

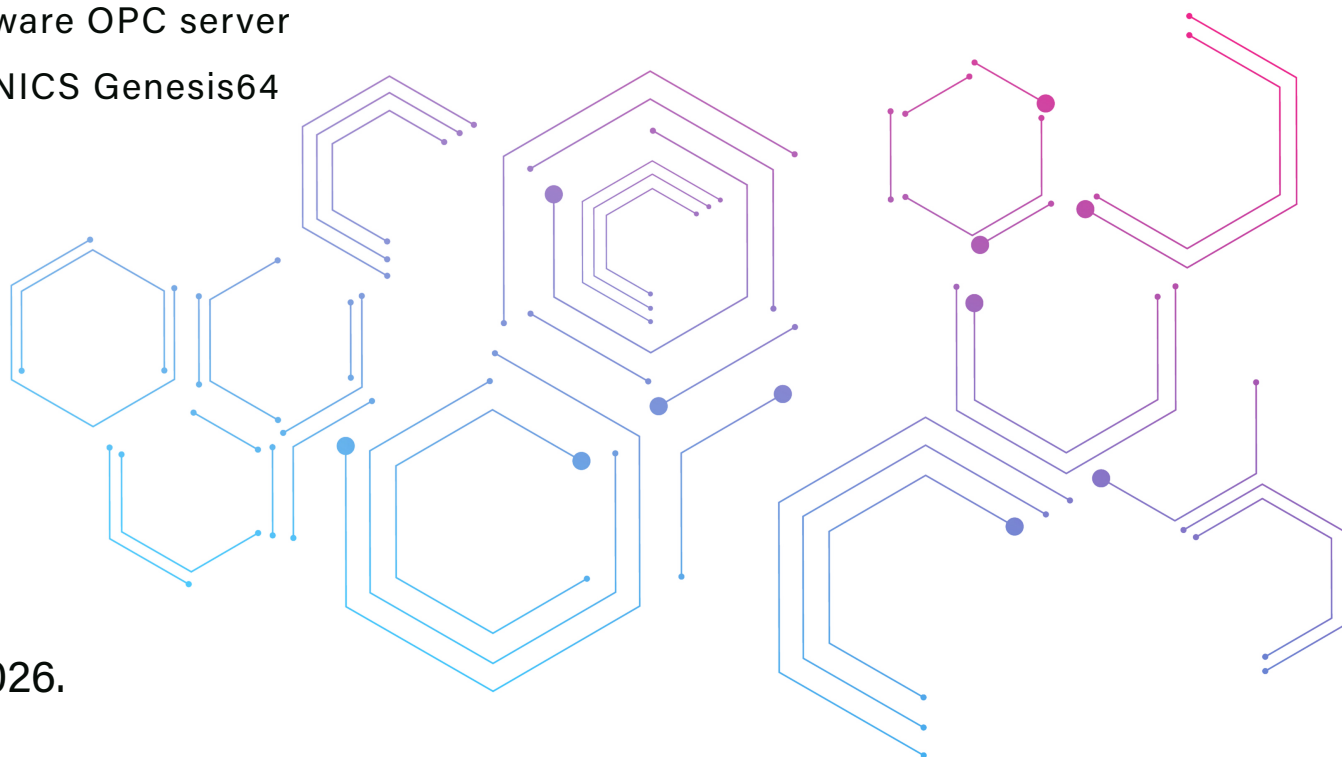


 **RBT**  
TECHNOLOGIES

# Opis izvedene rešitve

Digitalizacija in komunikacija /// kovinskopredelovalna industrija

- Anybus Defender
- Kepware OPC server
- ICONICS Genesis64



Januar, 2026.

