoz na síti - zda se neobjevily nějaké nečekané zprávy a zda ORCAview nehlásí problémy.
3. Změnit nastavení kontroleru na BBMD Device (bez nastavení BBMD IP adres).
4. Zkontrolovat provoz na síti - zda se neobjevily nějaké nečekané zprávy a zda ORCAview nehlásí problémy.
5. Přidat IP adresu lokálního kontroleru do BBMD (BDT) tabulky na BBMD kontroleru ve VLAN 11.
6. Zkontrolovat provoz na síti - zda se neobjevily nějaké nečekané zprávy a zda ORCAview nehlásí problémy.
7. Do BBMD (BDT) tabulky lokálního BBMD zařízení přidat IP adresu BBMD zařízení ve vlan 11.
8. Zkontrolovat provoz na síti - zda se neobjevily nějaké nečekané zprávy a zda ORCAview nehlásí problémy. Komunikace by již měla být funkční - kontrolery by měly být „vidět“ ze strany BMS MU a naopak ORCAview v lokální podsíti by mělo načíst kontrolery z BMS MU.

Pokud by se v jakémkoliv bodě připojování objevily problémy (nadbytečná komunikace, chyby v ORCAview, ztráty komunikace apod.), je nutné připojování okamžitě přerušit a zajistit, aby nebyl narušen provoz BMS MU. Je nutné vypnout IP adaptér (a/nebo BBMD) na straně lokální sítě (buď konfigurací BBMD kontroleru, nebo jeho odpojením od sítě nebo napájení).

2.6 Kontroly po připojení

1. Kontrola funkčnosti BMS MU: zda nedošlo ke zpomalení v ORCAview, ORCAwebu, zda fungují Historiany, komunikace všech zařízení,...
2. Kontrola funkčnosti alarmů (zda se objeví v ORCAwebu - musí být přihlášen Administrator).
3. Kontrola komunikace v vlan 11 pomocí programu Wireshark (broadcasty, top talkers apod.).

2.7 Dokončení připojení

Po úspěšném připojení je nutné provést následující kroky:

1. Předat Vizualizační obrazovky Garantovi prostřednictvím systému SVN (viz dokument Správa obrazovek BMS MU)
2. Požádat Garanta o nastavení uživatelských práv v BMS MU.
3. Předat Garantovi aktualizovaný soubor „AlarmGraphicMap.cfg“ (prostřednictvím SVN).
4. Požádat Garanta o vytvoření takových EVC ve Webovém rozhraní BMS MU, které budou odpovídat EVC na připojovaných zařízeních (odpovídat si musí BACnet ID, ale i název).
5. Požádat Garanta o vytvoření EVL objektu v Archivní databázi.
6. Přidat vybrané trendlogy do příslušné archivní databáze (seznam TL i výběr archivní databáze podléhá schválení Garanta).
7. Požádat Garanta o nastavení synchronizace času.
8. Uložit zálohu všech připojovaných kontrolerů a předat Garantovi.

SPRÁVA UNIVERZITNÍHO
KAMPUSU BOHUNICE
Masarykova univerzita

Metodika

Správa vizualizačních obrazovek BMS MU

OFM SUKB MU

12. července 2018

Obsah

1 Úvod

Tato metodika popisuje správu vizualizačních obrazovek BMS MU. Vizualizačními obrazovkami BMS MU jsou myšleny souhrnně obrazovky ORCAview a obrazovky ORCAweb.

Pro správu vizualizačních obrazovek ORCAview se používá Subversion (SVN), což je systém pro správu a verzování zdrojových kódů a umožňuje práci více uživatelů nad stejnými daty. Veškeré změny obrazovek ORCAview se odehrávají pomocí SVN, tedy i dodavatelé jsou povinni obrazovky předávat pomocí tohoto systému.

Na serveru SVN se vždy nachází aktuální verze dat. Každý uživatel si může pomocí klienta SVN tato data stáhnout do svého počítače (vytvoří se lokální kopie dat). Tato data může poté upravovat a případně nahrát na server, odkud si data stáhnou ostatní uživatelé.

Správu obrazovek ORCAweb provádí výhradně Garant. Dodavatelé a uživatelé BMS MU předávají pomocí SVN aktuální obrazovky ORCAview, Garant zajišťuje jejich překlad na obrazovku ORCAweb, namátkovou kontrolu a umístění na servery BMS MU.

Zodpovědnost za správnost obrazovek (jak formální, tak i obsahovou) nese dodavatel nebo uživatel, který obrazovku vytvářel nebo upravoval.

2 Požadavky na obrazovky ORCAview

Pro zajištění kompatibility a správné funkčnosti je nutné při vytváření/úpravách obrazovek dodržovat dále popsané zásady.

Zejména je třeba, aby se obrazovka po přeložení na ORCAweb korektně zobrazovala (musí se automaticky aktualizovat, nesmí být příliš tlusté čáry apod.). Obrazovky ORCAview musí používat pouze ty objekty, které podporuje i ORCAweb - musí být zajištěna plná funkcionalita obrazovek v ORCAwebu.

V obrazovkách nesmí být faktické chyby (např. špatně nalinkované objekty, zkopírované objekty a nezměněné linky ...).

