VAN – sistem

Vladimir Hunjadi
Ptujska c. 12b
2270 Ormož
vlado.hunjadi@gmail.com

VAN System

The works deals with an interesting technology for purposes of industrial automation. The Virtual Automation Networks (VAN) technology is an advanced Ethernet- based industrial communication system which much better corresponds to requirements of industry than all existing Industrial Ethernets. It enables an effective cooperation of puplic and private networks with a stress on security, safety and real time properties. It solves also problems with implementation of different wireless technologies into heterogeneous communication structure of distributed industrial automation system. Author present main problems of the virtual automation network as architecture, technological platform, network topology and device profiles in an overview. Finally, principal questions of the name-based routing, and OpenVPN tunneling is explained.

Kratek povzetek prispevka

Prispevek obravnava zanimivo tehnologijo za namane industrijske avtomatizacije. VAN tehnologija je napredna, na Ethernet-u osnovan industrijski komunikacijski sistem, ki se veliko bolje odziva na zahteve industrije, kot pa vsi obstoječi industrijski Ethernet-i. Omogoča učinkovito sodelovanje javnih in zasebnih omrežij s poudarkom na varovanju, varnosti in lastnostih realnega časa. Rešuje tudi težave z vpeljevanjem različnih brezžičnih tehnologij v heterogene komunikacijske strukture razdeljenih industrijskih avtomatizacijskih sistemov. Avtor predstavlja v pregledu glavne težave virtualnega avtomatizacijskega omrežja, kot tudi arhitekturo, tehnološke platforme, topologijo omrežja in profile naprav. Nazadnje pa so še razložena osnovna vprašanja na imenu temelječega usmerjanja in tuneliranja odprtega navideznega zasebnega omrežja (OpenVPN).

1 Virtualna avtomatizacijska omrežja (*ang.: Virtual Automation Networks - VAN*): rešitev za heterogena avtomatizacijska omrežja v proizvodnji

Veliko časa je preteklo, odkar so bili na Ethernet-u osnovani industrijski komunikacijski sistemi. Veliko jih je bilo standardiziranih in dokazanih, da so v uporabi učinkoviti in funkcionalni.

Dejstvo je, da je z industrijskega vidika največja pomanjkljivost na Ethernet-u osnovane komunikacije to, da je bil Ethernet serijsko vodilo s stohastično metodo dostopa. Na srečo je znani CSMA/CD, v Ethernet-u poznan kot algoritem izogibe kolizije, izgubil lastnost kolizije in je bil spremenjen v nezamašitveni zaradi stikal, ki so zamenjala zvezdišča (hub) in CAT kable, ki so zamenjali koaksialne kable. Razlog za to je, da so se z vzponom zgoraj omenjenega, domene trčenj, oblikovane s strani celotnega segmenta, prišle so na komunikacijo od točke do točke s PC karticami omrežnega vmesnika *(ang.: PC NIC - Network Interface Card)* in NIC stikali *(angl.: NIC Switch)*. Čeprav je bil stohastični element CSMA/CD-ja zmanjšan, je bila težava determinizma daleč od rešene. Nove težave s trčenjem so bile faktorji za uničenje determinističnega obnašanja, ki bi bilo dobrodošlo v industrijski komunikaciji. Prevladujoča težava na tem področju je prenasičenost izhodnih vrat. Zato na Ethernet-u osnovane rešitve za industrijsko avtomatizacijo uporabljajo različne pristope za zagotavljanje komunikacijskega determinizma. Nekatere tehnologije uporabljajo ciklično delovanje, druge uporabljajo virtualni obroč z žetonom (*angl.: token ring*) in tretje uporabljajo TDM (*angl.: Time Division multiplex*) za zmanjševanje trčenj paketov na vratih stikal. Razen tega ima vsaka tehnologija svoj pristop za zmanjševanje sklada prekoračitve *(angl.: Stack overhead)* z uporabo obvoza sklada *(angl.: Stack bypassing,* ali celo z razširjenjem strojne opreme NIC-ov. Z zaključitvijo tega evolucijskega koraka so bila za komunikacijo posameznega segmenta uspešno rešena vprašanja determinizma.

Zaradi razširjanja na fizične in povezovalne sloje na Ethernet-u osnovanih področnih vodil (fieldbus) je bilo vpeljevanje le-teh v kompleksno omrežje razdeljenih krmilnih sistemov v tovarne daleč od določevanja brezhibne rešitve, skupaj z nadzorom preobremenitve.

