# Vrste industrijskih mreža i njihova uloga u industrijskim sustavima

**Horvat, Goran**

**Undergraduate thesis / Završni rad**

**2020**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:200:313550

*Rights / Prava:* In copyright / Zaštićeno autorskim pravom.

*Download date / Datum preuzimanja:* **2025-03-21**

*Repository / Repozitorij:*

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

**SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU**

**FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA**

**Stručni studij**

# VRSTE INDUSTRIJSKIH MREŽA I NJIHOVA ULOGA U INDUSTRIJSKIM SUSTAVIMA

**Završni rad**

**Goran Horvat**

**Osijek, 2020.**

# SADRŽAJ

1. UVOD ..... 1
1.1. Zadatak završnog rada ..... 1
2. VRSTE KOMUNIKACIJSKIH MREŽA ..... 2
2.1. CAN (Controller Area Network) ..... 2
2.2. Profibus i PROFInet ..... 5
2.3. INTERBUS ..... 8
2.4. WorldFIP ..... 11
2.5. Foundation Fieldbus (FF) ..... 13
2.6. MODBUS ..... 15
2.7. Industrijski Ethernet ..... 17
2.8. EtherCAT ..... 19
2.9. LonWorks ..... 20
2.10. KNX ..... 22
3. UZROCI SMETNJI U INDUSTRIJSKIM MREŽAMA ..... 24
4. ULOGA INDUSTRIJSKIH MREŽA U INDUSTRIJSKIM SUSTAVIMA ..... 26
5. INDUSTRIJSKI PROTOKOLI U PRIMJENI KOD FREKVENCIJSKIH PRETVARAČA ..... 31
6. ZAKLJUČAK ..... 35
LITERATURA ..... 36
SAŽETAK ..... 39
ABSTRACT ..... 39
ŽIVOTOPIS ..... 40

# 1. UVOD

Rane 1970-te godine donijele su nagli razvoj računala koja su nalazila svoju primjenu u različitim ljudskim djelatnostima, čime se javlja i potreba povezivanja različitih računalnih sustava s ciljem brže razmjene podataka i lakšeg upravljanja.

Razvoj tih ranih računalnih komunikacijskih mreža uglavnom se naslanjao na mnogobrojna vlasnička tehnološka rješenja (engl. proprietary solutions) pojedinih proizvođača opreme. Svako od tih rješenja bilo je izvedeno prema vlastitim specifikacijama te gotovo u pravilu nije bilo kompatibilno s mrežnom opremom drugih proizvođača, što znači da se komunikacijske mreže različitih dobavljača nisu mogle jednostavno povezivati. Kako su se takve mreže širile, problemi su postajali sve očitiji. Proizvođači su ubrzo uvidjeli da se moraju odmaknuti od dotadašnje prakse i okrenuti normiranim i otvorenim tehnološkim rješenjima.

Razvoj komunikacijskih mreža koje su bile kompatibilne sa mrežnom opremom drugih proizvođača uvelike je smanjilo troškove i složenost povezivanja. Sa ovom praksom započeo je Bosch već 1985. razvojem CAN mreže. Nakon toga pojavljuje se niz komunikacijskih mreža koje se koriste u industrijskim sustavima. U ovom završnom radu bit će detaljnije objašnjene neke od njih kao što su Profibus i PROFInet, INTERBUS, WorldFIP, Foundation Fieldbus, MODBUS, Industrijski Ethernet, EtherCAT, LonWorks i KNX. Također, detaljnije će biti objašnjeni uzroci smetnji u industrijskim mrežama te vrste napada. Na kraju rada bit će objašnjena uloga industrijskih mreža u industrijskim sustavima te jedan primjer primjene industrijskih protokola kod frekvencijskih pretvarača.

## 1.1. Zadatak završnog rada

Zadatak završnog rada je detaljno objasniti sve vrste industrijskih mreža te kako su se one s godinama razvijale. Još jedan od zadataka je objasniti ulogu tih računalnih mreža u industrijskim sustavima.

# 2. VRSTE KOMUNIKACIJSKIH MREŽA

U ovom se dijelu završnog rada navode često korištene, ali i neke rjeđe no tehnički zanimljive komunikacijske mreže, koje se koriste u raznim industrijskim sustavima. Za svaku od njih dan je vrlo sažet pregled koncepta rada, područja primjene te prednosti i nedostaci svake od njih.