2.1 Rozlišení/velikost obrazovek

Standardním rozlišením je 1366x768 (WXGA), což odpovídá hodnotám 45313x28406 v Illustratoru. Použití většího rozlišení není přípustné (tyto obrazovky by nebylo možné používat na notebooku), použití nižšího rozlišení není vhodné - obrazovka je příliš malá.

2.2 Jazyk ORCAview

Je nutné mít při vytváření či úpravě obrazovek přepnut jazyk ORCAview na češtinu.

2.3 Navigace z alarmů do obrazovek

Pro každý alarm v BMS MU musí být definována obrazovka, na které je zobrazen daný alarmový objekt. Tato definice se provádí v souboru `AlarmGraphicMap.cfg`, umístěném v SVN (složka `ObrazovkyORCAview`).

Po každé úpravě obrazovek či alarmů je autor povinen zkontrolovat, zda nedošlo ke změnám ve vazbách alarmů a obrazovek a případně dle provedených změn upravit soubor `AlarmGraphicMap.cfg` prostřednictvím SVN.

Struktura konfiguračního souboru je následující:

```
graphic=<obrazovka>
<objekt1>, <objekt2>, <objekt3>
```

kde `<obrazovka>` je relativní cesta k obrazovce na serveru ORCAweb vůči `C:\inetpub\wwwroot\DeltaWeb\Graphics` a `<objekt>` je definice objektu, který je zdrojem alarmu.

Například:

```
graphic=ukb/Vytahy.asp
4627.bi3, 4627.bi10, 4627.bi11, 4100.BI114, 4100.BI115, 4100.BI116
```

Požadavek na aktualizaci souboru `AlarmGraphicMap.cfg` na serverech se provádí dle kap. 4.1.

2.4 Obrázky v obrazovkách

Veškeré obrázky v obrazovkách musí být odkazovány relativně (tedy umístění obrázku vůči aktuální cestě), absolutní cesty jsou zakázány.

Opakující se obrázky se nepřikládají ke každé obrazovce, ale umisťují se do zvláštní složky v SVN. Následně si každý uživatel ORCAview nastaví SVN tak, aby se aktualizovala složka `C:\Program Files (x86)\Delta Controls\3.40\Dialogs`, nebo si při zjištění chybějícího obrázku do této složky zkopíruje obrázky ze složky v SVN.

2.5 Adresářová struktura a názvy obrazovek

Adresářová struktura obrazovek ORCAview je vytvořena v SVN a je nutné ji dodržovat. Zejména platí následující:

- První úrovní jsou rozšířené lokality (shodná první dvě písmena polohového kódu; např. sloučeny Brno-Město I, Brno-Město II, Brno-Město III do rozšířené lokality „MB“)
- Druhou úrovní jsou složky trunk, tags a branches. Uživatelé a dodavatelé používají pouze trunk, tags a branches jsou pro správce obrazovek.
- V třetí úrovni jsou složky jednotlivých budov, přehledové obrazovky lokalit případně rozšířených lokalit a další obrazovky a soubory vztahující se k lokalitě (legendy, komunikace, nápověda apod.)
- Ve čtvrté úrovni jsou složky jednotlivých podlaží budovy a obrazovky společné pro celou budovu (VZT, ÚT, TUV, CHL . . .)
- V páté úrovni (uvnitř složek podlaží) jsou technologie příslušející k danému podlaží (IRC, EZS/PZTS, EPS, Teploty . . .)

Názvy složek a obrazovek jsou určeny podle následujících pravidel:

- Název složky pro rozšířenou lokalitu je odvozen z jejího názvu (Staré Brno → SB, Pisárky → PIS . . .)
- Názvy složek budov jsou odvozeny z jejího názvu (Tvrdého 5 → Tvr5), případně je možné použít polohový kód budovy (např. BBA11)
- Názvy přehledových obrazovek lokalit jsou tvořeny jejich polohovými kódy (BBA), které mohou být doplněny o upřesnění.
- Názvy obrazovek jsou tvořeny názvem budovy a technologií, případně polohovým kódem budovy a technologií pro obrazovky společné pro celou budovu (např. „Tvr5_UT“ nebo „BBA11_UT“)
- Názvy obrazovek jsou tvořeny názvem budovy, podlažím a technologií, případně polohovým kódem budovy a podlaží a technologií pro obrazovky jednotlivých podlaží (např. „Tvr5_1NP_IRC“ nebo „BBA11N01_EZS“)
- Názvy složek podlaží jsou tvořeny buď ve stylu 1PP, 1NP, 2NP nebo podle polohového kódu P01, N01, N02.

V případech, které nejsou zde popsány, dodavatel (či uživatel) navrhne adresářovou strukturu a názvy obrazovek a předá k odsouhlasení Garantovi.

Každá obrazovka je označena nadpisem (který se může, avšak nemusí shodovat s názvem obrazovky). Tento nadpis musí být dostatečně vypovídající a popisný (vhodný je např. „A25 - 3NP - EPS“). Nadpis musí být shodný s CAPTION obrazovky.

3 Návod k SVN pro obrazovky ORCAview

3.1 Instalace

Pro práci s SVN je vhodné použít rozhraní TortoiseSVN, avšak je možné používat i jiné klienty.