Ta pomanjkljivost je najbolje vidna v dejstvu, da je izvajalni čas komunikacije omejen. Na primer, čas izvajanja komunikacije ne more premostiti meje LAN segmenta njegovih garantiranih hitrost. Nasprotno pa nekatere na Ethernet-u osnovane rešitve ne dovoljujejo dodatnega TCP/IP prometa brez izvajalnega časa v svojih nadzornih domenah, še posebej, ker je bila originalna Ethernet metoda dostopa preveč spremenjena.

Komunikaciji mora biti preprečeno, da bi bila preveč odprta zaradi tveganj v varnosti, ki jih prinaša v industrijsko komunikacijo Ethernet je odprti standard. Zato bi lahko nekdo pomislil, da je ta omejitev dobrodošla, razen v primeru, če je treba izvesti naprednejšo komunikacijo. Prišli smo do točke, kjer smo spoznali pomanjkljivosti obstoječe, na Ethernet-u osnovane komunikacije v industrijski avtomatizaciji. Prepoznali smo številna glavna nerešena vprašanja in poskušali najti rešitve za:

- **Vključevanje brezžičnih tehnologij**; še posebej cenjen bi bil 802.11 (WLAN), saj je WLAN semantično najbolj primeren za TCP/IP komunikacijo. Razen tega je ZigBee tehnologija smatrana kot možna za razširjanje zmožnosti komunikacije.
- **Komunikacija v realnem času** je že bila razrešena za na Ethernet-u osnovana področna vodila (fieldbus). Obnašanje je zagotovljeno samo za samostojne LAN segmente, saj je komunikacija skupnega izvajalnega časa najpogosteje poenostavljen povezovalni sloj in je ne moremo usmerjati. Zagotovljena mora biti komunikacija v realnem času preko bolj kompleksnih infrastruktur. To se zahteva predvsem pri sinhronizaciji robotskih naprav in osi robotov ter proizvodnih strojev v proizvodnji.

- **Funkcionalni varnostni mehanizmi so potrebni** za zagotavljanje zanesljivosti in razpoložljivosti komunikacije ne glede na spodnje fizične sloje; potemtakem temeljijo na principu črnega kanala.
- **Varnostna tveganja se pojavijo**, če je komunikacija izpostavljena z zunanjim omrežjem in njenimi negativnimi vplivi. Zato postane komunikacija bolj ranljiva v primerjavi z zapuščino področnih vodil. Značilna količina podatkov izvajanega časa je podvržena poslovni skrivnosti (zapisi, oblike, itd.).
- **Pisarniške in telekomunikacijske tehnologije** bi priskrbele sredstva za oddaljeno administracijo in upravljanje. Mehanizmi za preklop med ponudniki *(angl.: Provider Switching)* morajo biti integrirani, da bi bila pod različnimi pogoji zagotovljena komunikacija.

2 Virtualna avtomatizacijska omrežja

V VAN-u si prizadevamo za razvoj odprte, univerzalne, brezhibne, multi prodajno omrežne rešitve, ki bo lahko povezala heterogene komponente in industrijsko avtomatizacijo od enega senzorja v eni tovarni do oddaljenih mehanizmov v decentraliziranih podjetjih po vsem svetu. VAN-ova povezovalna komunikacija je lahko realizirana preko področnih vodil, pisarniških omrežij in celo javne komunikacijske infrastrukture – žično ali brezžično.

Način za uvedbo brezhibne, unikatne, transparentne in povezovalne komunikacije v heterogeno ogrodje, ki je sestavljeno iz področnih vodil (fieldbus), industrijskih Ethernet-ov, zasebnih LAN-ov in javnih omrežij (osnovanih na različnih medijih in tehnologijah transporta), so virtualna omrežja. V tem prispevku je predstavljena ideja in trenutni razvoj takih komunikacijskih sistemov za avtomatizacijo z imenom VAN. Glavne zahteve za predstavljene rešitve so slednje:

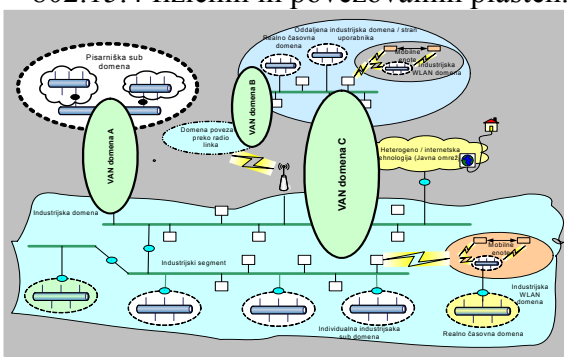
a. **Rešitev mora uporabljati IEC 61158 standard.** Na novo niso predstavljena nobena nova področna vodila (fieldbus) ali industrijski Ethernet sistemi, ampak so za nadzor in v komunikacijske namene uporabljene in vgrajene že obstoječe industrijske rešitve.

