Versionhallinta

Versio	Kuvaus	Julkaistu
v26102016		10/2016 BIG-FI sivustolla
170123	BACnet/SC lisätty	luonnos
180923	BACnet/SC 1. kommenttikierros	luonnos
091023	2. kommenttikierros	julkaisu BIF-FI sivustolla

JOHDANTO

Ao. teksti on tarkoitettu ohjeelliseksi kirjoitettaessa RAU-työselitystä, jolla on tarkoitus kattaa BACnet-järjestelmävaatimukset, niin valvomo kuin alakeskustasolla. Tavoitteena on, että tarjoukset olisivat vertailukelpoisia, eri toimittajat toimivat samoilla reunaehdoilla ja myös rakennuttajan velvoitteet on huomioitu tältä osin.

BACnet-aluevalvontajärjestelmän toiminnan kannalta olennaista on, että valvomotoimittajia on aina vain yksi. Muut toimittajat laskevat tarjoukseensa BACnet-alakeskusten liittämisen valvomoon yksikköhinnoin, joihin valvomotoimittaja on sitoutunut.

****

Rakennusautomaatiojärjestelmän BACnet-vaatimukset

Järjestelmän tiedonsiirto

Järjestelmän tiedonsiirron tulee perustua BACnet-standardin mukaiseen tiedonsiirtoprotokollaan (EN ISO 16484-5). Valvontajärjestelmän ohjelmistojen sekä laitteiden tulee olla BACnet-sertifioituja.

Valvomo-ohjelmiston tulee olla hyväksytty BACnet-työasemaksi (vähintään B-OWS = BACnet Operator Workstation).

Kaikkien järjestelmään liitettävien BACnet-laitteiden tulee olla sertifioituja. Mikäli laite ei ole sertifioitu, toimittaja vastaa siitä, että liityntä on BACnet-standardin mukainen.

Järjestelmään liitettävien alakeskusten tulee täyttää vähintään BACnet-alakeskustason vaatimukset (B-BC = BACnet Building Controller). Alakeskusten tulee tukea eri aliverkoissa sijaitsevien laitteiden välistä BBMD-reititystä (BACnet Broadcast Management Device).

Toimintaselostuksessa määritellyt fyysiset ja ohjelmalliset pisteet sekä toiminnot tulee julkaista järjestelmässä BACnet-protokollamuodossa.

Kalentereita tulee määrittää valmiiksi seuraavasti riippuen valvonta-alakeskuksen fyysisten pisteiden määrästä (min):

- Pistemäärä < 50 – 1 kpl
- Pistemäärä <100 – 3 kpl
- Pistemäärä < 200 – 5 kpl

Hälytysten prioriteetit

BACnet standardin mukaisesti hälytykset eritellään eri ryhmiin seuraavasti:

1. Turvallisuus / hätä (esim. palohälytys)
2. Vaara (esim. jäätymissuoja)
3. Vika (esim. ristiriita)
4. Huolto (esim. suodatinvahti)
5. Kohdekohtaiset ilmoitukset
6. Ilmoitukset (vain trendit)

JÄRJESTELMÄN OHJAUSPRIORITEETIT

Järjestelmän ohjelmoinnissa kojeiden ja laitteiden ohjausprioriteetit tulee määritellä seuraavasti:

Prioriteetti 1: Hengenvaara, käsiohjaus (esim. palokunta)
Prioriteetti 2: Hengenvaara, automaattiohjaus (esim. paloilmoituskekus)
Prioriteetti 5: Kriittinen ohjaus, esim. jäätymisvaara
Prioriteetti 6: Minimi päälläoloaika
Prioriteetti 8: Käsiohjaus (esim. laitteiden käsinohjaus valvomosta tai paikallisella käsipäätteellä)
Prioriteetti 10: Paikallisohjaus, esim. jatkoaikapainike
Prioriteetti 15: Automaattiohjaus, esimerkiksi aikaohjelma/kalenteri

PISTEIDEN NIMEÄMINEN

Järjestelmien toiminnan ja käytettävyyden kannalta piste-/positiotunnukset tulee olla nimetty yhteneväisesti. Alla on esitetty periaatteet mutta tarkempi positiointiohje on kohde-/asiakaskohtainen:

BACnet-osoite (Mandatory object-name)

- EI välilyöntejä
- EI erikoismerkkejä
- Yksilöllinen
- järjestelmän tulee tukea min 20 merkkiä

Esim. A_TK01_TE10 Tuloilmapuhaltimen jälkeinen sisäänpuhallusanturi
H_PV01_TE40 Patteriverkoston menovesianturi
C_JK01_TE60 Jäähdytyskoneen menovesianturi
E_PI01_PE01 Paineilmaverkoston paineanturi

Järjestelmälyhenne, johon piste kuuluu

A_= Ilmastointi
H_= Lämmitys
C_= Jäähdytys
E_= Sähkö/Erillispisteet

Laitetunnus on erotettava sallitulla merkillä esim. _ (alaviiva) tai muu sallittu

TK01_ = ilmanvaihtokone
PV01_ = patteriverkosto
JK01_ = jäähdytyskone

Laitenimi

TE10 = tuloilma-anturi
TE40 = menovesianturi

Pisteen selväkieliteksti (Optional Description)

- suomenkielinen pitkä kuvaus pisteelle, joka näkyy edellisissä esimerkeissä

BACnet-järjestelmien liittäminen valvomoon

Tilaajan velvoitteet

Tilaajan tulee antaa järjestelmään liitettävien BACnet-laitteiden IP-osoitteet, ja toteuttaa vaadittava IT-verkko. Järjestelmässä tulee käyttää yhtenäistä laitteiden positiointia (positiointiohje).

IT-verkon kannalta on huomioitava, että:

- normaali reititetty verkko on riittävä BACnet:lle
- BACnet/IP on TCIP-protokollan varaan rakennettu oma protokolla
- BACnet-protokolla aiheuttaa suuren määrän Broadcasteja verkkoon
- NAT ei ole mahdollista
- tietoturvallisuuden takia dataa ei saa siirtää julkisen verkon läpi, kuin salattuna kts. BACnet/SC.
- Eri aliverkoissa sijaitsevat BACnet-laitteet kommunikoivat BBMD (BACnet Broadcasting Management Device) avulla. BBMD tuntee muiden verkkojen laitteet ja avaa reitin niiden välille, jolloin fyysiset laitteet voivat kommunikoida keskenään.

Valvomotoimittajan velvoitteet

Valvomotoimittajan tulee jakaa muille laitetoimittajille BACnet-laitteiden ID:t eli yksilölliset BACnet-laiteosoitteet ja pitää yllä listaa niistä.

Yksikköhintaluettelossa huomioitavaa

Sertifioidun BACnet-laitteen liittämisen tulee olla kokonaishinnaltaan sama kuin valvomotoimittajan oman laitemerkin vastaavan säätimen/laitteen liittäminen. Positiointijärjestelmää on noudatettava.

Valvomoon liittämiseen laskettavan työmäärän perusta on BACnet-objektien määrä (fyysiset ja ohjelmalliset pisteet, aikaohjelmat/schedule, trendit, jne.). Tarjous lasketaan seuraavan kustannusrakenteen perusteella esim.:

- Valvomolisenssi - ____ € / 100 BACnet-objektia
- Valvomotyön tuntihinta - ____ € / h (alv 0%)
- Projektin/kohteen perustaminen - ____ h
- Pisteiden liittäminen valvontajärjestelmän tietokantaan – _____ objektia / h
- Historiatietojen perustaminen - ____ h / kuuden objektin trendiryhmä
- Grafiikkakuvan piirto - ____ h / kpl
- Grafiikkakuvan aktivointi/pistekiinnitykset ____ h / 40 objektia
- …

Tietoturva

BACnet Secure Connect

Kaikki kiinteistöautomaatiossa nykyisin käytettävät avoimet protokollat, kuten Modbus, M-bus, KNX ja BACnet ovat protokollia ilman salausta.
Kasvaviin tietoturvavaatimuksiin on kehitetty BACnet Secure Connect (SC), jossa viestit ovat salattuja ja laitteet autentikoituja, jolloin koko järjestelmä on suojattu ja siten tietoturvallinen.