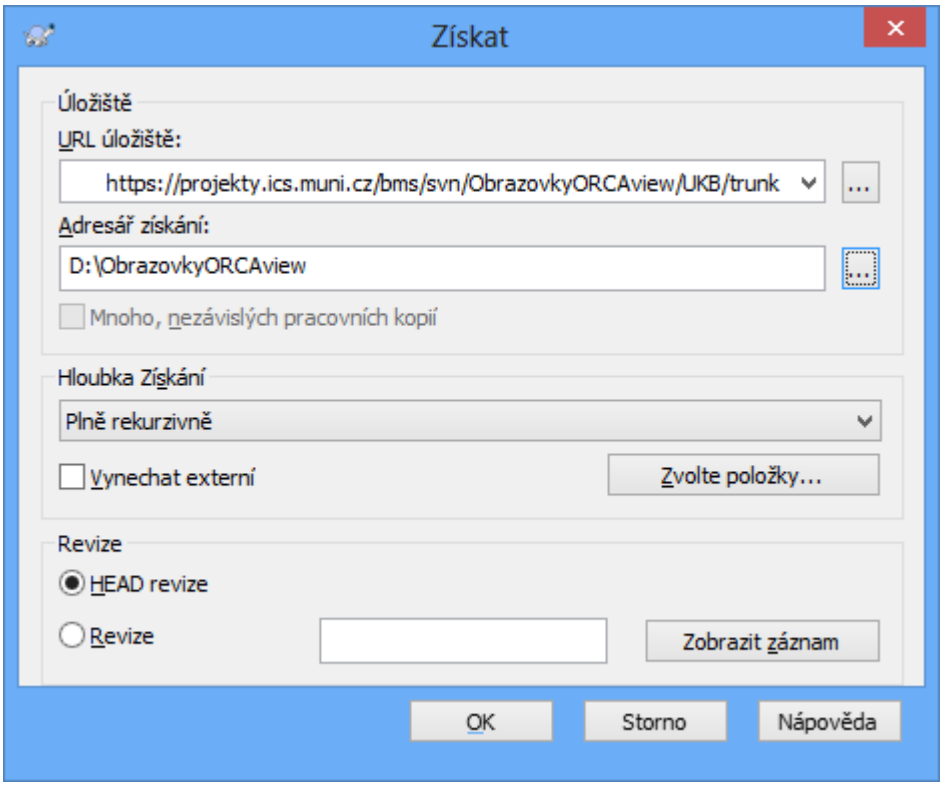
1. Stáhnout instalační soubor podle verze operačního systému ze http://tortoisesvn.net/downloads.html
2. Provést instalaci, je možné ponechat všechny nastavení výchozí (instalace může vyžadovat restart počítače, v tom případě je nutný).
3. (Nepovinné) Stáhnout jazykový balíček dle verze operačního systému ze http://tortoisesvn.net/downloads.html (níže na stránce)
4. (Nepovinné) Změnit jazyk TortoiseSVN (kliknout pravým tlačítkem např. na plochu, `TortoiseSVN` ⇒ `Settings`, první položka `Language` - nastavit na `čeština`)
5. Tím by měla být dokončena instalace TortoiseSVN a je možné ji začít používat (je možné ověřit přítomností nových možností po kliknutí pravým tlačítkem na plochu nebo v Průzkumníku).

3.2 První použití

Při prvním použití je nutné nastavit adresu vzdáleného úložiště a přihlašovací údaje.

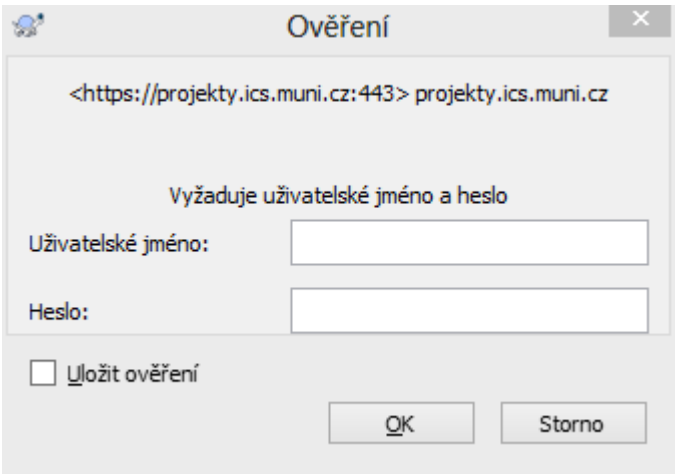
3.2.1 Uživatelé jedné lokality - Správa budov SUKB

1. Vytvořit novou složku s názvem `ObrazovkyORCAview` ve vybraném adresáři.
2. Kliknout na vytvořený adresář pravým tlačítkem myši, `SVN Získat ...`, otevře se dialogové okno:



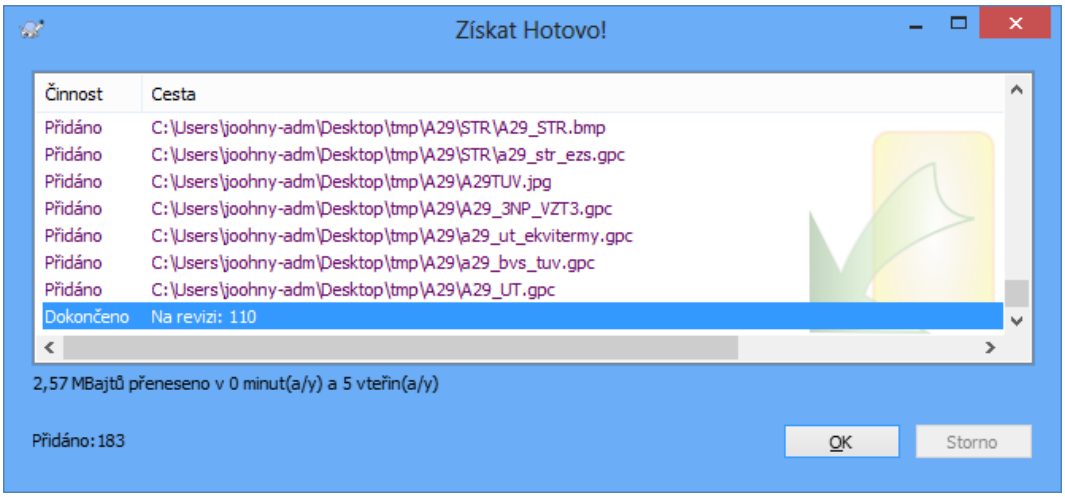
Je nutné do `URL úložiště` vyplnit `https://projekty.ics.muni.cz/bms/svn/ObrazovkyORCAview/UKB/trunk`, jinak je možné tento dialog nechat ve výchozím nastavení a potvrdit `OK`.

3. Objeví se přihlašovací okno:



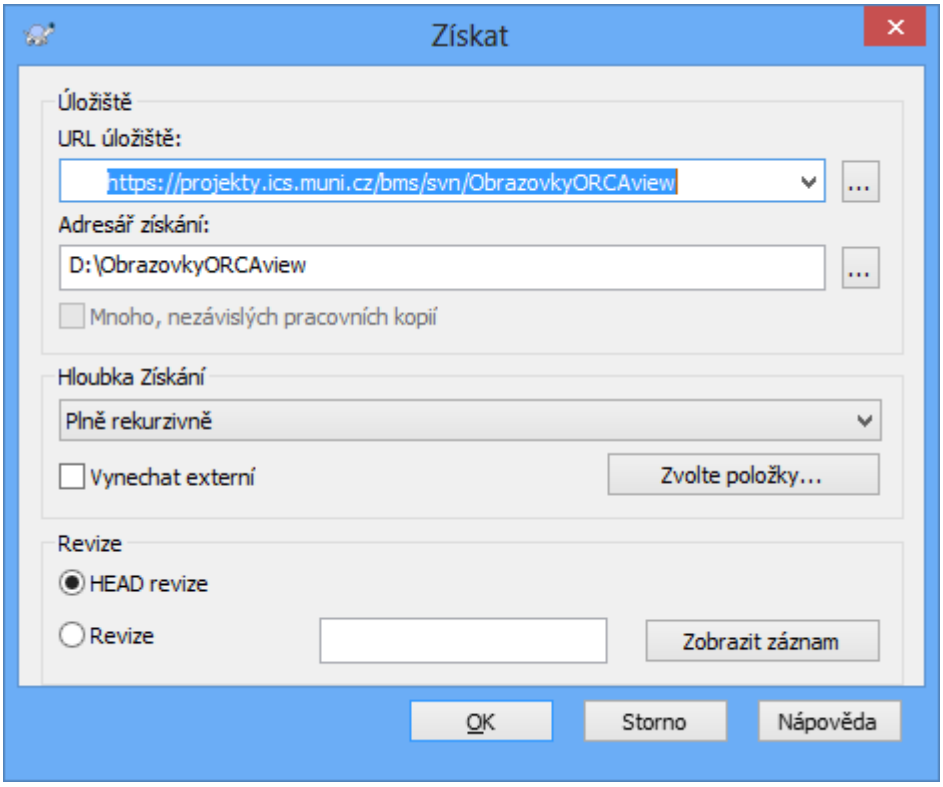
Je nutné zadat své UČO a sekundární heslo a doporučujeme zatrhnout možnost `Uložit pověření`, následně potvrdit `OK`.

4. Proběhne stažení obsahu vzdáleného úložiště do počítače a po dokončení by se mělo objevit následující okno, které je možné potvrdit `OK`.