b. **VAN je skrita infrastruktura**, ki posnema lastnosti komunikacijskih entitet v geografsko razdeljeni komunikacijski strukturi preko zasebnih kot tudi javnih omrežij.

c. **Povezava med geografsko razdeljenimi avtomatizacijskimi domenami** uporablja varno tunelirano komunikacijo, ki jo zagotavlja VAN z uporabo infrastrukture različnih ponudnikov internetnih storitev (ISP) in ponudnikov telekomunikacijskih storitev (TSP) z namenom, da se izvaja najbolj primerno izmenjevanje podatkov med entitetami. Ko so tuneli med domenami ustvarjeni, se izmenjevanje podatkov izvajajo na enak način kot med lokalnimi industrijskimi domenami, ki so podrobneje označene s skladnimi IEC 61158 in IEC 61784 standardi.

d. **Naslavljanje v VAN omrežjih bo temeljilo na imenih** (*ang.: Name-Based Addressing*), da se izognemo zapletom z IP naslovi, ki se jih ne da usmerjati, saj so obširno uporabljeni v industriji, ter da bodo tako izpolnjevali cilj oblikovanja brezhibne rešitve.

e. **Zaradi pojavljajočih se trendov v brezžični komunikaciji** je arhitektura VAN-a oblikovana tako, da spoštuje integriranje brezžičnih povezav, ki prevladujoče temeljijo na IEEE 802.11 in 802.15.4 fizičnih in povezovalnih plasteh.



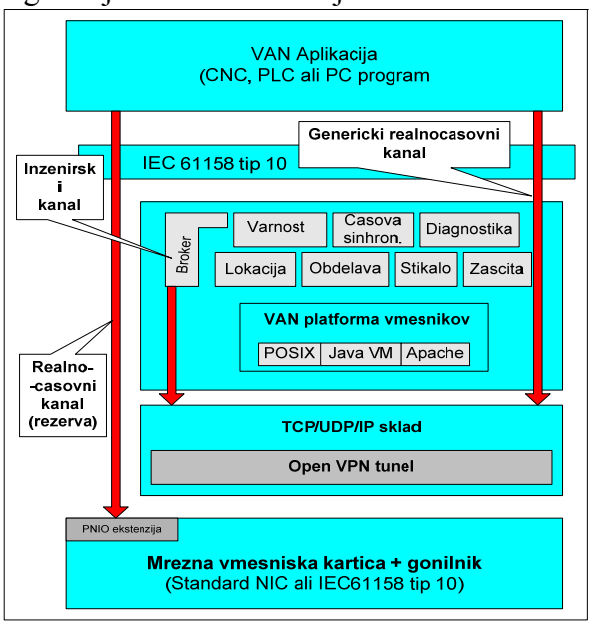
Slika 1: VAN domene

Vir: "Virtual Automation Networks", Invited Session Proposal for IFAC World Congress, Peter Neumann and Ulrich Jumar, 2008.

Na sliki 1 je prikazano heterogeno avtomatizacijsko omrežje. Sestavljeno je iz posameznih industrijskih domen in nadalje strukturirano v segmente in poddomene (*ang.: subdomains*) ter eno pisarniško domeno. Podjetje, ki vsebuje takšne domene, je lahko geografsko razdeljeno v več obratov. Povezava med vsemi domenami je zagotovljena s strani javnih omrežij. V eni domeni lahko zasledimo tako žične kot brezžične povezave med domenami in segmenti. Nekatere poddomene so v realnem času, druge pa ne zahtevajo lastnosti realnega časa. Obstajajo dodatne zahteve po funkcionalni varnosti glede na standard IEC 61508 v večini industrijskih domen (npr. fleksibilne produkcijske celice z roboti in drugo). Njihova integracija oblikuje eno izmed zelo pomembnih VAN funkcionalnosti - domen. Vsi privatni in javni komunikacijski segmenti imajo natančne zahteve, kar se tiče varnosti podatkov. Reševanje varnostnih vprašanj predstavlja eno glavnih težav sistema VAN. Z varnostnega vidika si realni čas in varnostne zahteve nasprotujejo. Implementacija varnostnih ukrepov predstavlja dodatno zamudo z močnim potresavanjem (*ang.: jitter*), ki negativno vpliva na delovanje v realnem času.
Slika 1 prikazuje princip virtualizacije. Ne glede na prostorsko razporeditev fizičnih domen in posameznih naprav, bodo virtualne VAN domene povzročile, da zgleda, kot da so vse naprave v enem segmentu, tako pri naslavljanju kot tudi razpoložljivost/dostopnosti.

