

Sustavi automatizacije u zgradarstvu

SIGURNOST PRIJE SVEGA

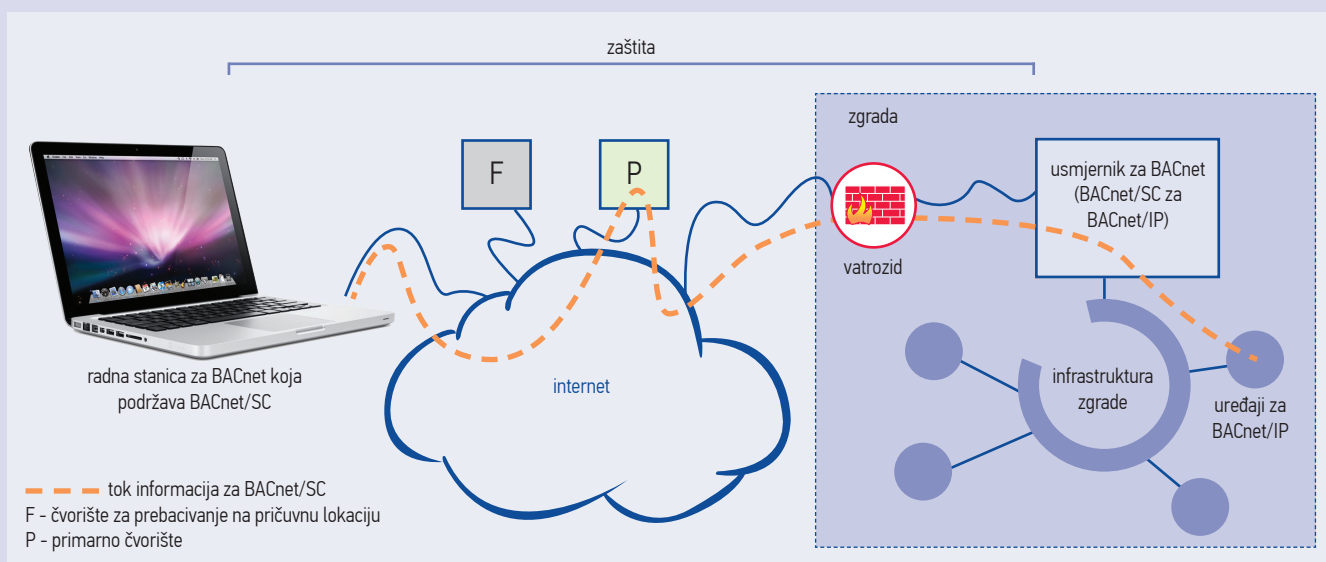
Danas postoji više pristupa za zaštitu infrastrukture za protokol BACnet u zgradarstvu, ali su takva rješenja ponekad složena za primjenu i dodatno opterećuju informatičku potporu. No, razvijeno je rješenje kojim se ostvaruje standardizirana i zaštićena infrastruktura sustava automatizacije zgrade i koja je u cijelosti usklađena s protokolom BACnet i omogućava sva rješenja temeljena na računarstvu 'u oblaku'.

Zbog sve većeg zanimanja za primjenu rješenja koja se osnivaju na primjeni tzv. računarstva u oblaku u sustavima automatizacije i upravljanja zgradama povećala se i potreba za infrastrukturom koja će omogućiti visoku razinu mrežne i informatičke sigurnosti i integritet svih tih sustava. S druge strane informatička struka već ima provjerenjena rješenja koja omogućavaju upravljanje zaštitom komunikacijske infrastrukture i njezinu primjenu.