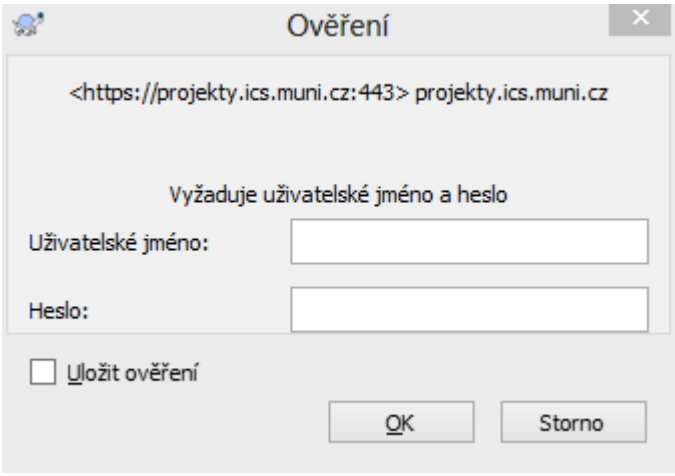
3.2.2 Uživatelé více lokalit - Správci BMS MU, dodavatelé

1. Vytvořit novou složku s názvem `ObrazovkyORCAview` ve vybraném adresáři.
2. Kliknout na vytvořený adresář pravým tlačítkem myši, `SVN Získat ...`, otevře se dialogové okno:



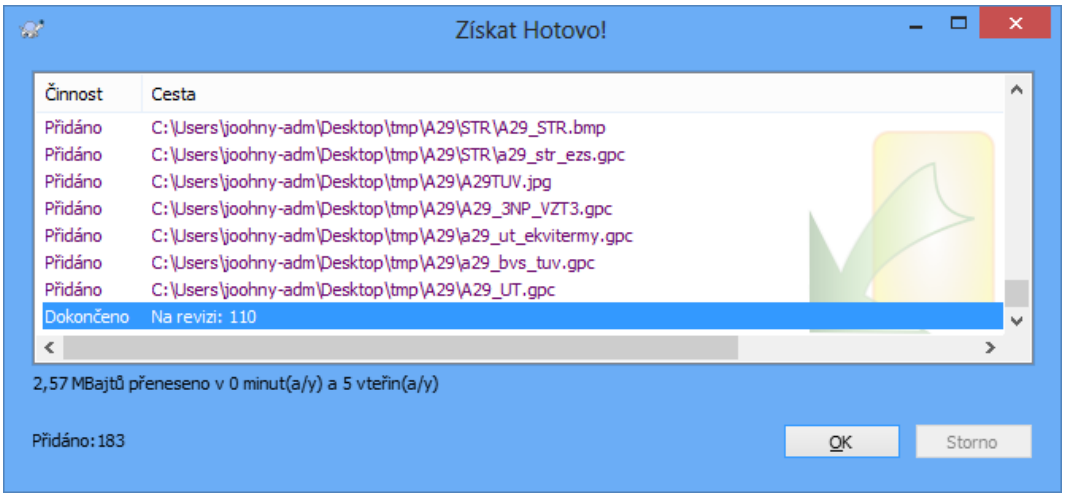
   Je nutné do `URL úložiště` vyplnit
   `https://projekty.ics.muni.cz/bms/svn/ObrazovkyORCAview`,
   jinak je možné tento dialog nechat ve výchozím nastavení a potvrdit `OK`.

3. Objeví se přihlašovací okno:



Je nutné zadat své UČO a sekundární heslo (případně GuestID a heslo) a doporučujeme zatrhnout možnost `Uložit pověření`, následně potvrdit `OK`.

4. Proběhne stažení obsahu vzdáleného úložiště do počítače a po dokončení by se mělo objevit následující okno, které je možné potvrdit `OK`.

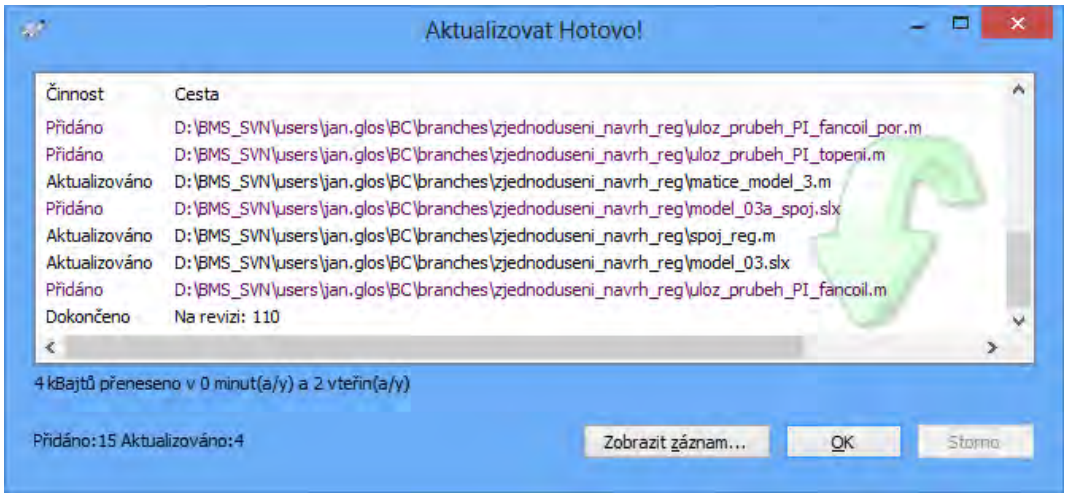


3.3 Práce s SVN

Při práci s SVN je nutné vždy udržovat aktuální data jak na serveru, tak i v lokálním úložišti. V této kapitole je popsáno jak toho dosáhnout. Vždy je nutné před úpravou jakéhokoliv souboru provést `SVN Akutalizace` (nebo mít nastavenou automatickou aktualizaci) a upravené soubory co nejdříve po změně nahrát na server pomocí `SVN Odevzdání`. Při aktualizaci dat nesmí být otevřené soubory, které jsou obsaženy v SVN (obrazovky, obrázky apod.). Pokud nejsou upravené soubory neprodleně nahrány na server, může jiný uživatel stejné soubory upravit a nahrát na server dříve - hrozí zde ztráta lokálních úprav.