## 2.1. CAN (Controller Area Network)

Bosch je izvorno razvio Controller Area Network (CAN) 1985. godine za mreže u vozilu. U prošlosti su proizvođači automobila povezivali elektroničke uređaje u vozilima koristeći sustave ožičenja od točke do točke. Proizvođači su počeli koristiti sve više i više elektronike u vozilima, što je rezultiralo glomaznim kabelskim snopovima koji su bili teški i skupi. Potom su namjensko ožičenje zamijenili mrežama u vozilu, što je smanjilo troškove, složenost i težinu ožičenja. CAN, visoko integrirani serijski sabirnički sustav za umrežavanje inteligentnih uređaja, pojavio se kao standardna mreža u vozilu. Automobilska industrija brzo je usvojila CAN, a 1993. godine postao je međunarodni standard poznat kao ISO 11898. Od 1994. godine na CAN-u je standardizirano nekoliko protokola više razine, poput CANopen i DeviceNet. Druga su tržišta uveliko prihvatila ove dodatne protokole, koji su sada standardi industrijske komunikacije. Prednosti CAN komunikacijske mreže su:[1]

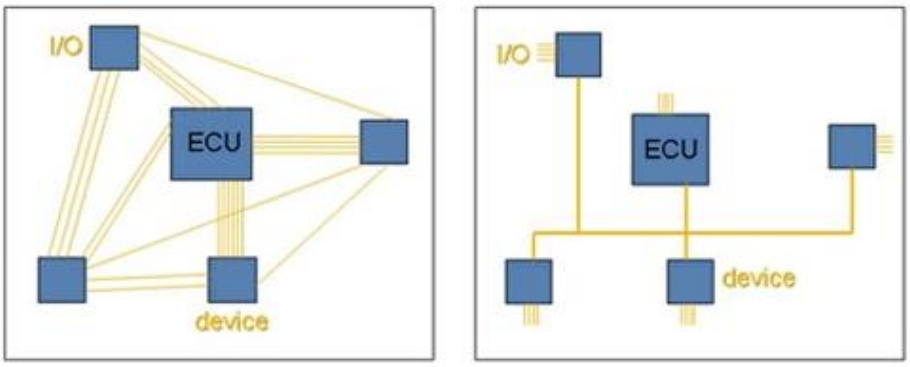
- **Niska cijena, lagana mreža -** CAN pruža jeftinu i izdržljivu mrežu koja pomaže višestrukim CAN uređajima da međusobno komuniciraju. Prednost u tome je što elektroničke upravljačke jedinice (ECU) mogu imati jedno CAN sučelje, a ne analogne i digitalne ulaze za svaki uređaj u sustavu. Time se smanjuju ukupni troškovi i težina automobila.

- **Prijenos komunikacije** - Svaki od uređaja na mreži ima CAN kontroler i zato je inteligentan. Svi uređaji na mreži vide sve prenesene poruke. Svaki uređaj može odlučiti je li poruka relevantna ili treba li je filtrirati. Ova struktura omogućuje izmjene CAN mreža s minimalnim učinkom. Dodatni čvorovi koji se ne prenose mogu se dodavati bez promjene na mreži.

- **Prioritet** - Svaka poruka ima prioritet, tako da ako dva čvora pokušaju istovremeno slati poruke, jedan s višim prioritetom se prenosi, a onaj s nižim prioritetom odgađa. Ta je arbitraža nerazorena i rezultira neprekidnim prijenosom poruke najvišeg prioriteta. To također omogućuje mrežama da udovolje određenim vremenskim ograničenjima.

- **Mogućnosti pogreške** - Specifikacija CAN uključuje Cyclic Redundancy Code (CRC) za obavljanje provjere pogreške na sadržaju svakog okvira. Okviri s greškama zanemaruju se svi čvorovi, a okvir pogreške može se proslijediti da signalizira pogrešku mreži. Globalne i lokalne pogreške kontroler razlikuje i ako se otkrije previše pogrešaka, pojedini čvorovi mogu prestati prenositi pogreške ili se potpuno isključiti iz mreže.