3 Arhitektura naprav in tehnološka platforma

Ta del predstavlja tehnološko platformo VAN-a kot temelj prihodnje naprave VAN.
Tehnološka platforma odraža vse potrebne vire naprav glede strojne in programske opreme, namenjene za naprave VAN.
Hierarhična struktura tovarniške avtomatizacije zahteva drugačne vire različnih tehnoloških stopenj. Na primer, stopnja operaterja *(ang.: Operator Level)* vedno temelji na platformah (pogosto na pisarniških PC-jih) z operacijskim sistemom. Na drugi strani, stopnja nadzora procesov *(ang.: Process Control Level)* uporablja ICP ali PLC. Posledično mora biti platforma dogradljiva. Jasno je, da naprava z enim procesorjem ni dovolj zmogljiva, da bi zadovoljila več komunikacijskih skladov naenkrat, kar je nujno pri skoraj vseh VAN napravah.
Eden izmed osnovnih namenov rešitve VAN - sistema je bila ne le razvoj novih, temveč tudi razširitev že obstoječih naprav, saj tak način zagotavlja učinkovit razvoj.



Slika 2: Tehnološka platforma
Vir: Virtual Automation Networks: A Solution for Heterogeneous Automation Networks in Manufacturing, Frantisek Zezulka, Jan Bera; University of Technology, Brno 2009.

Z upoštevanjem funkcionalnih zahtev naprav VAN in domnev je bilo odločeno, da se uporabijo izključno naprave, snovane na progranski opremi. Vendar bo zaradi jasnih trendov na tem področju platforma neodvisna od programske opreme. Primarno se razmišlja o Windows XP, Linux-u in OpenBSD-u. Slika 2 prikazuje podrobneje opisano tehnološko platformo.

4 Vmesniki VAN omrežja

Spodnji del slike 2 (kartica omrežnega vmesnika + gonilniki) predstavlja komunikacijski vmesnik naprave VAN. Platforma je bila oblikovana na tak način, da podpira klasično kartico omrežnega vmesnika - NIC *(ang.: Network Interface Card – NIC),* vse pričakovane standarde, povezane z IEEE

802.3 in superiorne komunikacijske sloje (TCP/UDP/IP).
Na izbiro bo tudi, ne glede na ostale standarde, IEC 6158 Type 10 (Profinet). Ta standard se kaže kot zelo obetajoč, še posebej po implementaciji funkcije RToverUDP z avtomatizacijo instrumentalnih avtomatov *(ang.: Instrumental Vendors*). RToverUDP omogoča usmerjeno komunikacijo, snovano na UDP datagramih z zmanjšanim »overheadom« procesiranja skladov. Večina komunikacij v realnem času je ciklična ter tako vnaprej določena. Odnos med ponudnikom in potrošnikom, ciklični čas izvajanja (run-time) komunikacije so znani že vnaprej. Princip realnega časa preko UDP (*ang.: Real Time over UDP*) izkorišča te pogoje in vnaprej sestavi vsebino UDP paketa v spomin specializirane NIC. Komunikacijo sproži NIC časovnik. Tovor koristne podatkovne vsebine (*ang.: payload*) je posodobljen, nadzorna vsota (*ang.: checksum*) je izračunana in paket je poslan. Zato so »overheadi«, ki nastanejo s potovanjem skozi sklade, implementirani s programsko opremo in eliminirani. Rečemo lahko, da alarme sprožajo dogodki ter da potekajo v realnem času. Zato se prilegajo v ta pristop. Leva rdeča puščica (slika 2) predstavlja komunikacijo za realni čas, najbolj občutljivo na podatke. Aplikacija komunicira s podaljškom NIC-a (*ang.: NIC extension*) preko objektnega modela VAN, ki je snovan na standardu IEC 61158, odvisno od implementacije.
Poleg Ethernet vmesnikov lahko po manjših modifikacijah uporabimo tudi druge tipe. Glede na dejstvo, da je oblika platforme odprta in dogradljiva, lahko naprave brez težav prilagodimo različnim vmesnikom.