# OPIS PROBLEMA

## Začetna situacija

Proizvodno podjetje, ki proizvaja aluminij, ima v strojnem parku več različnih proizvodnih linij, ki delujejo kot samostojne celote. Glavni krmilnik na linijah je Siemens S7-1200. Vse proizvodne linije komunicirajo preko Profinet komunikacije, problem pa nastane zaradi dejstva, ker imajo vsi PLC krmilniki identične IP naslove. Identični IP naslovi onemogočajo enostavno povezovanje skupno osmih proizvodnih linij na eno centralno točko ter integracijo v SCADA sistem brez dodatnih

omrežnih prilagoditev. Povezovanje proizvodnih linij na SCADA sistem posega v IT področje, kar predstavlja dodaten izziv. S tem se proizvodni sistemi izpostavljajo kibernetiskim tveganjem, vključujoč nepooblaščen dostop, manipulacijo procesnih podatkov in prekinitev obratovanja. Glede na rastoče število kibernetiskih napadov na industrijske sisteme je nujno razmisliti o uvedbi ustreznih ukrepov za povečanje kibernetiske varnosti.

<b>PROBLEM</b>	Več proizvodnih linij koristi Siemens S7-1200 PLC z istim IP naslovom. Vse linije komunicirajo preko Profinet omrežja, kar onemogoča enostavno centralno povezovanje. Neposredno povezovanje vseh PLC krmilnikov na en SCADA sistem ni mogoče brez omrežnih konfliktov. Obstaja tveganje izpostavljanja proizvodnih linij kibernetiskim napadom tekom povezovanja proizvodnih linij na IT omrežje.
<b>KONTEKST</b>	Proizvodne linije izvorno delujejo kot ločene/individualne celote brez planirane skupne omrežne arhitekture. Integracija vseh linij v centralni SCADA sistem pomeni poseg na IT nivo. Industrijski sistemi (OT) so vse bolj tarča kibernetiskih groženj.
<b>MERLJIVOST</b>	Številno proizvodnih linij/krmilnikov, ki imajo enak IP naslov. Nezmožnost istočasnega povezovanja vseh linij na SCADA sistem. Število identificiranih omrežnih konfliktov (IP kolizije). Stopnja izpostavljenosti omrežja (ni segmentacije, požarnega zidu ali DMZ cone).
<b>VPLIV</b>	Otežen oziroma nemogoč centralni nadzor in upravljanje s proizvodnimi linijami. Povečano tveganje kibernetiskih napadov in nepooblaščenih dostopov.. Mogoči zastoji proizvodnje in izguba podatkov. Omejena skalabilnost sistema in otežena širitev v prihodnosti.

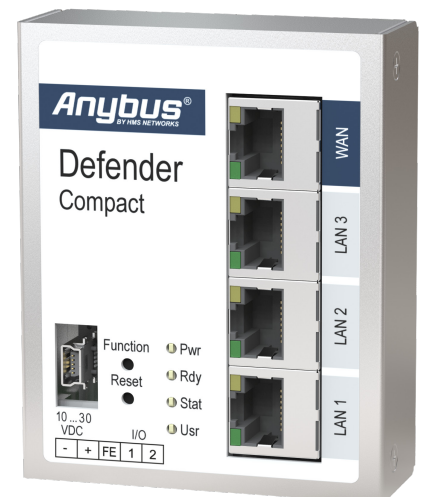
# PREDLAGANA REŠITEV

Kot rešitev za navedene probleme komunikacije in kibernetske varnosti smo predlagali implementacijo naprave Anybus Defender Compact 1004 na vsako posamezno proizvodno linijo. Ta naprava deluje kot industrijski varnostni gateway, ki omogoča mrežno segmentacijo, nadzor prometa in zaščito proizvodne linije pred nepooblaščenimi dostopi iz višjih nivojev.