3.3.1 Aktualizace - Update

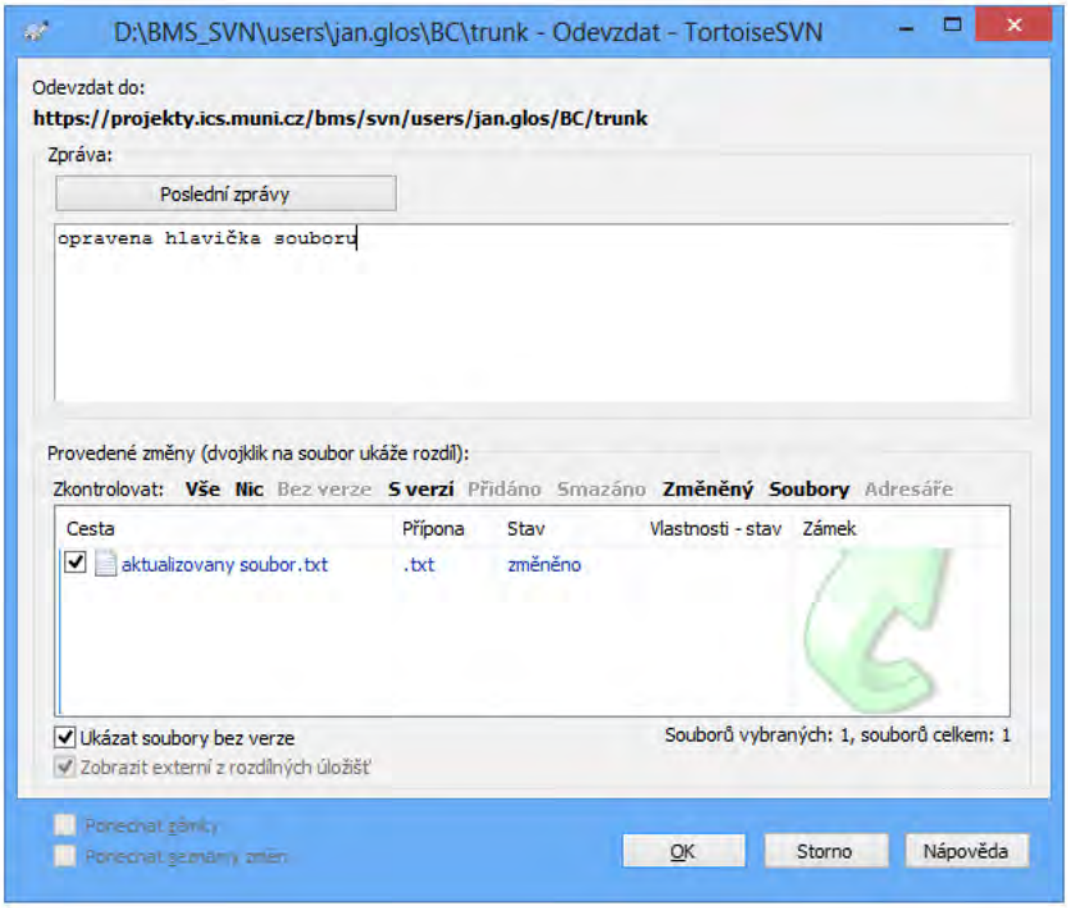
Je třeba zavřít všechny soubory, které jsou v SVN obsaženy (obrazovky, obrázky apod.). Pro aktualizaci dat (update) je nutné kliknout pravým tlačítkem na příslušnou složku (obvykle `ObrazovkyORCAview`) a použít volbu `SVN Aktualizovat`. Uživatel může být vyzván k přihlášení a objeví se následující dialogové okno:



Pokud se ve výpisu neobjeví žádné chyby, je možné toto okno zavřít. Nyní je obsah lokálního úložiště shodný s daty na serveru (vyjma souborů, které byly před aktualizací změněny a nebyly odevzdány).

3.3.2 Odevzdání - Commit

Pro odevzdání dat (commit) je nutné kliknout pravým tlačítkem na příslušnou složku (obvykle `ObrazovkyORCAview`) a použít volbu `SVN Odevzdat`. Objeví se následující dialogové okno



Do textového pole `Zpráva` je nutné popsat prováděnou změnu tak, aby bylo ostatním uživatelům zřejmé, čeho se změna týkala. Není nutné do tohoto pole vypisovat seznam změněných souborů, ten je v poli níže. Příklady vhodných zpráv:

- Oprava linků EPS na CETOCOENu
- Přidány odkazy na trendlogy
- Změněno obarvování toho a toho objektu

Pokud má být automaticky vygenerován požadavek na aktualizaci obrazovek na serverech ORCAweb, je nutné na začátek pole `Zpráva` umístit text „webUpdate“, např.:

- webUpdate Oprava linků EPS na CETOCOENu
- webUpdate Přidány odkazy na trendlogy
- webUpdate Změněno obarvování toho a toho objektu

V tabulce `Provedené změny` je seznam souborů, které budou odevzdány na server. Je možné vybrat, které soubory budou odevzdány a které ne. Je vhodné odevzdávat pouze ty soubory, které mají mít

k dispozici i ostatní uživatelé (tedy pomocné a jiné soubory neodevzdávat). Pokud je vytvořena nová obrazovka, je nutné ji v tomto dialogovém okně zatrhnout, aby byla odevzdána na server.