5 TCP/IP sklad in tuneliranje OpenVPN

Platforma vsebuje TCP/UDP/IP sklad za izvajalno (run-time) komunikacijo, ki ne poteka v realnem času (desna rdeča puščica, slika 2), ter strojno in upravljalno (inženirsko) komunikacijo (sredinska rdeča puščica). Sklad je razširjen z *OpenVPN (ang.: Open Virtual Private Nerwork*). Ta entiteta zagotavlja dve pomembni funkciji: daje nam možnost, da šifriramo podatke in povečamo njihovo zaščito, ter zagotavlja komunikacijsko razmerje naprava-naprava, ne glede na topologijo omrežja. Vsakemu določenemu komunikacijskemu razmerju je dan unikaten OpenVPN tunel tako, da lahko posamezna naprava operira s številnimi tuneli istočasno.
Tehnološka platforma uporablja napravo VPN TAP. Ta naprava zagotavlja povezavo pri L2. To dejansko pomeni, da je vstop tunela uporabniku na razpolago v obliki vmesnika L2 (virtualna Ethernet kartica) z unikatnim naslovom MAC. V izvajalnem času (run-time) se tuneliranje OpenVPN kaže na tak način, da TCP/IP vmesnik, skozi katerega poteka komunikacija, ne spusti Ethernet tovora, IP glave, tovora in noge do Ethernet vmesnika, ampak do virtualnega vmesnika OpenVPN. Instanca tunela OpenVPN vzame to vsebino in jo ponovno zavije, kar temelji na predhodno dogovorjenih informacijah. Če je potrebno, je vsebina šifrirana. Instanca tunela potem pošlje paket pravemu Ethernet vmesniku. Funkcija tunela OpenVPN je podprta v vseh dostopnih točkah - VAN-AP *(ang.: VAN Access Point – VAN-AP)* tako, da bi lahko paket nemoteno potoval skozi heterogeno infrastrukturo. Pomanjkljivost tega pristopa je povečan časovni »overhead« te instance. Vendar zaradi dejstva, da platforma ponuja komunikacijski kanal v realnem času za kritične podatke, je ta pristop temeljito podkrepljen.

6 VAN sklad in vmesniki

VAN sklad predstavlja glavni priključek do naprav, ki jih dobavlja konzorcij VAN. Vsa funkcionalnost VAN-a je zbrana v tem skladu, ki omogoča strojne, konfiguracijske in nadzorovalne storitve ter skladiščenje podatkov.
Aplikacijski storitveni elementi - ASE-ji (*ang.: Application Service Elements*) skrbijo za osnovno funkcionalnost VAN-a. Vsak ASE predstavlja hierarhično strukturo parametrov, ki tvori vmesnik do sorodnih storitev. Vsak od teh parametrov je lahko bran in/ali napisan, odvisno od tipa in pravice dostopa. ASE-ji so oblikovani v XML-u (*ang.: Ekstensible Markup Language*) z uporabo dedovanja. Tako generična predloga definira semantiko skladnosti XML-a. Vsi kasnejši ASE-ji so podedovani, dodanih je več specifičnih

informacij. Operacije ASE-ja beri/piši so osnovane na zahtevo Web servisa - WS *(ang.: Web Service*). Zahtevan ASE vrne odgovor, ki vsebuje potrditev želenih sprememb ali želenih podatkov. Sprememba parametra vpelje postopek, ki je povezan s parametrom in njegovo vrednostjo.
Komunikacija z ASE-ji in sorodnimi storitvami je osnovana na WS-ju (*ang.: Web Services*). V implementaciji VAN-a je zahteva/odziv (*ang.: request/responce*) osnovan na XML-u, kot je opisano zgoraj. Povezava med storitvijo in zahtevo je osnovana na enostavnem objektnem dostopnem protokolu - SOAP-u (*ang.: Simple Object Access Protocol*). Zahteve in odzivi so poslani skozi protokol HTTP. Zato potrebujejo ASE-ji spletni strežnik, ki lahko sprejema povezave in zahteve.
Na primer, varnostni ASE varuje dostopno nadzorovano listo - ACL (*ang.: Acess Control List*), časovna sinhronizacija ASE (*ang.:TimeSync ASE*) zagotavlja storitve za časovno in ciklično sinhronizacijo, rutina ASE pa zagotavlja funkcionalnost na imenu temelječega usmerjanja (*ang.: Name-based routing*), podrobneje opisanega v nadaljevanju. Slika 2 vsebuje množico vseh ASE-jev za poenostavitev.
Ker mora biti implementacija neodvisna od operacijskega sistema, je vmesnik med skladom VAN in OS osnovan na POSIX-u, Java VM ter Apache-ju.
Java VM in Apache sta orodji, neodvisni od platform, in omogočata napravi VAN, da izvaja aplikacije in postopke, ki jih potrebuje SOAP (*ang.: Simple Object Access Protocol*) ter poganja strežnike WS. POSIX oskrbuje sklad VAN s poenotenim vmesnikom za storitve operacijskega sistema.