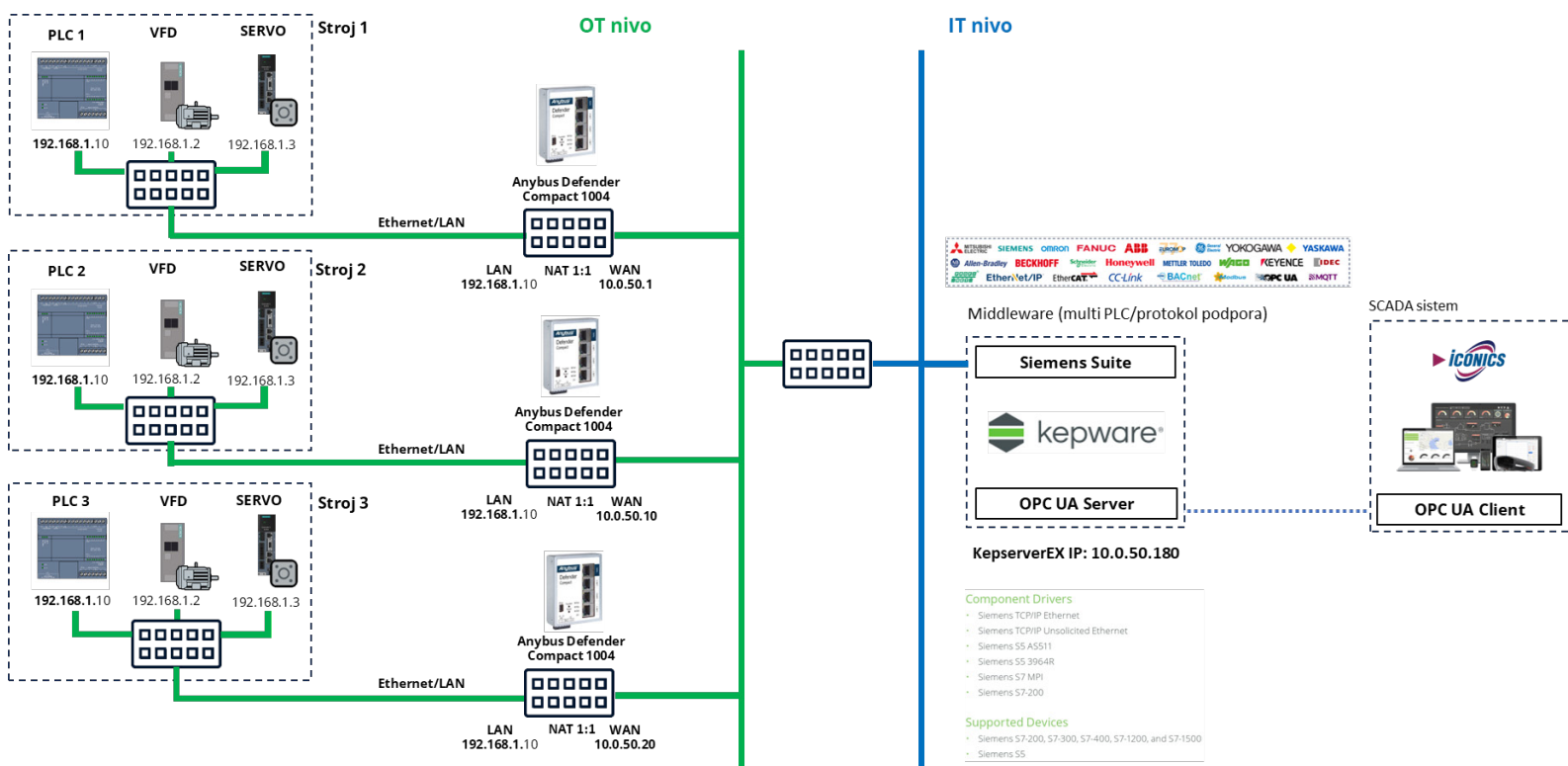
- Anybus Defender se konfigurira z uporabo 1:1 NAT (Network Address Translation) funkcije, kjer se vsaki proizvodni liniji dodeli zaseben „virtualni“ IP naslov. Na ta način nadrejeni sistem, oziroma SCADA, vidi vsako proizvodno linijo kot edinstveno omrežno entiteto s svojim IP naslovom, čeprav fizično vsi krmilniki obdržijo enake, tovarniško definirane IP naslove. S tem se popolnoma izloči problem IP konfliktov brez sprememb obstoječih omrežnih konfiguracij proizvodne linije.