BACnet SC käyttää siirtotienään TCP:tä ja se on mahdollista implementoida järjestelmästä riippuen, joko IPv4 tai IPv6 verkkoon. TCP paketinhallinta mahdollistaa toiminnan moderneissa IT ympäristöissä ja esimerkiksi NAT:in takaa toimimisen.

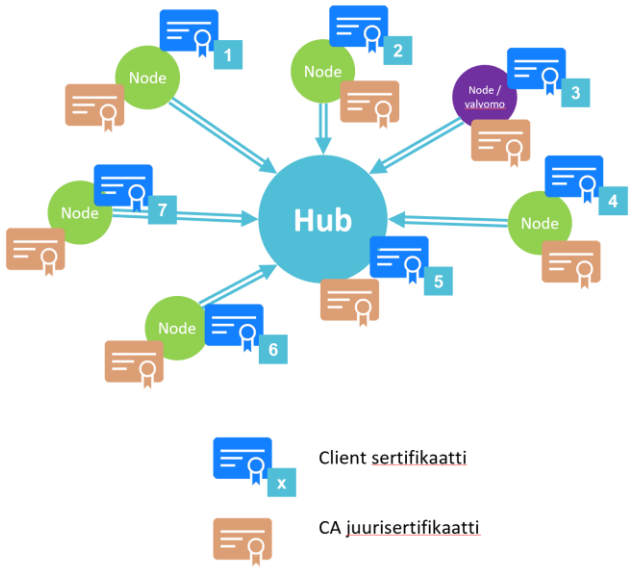
BBMD-laitteita ei SC-laiteverkossa tarvita kahden aliverkon välillä.

BACnet SC perustuu WebSocket:hin ja TLS salaukseen. SC:n käyttö on mahdollista rinnan BACnet IP:n ja muiden siirtoprotokollien kanssa. Protokollien välisestä kommunikaatiosta huolehtii Gateway-laite, joka on yleensä samalla säädin.

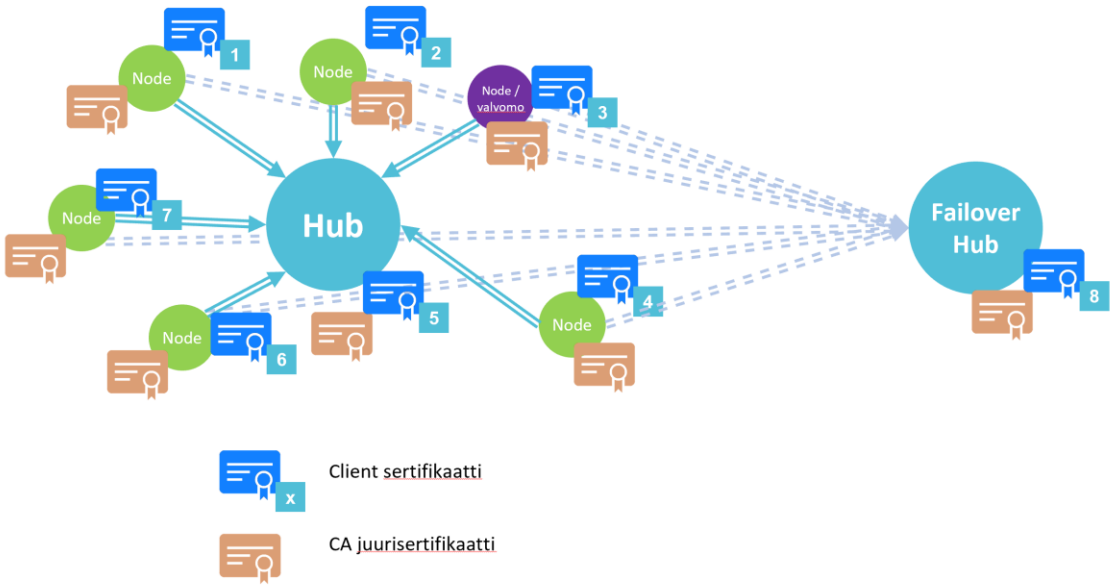
BACnet/SC:tä kannatta harkita silloin, kun on kyse kriittisestä kohteesta. SC:n rakentaminen ja ylläpito tuo mukanaan kustannuksia ja vastuita koko elinkaaren ajalle mm. sertifikaattien hallinta (omistaja, ylläpitäjä).