To je bio razlog zašto je Odbor za BACnet Američkog društva inženjera za grijanje, hlađenje i klimatizaciju (ASHRAE) razvio rje-

šenje pod nazivom BACnet Secure Connect (BACnet/SC). Pojednostavljeno rečeno, njime se omogućava uspostavljanje zaštićene komunikacije između opreme i uređaja u sustavu automatizacije zgrade i preko 'oblaka' i preko lokalne mreže. Pri tome se koriste standardni internetski protokoli i najnovija rješenja za informatičku sigurnost i moguća je jednostavna integracija u postojeću informatičko-telekomunikacijsku (IT) infrastrukturu. Istodobno je BACnet/SC zadržao sve značajke BACneta i usklađen je s postojećim rješenjima za njegovu primjenu, opremom i uređajima koji ga koriste. Tako su

▼ **Ilustracija 1**
Siguran pristup
izvana postojećem
sustavu za BACnet



pojedini proizvođači već označili svoje proizvode i rješenja oznakom 'BACnet/SC ready' i samo ih treba prilagoditi najnovijem standardu.

OSNOVNE PREDNOSTI

Zapravo, BACnet/SC je virtualni podatkovni sloj (eng. data link layer) sa standardnim usmjernikom (eng. router) za BACnet i usklađen je sa svim postojećim uređajima i opremom za BACnet. Time se istodobno može riješiti većina problema s kojima se danas suočava informatička potpora za sustave automatizacije zgrada.

Budući da se BACnet/SC može koristiti u cijeloj mreži, za upravitelje i održavatelje zgrada predstavlja siguran i učinkovit alat za dobivanje svih potrebnih podataka o uređajima i opremi koji se koriste u zgradi i za primjenu rješenja koja se osnivaju na računarstvu 'u oblaku'. Istodobno se mogu izbjeći problemi koje su vlasnici, korisnici, upravitelji i održavatelji zgrada i informatička potpora imali s dosadašnjim proizvodima koji su koristili BACnet.

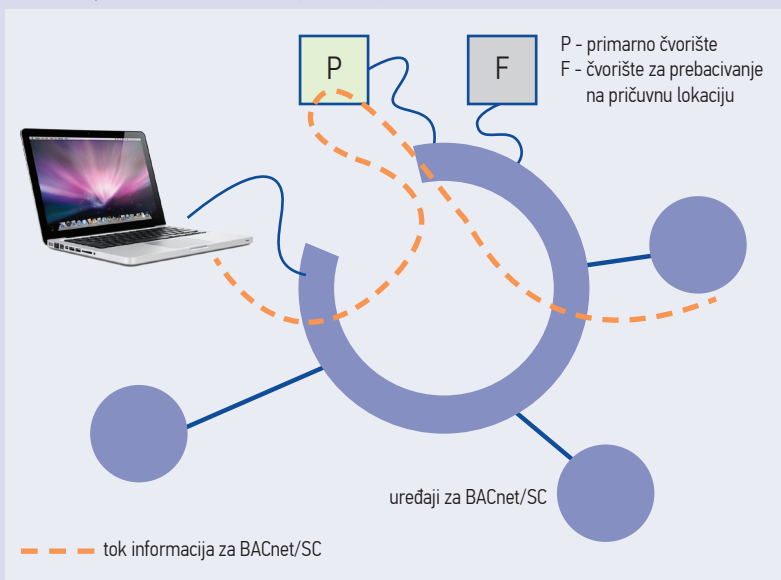
Nekoliko je osnovnih prednosti koje BACnet/SC ima u usporedbi s dosadašnjim rješenjima. Ponajprije, radi se o provjerenom rješenju za mrežnu sigurnost koje se osniva na standardu, pri čemu više nisu potrebe statičke adrese internetskog protokola (IP adrese) i više se ne mora toliko opterećivati informatička potpora. Isto tako, više nisu potrebni ni uređaji za upravljanje emitiranjem za BACnet/IP (BBMDs) ni njihova konfiguracija, a postoji i tolerancija na promjene u topologiji mreže. Također se BACnet/SC ne oslanja na emitiranje poruka i usklađen je sa svim sigurnosnim rješenjima za vatrozid (eng. firewall) koja su uobičajena u IT infrastrukturi. Temelji se na standardnoj sigurnosti TLS 1.2 i ima dodatnu mogućnost kriptografije elipsastim krivuljama sa 128 i 256 bitova.