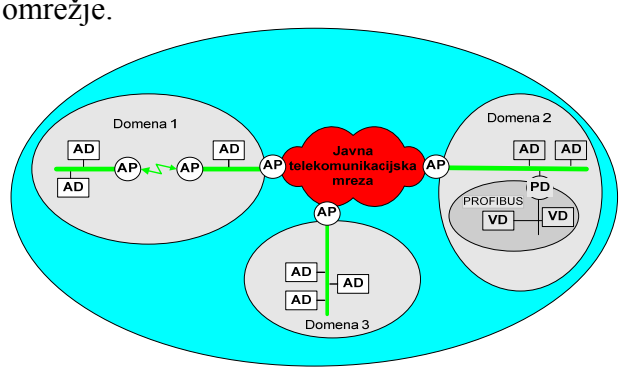
7 Objektni modeli komunikacije

VAN objektni model bo skladen z izvajalnim objektnim modelom Profineta (IEC 61158 Type 10) pri prvotni implementaciji. Vendar je arhitektura oblikovana na tak način, da je odprta za priključke k drugim izvajalnim objektnim modelom. Ta korak zagotavlja preprosto migracijo že obstoječih Profinet in Profibus aplikacij za VAN, kar pomeni, da že razvitih aplikacij ne bo treba znova pisati, temveč bodo prenosljive.

8 Topologija omrežja in profili naprav

V tem delu je predstavljen topološki koncept VAN omrežja skupaj z novimi pristopi k usmerjanju (routing) v heterogenih omrežjih.
Topologija je osnovana na zapleteni topologiji, saj lahko nepotrebna povezava alternativno razširi drevesno topologijo. Topologija lahko pravzaprav vsebuje več tipov povezav. Osnovna tehnologija je Ethernet, ki uporablja TCP/IP in tehnologijo IEC 61158 Type 10 (Profinet). Razen teh, lahko omrežje gosti telekomunikacijska omrežja, če so razpoložljivi primerni vmesniki. Nenazadnje, razmišlja se tudi o brezžičnem standardu 802.11.
Komunikacija preko javnih omrežij prinaša precejšnjo heterogenost, ki zmanjšuje prepustnost za določene tipe prometa (signaliziranja, upravljanje omrežja, prenos podatkov v realnem času (*ang.: run-time*), nadzorovanje in druge storitve). Primer heterogene topologije je prikazan na sliki 3. Zato morajo obstajati profili naprave z imenom VAN dostopna točka VAN-AP (*ang.: VAN Access Point*), ki upošteva meje med domenami VAN, ki jih ločujejo javna omrežja. VAN dostopne točke upravljajo tudi s prehodi tunelov Open VPN, če tunela ni mogoče virtualno vzpostaviti. VAN-AP-ji prav tako opravljajo varnostne funkcije, saj vzdržujejo dostopno nadzorovano listo−ACL (*ang.: Acess Control List*) in dovolijo/prepovejo dostop komunikacije do specifičnih vmesnikov. VAN-AP vsebuje le komunikacijsko funkcionalnost in ne avtomatizacijske funkcionalnosti. Zato bi to morale biti močne naprave, ki brez težav urejajo vse operacije, povezane z omrežji.
Kompatibilnost za nazaj, torej z obstoječimi industrijskimi rešitvami, mora biti zagotovljena, da podaljša življenjsko dobo obstoječih aplikacij. Zato morajo obstajati profili naprave, z imenom VAN-PD (*ang.: VAN Proxy Device*), ki zagotavljajo

integracijo naprav, ki niso naprave VAN, v omrežje.



Slika: 1: VAN mrežna topologija
Vir: Virtual Automation Networks: A Solution for Heterogeneous Automation Networks in Manufacturing, Frantisek Zezulka, Jan Bera; University of Technology, Brno 2009.