- Tak pristop znatno zmanjša potrebo po dodatnem inženirskemu delu, glede na to da menjava IP naslova PLC krmilnika v praksi zahteva tudi spremembe naslovov in parametrov povezanih frekvenčnih pretvornikov, HMI zaslonov in ostalih perifernih sistemov. Z zadrževanjem obstoječe interne sheme naslovov se izognemo tveganju napačne konfiguracije, skrajšamo čas implementacije ter zmanjšamo verjetnost zastojev v proizvodnji.
- Po namestitvi Anybus Defender naprav se vsi procesni podatki agregirajo in povezujejo v Kepware OPC server, kjer se koristi Siemens Suite paket za zanesljivo in standardizirano komunikacijo s Siemens S7-1200 krmilniki. OPC server predstavlja varno in centralizirano točko za pridobivanje in distribucijo podatkov v višje nivoje sistema.

- Za komunikacijo med Kepware OPC strežnikom in Iconics Genesis SCADA paketom je implementirana varna OPC UA povezava. Slednja je bazirana na izmenjavi digitalnih certifikatov, s čimer je zagotovljena avtentikacija, enkripcija podatkov in integriteta komunikacije. S tem se dodatno dvigne nivo kibernetske varnosti celotnega sistema. Na ta način se proizvodne linije varno integrirajo v IT/SCADA okolje.



# ARHITEKTURA SISTEMA



Vgrajena oprema	Opis	Število kosov
Anybus Defender Compact 1004	Industrijski požarni zid s 4 x 10/100 Mbit vhodi, ki ščitijo pred napadi, s segmentiranjem proizvodnega omrežja v smiselno ločene celote; podpora za NAT, "routing" ter "white" in "blacklisting" IP in MAC naslovov.	7
Anybus X-gateway IIoT	Anybus X-gateway IIoT PROFIBUS DP-V0 Slave prevaja in pošilja procesne podatke iz kateregakoli PROFIBUS nadzornega sistema v OPC UA / MQTT informacijske sisteme.	1
Kepware OPC Server - Siemens Suite	Kepware Siemens Suite vključuje nadzorne programe za stare in moderne Siemens omrežne protokole. Slednje omogoča enostavno in zanesljivo povezovanje Siemens Ethernet in serijskih krmilnikov ter naprav s Client aplikacijami kot so HMI/SCADA, MES/historian, ERP, IoT in prilagojeni OPC klijenti.	1
ICONICS Genesis64 Basic 150 Tag	ICONICS GENESIS64 Basic 150 Tag je SCADA/HMI programski paket namenjen vizualizaciji in nadzoru industrijskih procesov, s podporo do 150 tagov ter OPC UA povezovanje za pridobivanje in prikaz podatkov v realnem času.	1

# ČASOVNI IN FINANČNI PRIHRANKI



Z implementacijo predlagane rešitve so ustvarjeni znatni prihranki v fazi implementacije ter tudi dolgoročne operativne koristi. Glavna finančna korist izhaja iz dejstva, da ni bilo potrebe po spremembi obstoječih IP naslovov fizično na krmilnikih oziroma proizvodnih linijah. S tem smo se izognili inženirskim posegom, ki bi vključevali rekonfiguracijo PLC programa, frekvenčnih pretvornikov, HMI panelov in povezanih sistemov, kot tudi dodatna testiranja in zagoni linij. Z uporabo Anybus Defender Compact 1004 naprav je problem naslavljanja rešen na omrežnem nivoju preko 1:1 NAT segregacije, s čemer je implementacija omejena na minimalno intervencijo znotraj same proizvodne linije. S tem se je številno potrebnih

inženirskih ur znatno zmanjšal, skrajšal skupen čas projekta ter zmanjšalo tveganje napak in neplaniranih zastojev v proizvodnji, kar ima direktno pozitiven finančni učinek.