Uz sve te osnovne značajke, BACnet/SC ima i još nekoliko dodatnih funkcija kao što su:

- mogućnost primjene zajedničkih IP mreža bez potrebe za uspostavljanjem virtualne privatne mreže (VPN)
- mogućnost ostvarivanja mrežnih IP konfiguracija u svim rasponima (od jednostavnih do složenih i od lokalnih do globalnih) bez ikakvih problema i bez utjecaja na postojeće sigurnosne mehanizme kao što su vatrozidovi i podržani prevoditelji mrežnih adresa (NAT)

▼ Ilustracija 2

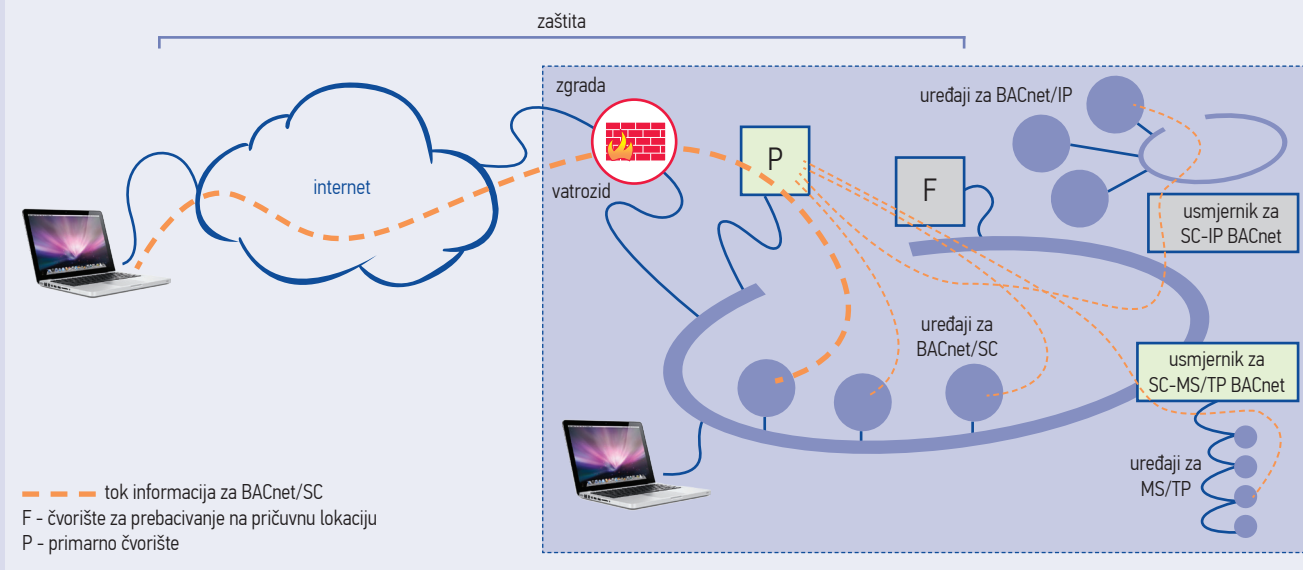
Zaštićeni promet za BACnet u zajedničkoj IP mreži



- siguran prijenos informacija pomoću standardnih sigurnih internetskih utičnica (en. web sockets) za protokol IP kojima se omogućava proširivanje za sigurni protokol HTTPS, a ostvaruje se pomoću kriptografskog protokola TLS
- neovisnost veze o mrežnoj konfiguraciji, uključujući IPv4, IPv6, WLAN i Mobilfunk
- usklađenost sa svim postojećim sustavima, uređajima i opremom za BACnet pomoću normalnog usmjerivanja za BACnet
- primjena zaštitnih mehanizama koji se mogu autentificirati pomoću uređaja i opreme za BACnet i autorizirati za primjenu mreže.

TOPOLOGIJA

Za izmjenu podataka između proizvoljnog broja sudionika u komunikaciji (npr. uređaja ili automatizacijskih stanica) BACnet/SC koristi jedno jedino čvorište (eng. hub). Ono analizira mrežni promet i u skladu s time ga prosljeđuje. Budući da je ono ujedno tzv. jedinstvena točka otkazivanja (eng. single point of failure), tj. točka čiji ispad za posljedicu ima ispad cijelog sustava, BACnet/SC ima ugrađen tzv. mehanizam za prebacivanje na pričuvnu lokaciju (eng. failover mechanism) s čvorištem za takvo prebacivanje (eng. failover hub). Time se osigurava nastavak rada sustava automatizacije zgrade i u slučaju ispada čvorišta, potreba za održavanjem ili nadogradnjom softvera ili hardvera.