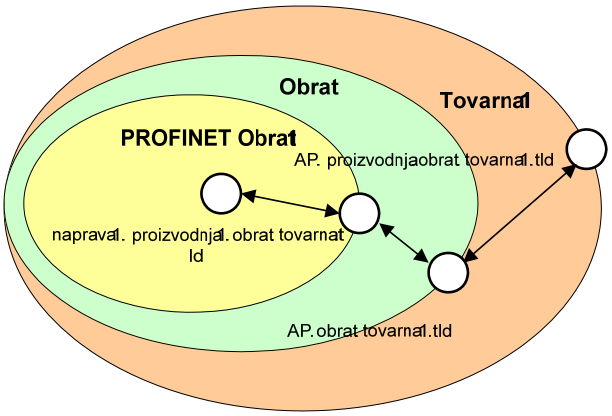
V tem primeru bi z objektnim modelom VAN, ki bi bil integriran v napravo, usposobljeno za VAN, upravljal VAN-PD, medtem ko bi z obstoječo aplikacijo upravljala naprava, ki se jo integrira. Ta naprava se imenuje virtualna naprava VAN-VD (*ang.: VAN Virtual Device*). Takšen pristop zagotavlja, da na noben način ni treba širiti virtualne naprave. Breme funkcionalnosti VAN-a v celoti nosi VAN-PD (*ang.: VAN Process Device*).
Nenazadnje se naprava, usposobljena za VAN (*ang.: VAN-enabled devices*), imenuje avtomatizacijska naprava VAN-AD (*ang.: VAN Automation Device*). VAN-AD vedno izvaja komunikacijo kot tudi avtomatizacijsko funkcionalnost, zato arhitektura obsega poln sklop entitet iz slike 3.

9 Na imenu temelječe usmerjanje (ang.: Name-Based Routing)

Vzpostavljanje povezav med napravami, ki so v celoti transparentne, zahteva naslovljivost vsake naprave s strani vsake naprave. Nekatera dejstva podkrepijo na imenu osnovano usmerjanje:

- Naslovi, ki jih uporabljajo obstoječa industrijska področna vodila (*ang.: Industrial Fieldbuses*), so ponavadi zasebni naslovi. Na primer, tipični segment področnega vodila, ki je osnovan na Ethernetu, je 192.168.1.0/24. Tako komunikacije ni mogoče usmerjati brez funkcij NAT/PAT. Vendar uporaba protokola NAT/PAT ni primerna v kombinaciji s tuneliranjem.
- Na splošno je naslavljanje naprave z IP naslovom nepriročno. Še posebej ni sprejemljivo, da operiramo na tako nizki stopnji v virtualiziranih omrežjih, ki želijo doseči stopnjo VAN omrežja. Naslavljanje z imeni je bolj priročno.
- Če upoštevamo heterogena omrežja, je lahko naslavljalna shema (*ang.: addressing scheme*) inkorporirane tehnologije (npr. ISDN), ki se razlikuje od Ethernet-a, popolnoma drugačna, verjetno celo brez uporabe IP naslovov.

Celoten koncept na imenu bazirane rutine - NBR (*ang.: Name-Based Routing*) se opira na funkcionalnost VAN-AP-jev. Za pričakovati je, da bo naprava morala razvozlati naslov, ko bo hotela komunicirati s partnerjem.
Vsaka naprava VAN mora imeti VAN ime. Ime predstavlja hierarhično določnost konteksta naprave in njenega imena z uporabo točkovnega dogovora. Na primer, ime VAN naprave je lahko: *device1.floor1.-plan1t.company1.tld* ali *(slov.: naprava1. proizvodnja1. obrat1. podjetje1.tld)*. *Tld* del predstavlja ime omrežja, VAN. *device1* predstavlja unikatno ime naprave v lokalnem segmentu VAN-a. Vse ostalo predstavlja hierarhično strukturo omrežja. Slika 4 prikazuje, kako je bilo omenjeno VAN ime izpeljano iz strukture VAN omrežja.
Rešitev naslavljanja z VAN imenom je omogočena s povezanimi zahtevami med VAN-AP-ji, ki zagotavljajo funkcionalnost za ta namen. Vsaka meja domene mora imeti VAN-AP.
Razvozlanje naslova naprave se zgodi le na začetku komunikacije. Ko so naprave dosežene, je tunel OpenVPN vzpostavljen, podatki o času izvajanja (*ang.: Run-Time Data*) pa se lahko prenesejo z rabo tunela OpenVPN.



