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.