Pokud odevzdání proběhne v pořádku, objeví se potvrzovací okno, které je možné zavřít.

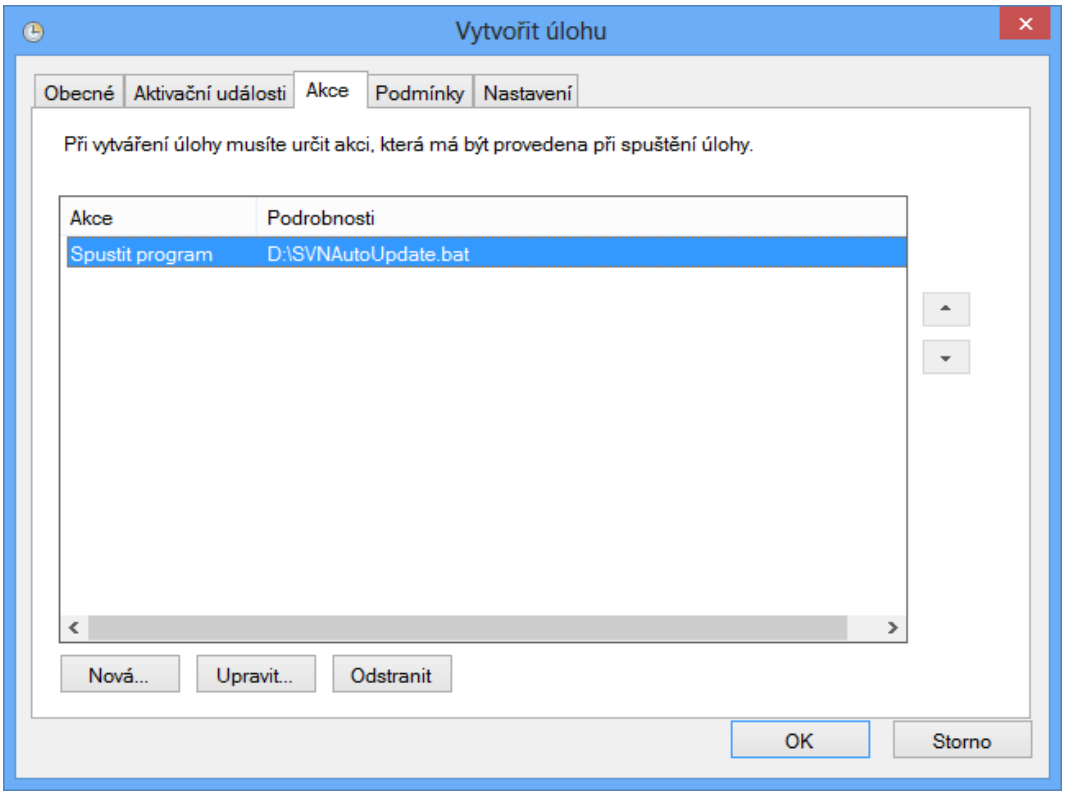
3.3.3 Automatická aktualizace

Je možné nastavit automatickou aktualizaci. Aktualizace se provádí vždy při přihlášení k počítači. Je nutné zajistit, aby byly zavřené všechny soubory, které jsou v SVN obsaženy (obrazovky, obrázky apod.).

1. Buď zkopírovat soubor `SVNAutoUpdate.bat` z SVN a změnit cestu k složce SVN nebo:
   (a) Na počítači vytvořit nový textový soubor (s názvem např. `SVNAutoUpdate.txt`)
   (b) Do souboru zkopírovat:

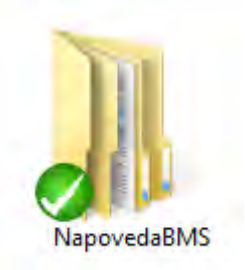
   ```
   @echo off
   TortoiseProc.exe /command:update /path:"<cesta_obrazovky>" /closeonend:2
   ```

   (c) Doplnit aktuální cestu složky s obrazovkami ORCAview místo `<cesta_obrazovky>`, např. `C:\ObrazovkyORCAview`
   (d) Uložit soubor.
   (e) Změnit příponu souboru z `.txt` na `.bat`
2. Spustit `Plánovač úloh` (např. Spustit ⇒ `Taskschd.msc`)
3. Importovat úlohu `SVNAutoUpdate.xml` (umístěna v složce SVN)
4. Nastavit správnou cestu k `.bat` souboru