Slika 1: Koncept na imenu bazirane rutine
Vir: Virtual Automation Networks: A Solution for Heterogeneous Automation Networks in Manufacturing, Frantisek Zezulka, Jan Bera; University of Technology, Brno 2009.

10 Preklapljanje ponudnikov (*ang.: Provider switching*)

VAN-AP ponuja še drugo funkcionalnost za povečanje razpoložljivosti komunikacije. Osnovan na prej definiranih parametrih opazovane komunikacijske metrike, npr. latenci, potresavanju (*ang.: jitter*), izgubi paketov, širokopasovni povezavi (bandwidth), itd., lahko VAN-AP odloči, da preklopi na drugačno komunikacijsko povezavo na vnaprej definiranih sprožilnih (*ang.: trigger*) parametrih. Taka povezava je ponavadi osnovana na drugačnem fizičnem sloju in omogočena s strani drugega ponudnika, da zagotovi primerno redundanco povezav. Na ta način lahko VAN omrežje reagira na obstoječe ali prihodnje izgube povezav in zagotovi preprost avtomatični preklop.

11 Zaključek

Od VAN koncepta se pričakuje razvoj odprte, univerzalne, brezhibne omrežne rešitve, ki bo lahko povezala heterogene komponente in industrijsko avtomatizacijo z enega senzorja v eni tovarni do oddaljenih mehanizmov v decentraliziranih podjetjih po vsem svetu. Povezovalna komunikacija VAN-a se lahko realizira s pomočjo industrijskih (področnih) vodil, pisarniških omrežij in celo javne ali zasebne komunikacijske strukture - žične ali brezžične.

Implementacija rezultatov raziskave in razvoja VAN-a omogoča efektivno sodelovanje javnih in zasebnih omrežij s poudarkom na varovanju, varnosti, lastnostih realnega časa ter integraciji različnih brezžičnih tehnologij v heterogeno komunikacijsko strukturo distribuiranih industrijskih avtomatizacijskih sistemov. Članek obravnava predvsem tehnične podrobnosti tehnološke platforme kot osnovo za arhitekturo naprav. Tehnološka platforma odraža vse potrebne vire naprav, tako strojno, kot tudi programsko opremo, namenjeno za naprave VAN.
Glede na navedeno ponuja VAN univerzalno rešitev povezovanja po vsem svetu, in sicer povezavo komponent v procesu avtomatizacije v tovarni iz enega senzorja v napravi do decentraliziranega podjetja. VAN interoperabilnost komunikacije se lahko uresniči prek vseh znanih komunikacijskih omrežij, javnih in privatnih, žičnih ali brezžičnih. Vključevanje VAN omrežja bo omogočilo vzpostavitev komunikacijske veleprometnice, zmožne konstantno spremljati svoje stanje ter stanje avtomatiziranih segmentov ter tudi ukrepe in o tem samodejno obveščati s konkretnimi ukrepi. To tudi omogoča omrežju elegantno preprečevanje lokalne okvare ali nadzora nad proizvodnim procesom.
Platforma je bila oblikovana na tak način, da podpira klasičen NIC (*ang.: Network Interface Card*), vse pričakovane standarde povezane z IEEE 802.3 in superiorne komunikacijske sloje (TCP/UDP/IP). Ne glede na standarde, izbran je Standard IEC 61158 Type 10 (Profinet).
Edini pomislek pri uporabi teh heterogenih omrežjih je neželjen vdor v mrežo. Čeprav so uporabljeni vsi možni ukrepi za preprečitev tega, pa vseeno vemo da popolne zaščite ni. Prvi prototipi, ki so v fazi realizacije in čas bodo ta pomislek potrdili ali pa odvrgli.

12 Literatura

[1] *http://www.van-eu.eu/projestinfo*
[2] *http://www.van-eu.eu/sitemenu*
[3] *Virtual Automation Networks: A Solution for Heterogeneous Automation Networks in*

Manufacturing, Frantisek Zezulka, Jan Bera; University of Technology, Brno 2009.
[4] *http://www.van-eu.eu/publications*
[5] *http://www.van-eu.eu/workpackages*
[6]*http://www.van eu.eu/generaldownloads*
[7] *http://www.van-eu.eu/objectives*
[8] *Deliverable D01.3-1V 1.01 "Final Evaluation and Conclusions", The VAN Consortium, 2009*