▲ Ilustracija 3

Zaštićeni promet za BACnet kod zaštićenih i nezaštićenih (starijih) uređaja za BACnet

TRI SCENARIJA PRIMJENE

Mnogo je načina na koji se BACnet/SC može primijeniti, a najčešća su tri scenarija.

U prvom scenariju radi se o zgradi s postojećim sustavom za BACnet, u kojoj upravitelj ili održavatelj sustavu pristupaju preko interneta (il. 1). Takvo rješenje najčešće se naziva se nadzorom na daljinu ili daljinskim održavanjem, no vatrozid onemogućava pristup samoj mreži u zgradi. U tom se slučaju u zgradu može dodati čvorište za BACnet/SC što uljučuje usmjernik na BACnet za usmjeravanje na postojeći sustav za BACnet, uspostaviti čvorište za BACnet/SC koje je temeljeno na računarstvu 'u oblaku' i koristiti softver za radne stanice čvorišta za BACnet/SC. Upravitelj ili održavatelj zgrada započinje spajanje čvorišta s 'oblakom' i nakon toga može upravljati sustavom automatizacije zgrade i bilo kojim za to prilagođenim tehničkim sustavom u zgradi kao što je radio i ranije.

U drugom se scenariju radi o zgradi u kojoj, prema smjernicama za IT, nije dopušten nezaštićeni promet za BACnet u zajedničkoj IP mreži (il. 2). U tom slučaju svi uređaji za BACnet koji se temelje na protokolu IP trebaju imati potporu za BACnet/SC. Čvorište za BACnet/SC i čvorište za prebacivanje na pričuvnu lokaciju moraju biti instalirani kao dio mreže.

Konačno, u trećem je scenariju riječ o zgradi u kojoj se koriste zaštićeni i nezaštićeni (stariji) uređaji (il. 3). Tada se primarna i čvorišta za prebacivanje na pričuvnu lo-

kaciju nalaze u vatrozidu i služe za zaštitu uređaja za BACnet/SC u sustavu. Usmjernik od BACnet/SC-a do BACnet/IP-a omogućava vezu zaštićene mreže za BACnet/SC i starije mreže za BACnet. Pri tome se usmjernik za BACnet/IP može koristiti kao usmjernik za MS/TP, a takav usmjernik proširuje zaštićeni pristup do krajnjih uređaja ili opreme.

DUG PUT DO NORME

Odbor za BACnet ASHRAE SSPC 135 je 2016. godine predstavio BACnet Secure Connect (BACnet/SC) kao 'Dopunu dokumentu 135-2016bj za BACnet'. Potom je uslijedilo objavljivanje na Vijeću direktora ASHRAE-ja i prihvaćanje kao norme Američkog nacionalnog instituta za normizaciju (ANSI) u veljači ove godine na Zimskom sastanku ASHRAE-ja u Orlando na Floridi u Sjedinjenim Američkim Državama. Konačno, pokrenut je i postupak kod Međunarodne organizacije za normizaciju (ISO) i Europskog normizacijskog odbora (CEN), što bi trebalo završiti preuzimanjem EN ISO 16 484-5 kao nacionalne norme u svim članicama CEN-a. Procjenjuje se da će taj postupak trajati do dvije godine.

No, proizvođači već na raspolaganju imaju američku normu (ANSI) za primjenu pojedinih zahtjeva u razvoju proizvoda koji koriste BACnet/SC, a projektanti i investitori također se već mogu pozivati na ASHRAE/ANSI Standard 135. Time je otvoren put prema sigurnom i zaštićenom umrežavanju proizvoda svih proizvođača opreme i uređaja u zgradarstvu s komunikacijskim protokolom BACnet. ■

IzvorNIK:

www.cci-wissensportal.de