Koska kaikkiin laitemuutoksin ja -lisäyksiin tarvitaan CA sertifikaattia, täytyy sen hallinta olla vain yhdellä taholla. On otettava huomioon projektin ja elinkaaren aikainen hallinta. Tämä pitää olla kirjattu esim. **ylläpitosopimukseen** (esim. laitetta vaihdettaessa kommunikaatiota ei saada toimimaan ilman alkuperäistä sertifikaattia).

BACnet/SC perustuu Hub/Node-rakenteeseen, jossa verkossa on yksi Hubi, jonka kautta kaikki SC-Node-laitteet kommunikoivat (kts. kuva 1).
Koska Hub on välttämätön, sille suositellaan tehtäväksi vara-Hubi ts. Fail-over Hub (kts. kuva 2).



Kuva 1: BACnet/SC verkon topologia



Kuva 2: Suositeltava BACnet/SC verkon topologia, jossa Hubille on vara-Hubi.

VPN ja laitekohtaisen salatun liikenteen ero

Yhtenä vaihtoehtoisena tietoturvan tasona voidaan pitää VPN tunnelointia. On kuitenkin muistettava, että VPN ei salaa itse liikennettä, vaan muodostaa salatun siirtotien jonka sisällä tietoliikenne on edelleen avointa esim. kiinteistön sisäverkossa, jos VPN-yhteys on vain ulos.

BACnet/SC taas on laitetasolla salattu protokolla, joten viestit ovat salattuja esim. valvomon ja sen kanssa kommunikoivien laitteiden välillä ja niiden kesken, joten viestiä ei pysty avaamaan kuin vastaanottaja ja lähettäjä.

Ominaisuuksien vertailu ao. taulukossa:

Vertailu BACnet/SC vs. IP

	Ominaisuudet	BACnet/ IP	BACnet/ SC	
1	Standardoitu datamalli kommunikaatioon	●	●	BACnetin klassiset ominaisuudet
2	Järjestelmän skaalautuvuus ja joustavuus	●	●	
3	Yhteensopivuus BTL listattujen toimijoiden kanssa BIBBS ja PICS dokumenttien mukaan	●	●	
4	BACnet versioiden välinen yhteensopivuus eteen ja taaksepäin	●	●	
5	BACnet reititys eri BACnet datalinkkien välillä (BACnet MS/TP, BACnet IP, BACnet SC) muodostaakseen BACnet verkon	●	●	
6	Laite ja objekti-instanssinumeroon perustuva uniikki pisteidentifiointi	●	●	
7	Identtinen käyttö	●	●	
8	Samat BACnet palvelut (whois, I-am jne.)	●	●	
9	UDP pohjainen varmistamaton tiedonsiirto	●		
10	TCP pohjainen varmistettu skaalautuva tiedonsiirto		●	BACnet SC ominaisuudet
11	Sertifikaattipohjainen molemminpuolinen laiteautentikaatio ja verkkorajoitus X.509 V3 sertifikaateilla		●	
12	Tuki vaihtoehtoisille sertifiointitavoille (self signed, CA) organisaation tarpeiden mukaan		●	
13	End-to-end liikenteen salaus TLS 1.3 WebSocketeilla		●	
14	Ei raskasta Broadcast liikennettä IP verkossa		●	
15	Riippumaton IP verkkoratkaisusta, tukee micro-segmentöintiä		●	
16	Riippumaton IP verkon topologiamuutoksille		●	
17	Toimii NAT-verkoissa		●	
18	Ei tarvitse staattista IP-osoitteistoa (HUB-laitteelle käyttöä suositellaan, ellei FQDN ole käytössä verkossa)		●	
19	Turvallinen kommunikaatio, jopa avoimissa verkoissa		●	
20	Mahdollistaa jaettujen IP verkkojen käytön ilman VPN:ää		●	
21	Sopii holistiseen tietoturva-ajatteluun (Defence-in-Depth)		●	

Työryhmä: BACnet Interest Group Finland (BIG-FI)