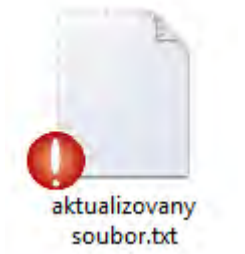


3.3.4 Signalizace stavu složek a souborů

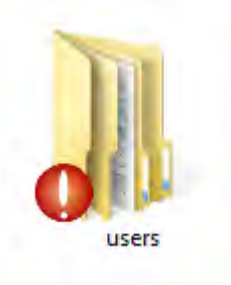
U každé složky a souboru, které jsou v SVN, je možné sledovat stav vůči úložišti na serveru. Možné jsou následující symboly:



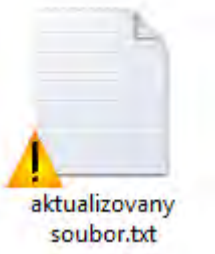
Zelená „fajfka“ značí shodný obsah souborů či složek v lokálním úložišti a na serveru.



Červený vykřičník značí neaktuální soubor, je tedy nutné tento soubor Odevzdat viz 3.3.2 (pokud se má tato úprava nadále používat).



Červený vykřičník značí neaktuální složku (tedy jeden nebo více souborů ve složce nebo podsložkách), je tedy nutné tuto složku odevzdat viz 3.3.2 (pokud se má tato úprava nadále používat).



Oranžový vykřičník značí konfliktní soubor. Je nutné data ručně opravit.

3.3.5 Přidání souboru nebo složky do SVN

Pro přidání souboru do SVN je nutné buď soubor „zaškrtnout“ při Odevzdávání 3.3.2, nebo použít volbu `Přidat` (pravým tlačítkem na soubor, `TortoiseSVN`). Při následujícím Odevzdání je již soubor označen.

4 Postup pro aktualizaci obrazovek ORCAweb

Aktualizaci obrazovek na serverech ORCAweb provádí na požádání OFM SUKB. Pro aktualizaci obrazovek (nebo umístění nových obrazovek) na serverech ORCAweb je nutné, aby obrazovky splňovaly požadavky definované v kapitole 2.

Obrazovky nesplňující tyto požadavky není možné umístit na servery ORCAweb a autor poslední změny musí obrazovky opravit do stavu odpovídajícího kapitole 2.

4.1 Požadavek na aktualizaci ORCAweb v tracu BMS

Vytvořit nové hlášení v tracu BMS (kliknutím na odkaz by většina polí by měla být předvyplněna, je nutné vyplnit tučně zvýrazněná).

- **Nadpis: stručný popis**
- **Popis: seznam obrazovek, které je třeba aktualizovat; nebo odkaz na revizi SVN (v rámci které byly obrazovky upraveny) ve formátu „[xxx]“, kde xxx je číslo revize**
- Typ: „uprava“
- Komponenta: „webUpdate“
- Kopie: „bms@ukb.muni.cz“
- Vlastník: přiřadit uživatele, který má aktualizaci provést

U požadavků zadaných jinak (mailem, telefonicky apod.) nelze garantovat jejich vyřízení - není možné je evidovat a sledovat jejich stav.

SPRÁVA UNIVERZITNÍHO KAMPUSU BOHUNICE
Masarykova univerzita

Rozdělení místností	Teplota vzduchu $[°C]$ topení min	topení max	chlazení min	chlazení max	Vlhkost $[\%RH]$ min	Vlhkost $[\%RH]$ max	Koncentrace CO_2 $[ppm]$ min [1]	Koncentrace CO_2 $[ppm]$ max [2]	Osvětlení $[lx]$	Index oslnění	Přívod vzduchu (minimální) $[m^3 \cdot h^{-1}]$ na osobu
kancelář neklimatizovaná	20	24	–		30	60	350	1000	300	19	50
kancelář klimatizovaná	20	24	23	26	30	60	350	1000	300	19	50
posluchárna	20	24	23	26	30	60	350	1000	500	19	50
seminární místnost	20	24	23	26	30	60	350	1000	500	19	50
zasedací místnost	20	24	23	26	30	60	350	1000	500	19	50
knihovna	20	24	23	26	30	60	350	1000	500	19	50
laboratoř bez techn. požadavku na teplotu	20	24	23	26	40	60	350	1000	750	19	70
laboratoř s techn. požadavkem na teplotu	±0,5		±0,5		dle pož.		350	1000	750	19	70
šatna	20	24	23	26	30	65	350	1000	300	25	25
vnitřní sportoviště	20	24	23	26	30	70	350	1000	500	22	100
skladové prostory	20	24	23	26	30	70	350	1000	300	25	25
strojovna HVAC, výtahu, SLN (nevytápěné)	–		15	20	30	60	350	1000	300	25	25
rozvodna SLP, serverovna, telefonní ústředna	–		20		30	60	350	1000	300	25	25
kuchyňka (denní místnost)	20	24	23	26	30	70	350	1000	300	25	25
garáž	7	15	–		30	80	350	1000	300	25	70
toalety	16	22	–		30	70	350	1000	300	25	25
komunikační prostory (chodby, schodiště)	18	22	25	30	30	60	350	1000	300	22	25

[1] prospěšná pro lidský organismus
[2] ve vnitřních prostorách.