Dodatni prihranki so ustvarjeni z uporabo Kepware OPC strežnika, ki omogoča avtomatsko kreiranje in mapiranje TAGov za Siemens PLC krmilnike. Ta funkcija znatno zmanjšuje čas potreben za konfiguracijo komunikacije in eliminira ročni vnos velikega števila TAGov, ki je sicer izpostavljen napakam in zahteva dodatno testiranje. S tem so zmanjšani stroški razvoja, povečana pa je zanesljivost podatkovnega sloja sistema.

# ZAKLJUČEK

Uporabnik se je soočil s tehničnim in varnostnim izzivom pri projektu integracije več proizvodnih linij, baziranih na Siemens S7-1200 PLC krmilnikih, v centralni SCADA sistem. Zaradi dejstva, da so vse proizvodne linije dobavljene kot posamezne celote, so vsi PLC krmilniki uporabljali iste IP naslove, kar je onemogočalo neposredno in skalabilno povezovanje na skupno omrežno infrastrukturo. Dodaten izziv je predstavljalo dejstvo, da povezovanje proizvodnih linij v IT/SCADA okolje pomeni poseg na IT raven, kar odpira nova kibernetska tveganja.

Predlagana in implementirana rešitev je temeljila na instalaciji Anybus Defender Compact 1004 naprav na vsako proizvodno linijo. Z uporabo 1:1 NAT funkcionalnosti je omogočeno dodeljevanje edinstvenih virtualnih IP naslovov vsaki liniji, kjer je obstoječa struktura naslova ostala nespremenjena. S tem je izločena potreba po večjih spremembah PLC programa, parametrov frekvenčnih pretvornikov, HMI sistemov in ostale OT opreme. S tem so zmanjšana tehnična tveganja in kompleksnost implementacije.

Vsi procesni podatki so centralizirani preko Kepware OPC strežnika in uporabe Siemens Suite paketa, kar omogoča hitro in zanesljivo vzpostavitev komunikacije ter avtomatsko kreiranje TAGov. Nadrejeni Iconics Genesis SCADA sistem je integriran s pomočjo varne OPC UA integracije, ki temelji na izmenjavi digitalnih certifikatov. S tem so zagotovljeni visoki standardi kibernetske varnosti, integritete in zaupnosti podatkov.

Iz finančnega vidika je rešitev rezultirala v znatnih prihrankih potrebnega inženirskega dela, krajšemu času implementacije in minimalnemu tveganju zastoja proizvodnje. Hiter razvoj SCADA aplikacij, avtomatizirana konfiguracija in izogibanje tveganih sprememb v obstoječih sistemih so omogočili hitro povračilo investicije (ROI), že v zgodnji fazi projekta. Dolgoročno je tak sistem skalabilen, varen in pripravljen za širitve brez dodatnih infrastrukturnih komplikacij.

Implementirana rešitev predstavlja optimalno kombinacijo tehnične učinkovitosti, kibernetske varnosti ter finančne upravičenosti, kar uporabniku nudi stabilno in zanesljivo platformo za centraliziran nadzor, upravljanje in prihodnji razvoj industrijskih sistemov.

## KONTAKT

Smo zastopnik za proizvode in rešitve za avtomatizacijo in digitalizacijo industrijskih okolij in infrastrukture. Dolgoletne izkušnje na področju industrijske avtomatizacije in robotizacije nadgrajujemo s proizvodi in rešitvami za digitalizacijo.



[info@rbt-technologies.si](mailto:info@rbt-technologies.si)