**Bez CAN mreže** **Sa CAN mrežom**



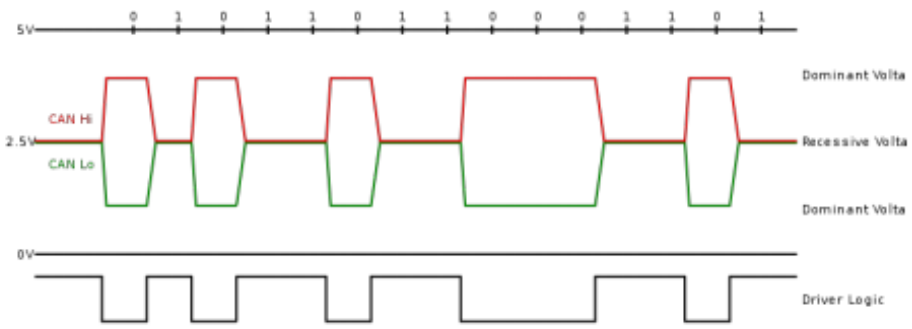

**Slika 2.1.** CAN mreže značajno smanjuju ožičenje [1]

CAN je prvo stvoren za automobilsku upotrebu, pa je njegova najčešća primjena elektroničko umrežavanje u vozilu. Međutim, kako su i druge industrije shvatile pouzdanost i prednosti CAN-a u posljednjih 20 godina, prihvatile su ga za široku primjenu. Željezničke aplikacije kao što su tramvaji, podzemna željeznica, lagane željeznice i vozovi na velike pruge sadrže CAN. CAN možete pronaći na različitim razinama više mreža unutar ovih vozila - na primjer, u povezivanju vrata ili upravljača kočnica, jedinica za brojanje putnika i još mnogo toga. CAN također ima aplikacije u zrakoplovima sa senzorima stanja leta, navigacijskim sustavima i istraživačkim računalima u pilotskoj kabini. Pored toga, CAN komunikacijske mreže možete pronaći u mnogim zrakoplovnim primjenama, u rasponu od analize podataka tijekom leta do sustava upravljanja zrakoplovom kao što su sustavi goriva, pumpe i linearni aktuatori.[1]

Proizvođači medicinske opreme upotrebljavaju CAN kao ugrađenu mrežu u medicinskim uređajima. Zapravo, neke bolnice koriste CAN za upravljanje kompletnim operacijskim salama. Bolnice kontroliraju komponente operacijske dvorane kao što su svjetla, stolovi, kamere, rendgenski strojevi i bolesnički kreveti sa sustavima temeljenim na CAN-u. Dizala i pokretne stepenice koriste ugrađene CAN mreže, a bolnice koriste CANopen protokol kako bi međusobno povezale uređaje za dizanje, poput ploča, kontrolera, vrata i svjetlosnih barijera. CANopen se također koristi u neindustrijskim aplikacijama kao što su laboratorijska oprema, sportske kamere, teleskopi, automatska vrata, pa čak i aparati za kavu.

Nedostaci CAN-a su brzina prijenosa podataka, prijenos podataka na relativno kratke udaljenosti te nedeterminističnost prijenosa podataka. Zbog toga se kroz godine javljaju novi protokoli temeljeni na CAN-u, poput CANopen [CIA02], DeviceNet [BiVan96], FTT-CAN (Flexible-time-triggered CAN) i TTCAN (Time-triggered CAN) [ISOCAN01]. [1]

U 2012. godini nastaje specifikacija CAN FD 1.0 (CAN with Flexible Data-Rate) s nešto drukčijim formatom okvira te uvodi mogućnost preklapanja tj. prespajanja (switching). Važno je primijetiti kako je sabirnica CAN FD kompatibilna s CAN 2.0. Sabirnica CAN podržava više glavnih (master) jedinica tj. čvorova, pri čemu je nužno imati najmanje dva čvora kako bi komunikacija radila. Svi se čvorovi povezuju preko parice impedancije 120 oma, a istu je potrebno na krajevima i terminirati. U početku su predviđene dvije vrste CAN sabirnice: brza CAN sabirnica (ISO 11898-2) koja dostiže brzine do 1Mib/s (5Mib/s za CAN-FD), te spora CAN sabirnica (poznatija kao fault-tolerant CAN sabirnica, ISO 11898-3). Zahtjevi CAN sabirnicu su da svaki čvor mora imati: • upravljački procesor (CPU, mikroprocesor) koji upravlja logikom svog rada te ostalim povezanim uređajima (senzori, aktuatori itd.), • CAN kontroler koji čini integralni dio upravljačkog dijela (služi primopredaji podataka/poruka na razini niza bitova) • primopredajnik (engl. transceiver) koji ostvaruje pristup mediju na razini naponskih signala, te konvertira bitove na očekivane naponske razine signala na sabirnici. [2]




**Slika 2.2.** Prikazuje primjer napona koji se javljaju na CAN sabirnici [2]

Danas se na tržištu nalaze mnogobrojni integrirani sklopovi i moduli koji služe radu s sabirnicom CAN (primjerice primopredajnici ISO1042-Q1, ADM3056E, MCP2542FD).

## 2.2. Profibus i PROFInet

Profibus i Profinet su kreirali i dizajnirali iste organizacije. Profibus je kratica za Process Field Bus, a Profinet je za Process Field Net. Budući da je obje stvorila ista organizacija, u dizajnu i inženjerskim konceptima slični su za definiranje hardvera svakog uređaja. Tako korisnik ima koristi od prelaska s Profibusa na Profinet zbog sličnosti u projektiranju, dizajnu i primjeni. Profibus je serijski protokol, dok je Profinet protokol temeljen na Ethernetu. Profinet je napredna verzija Profibusa, jer djeluje na protokolu koji se temelji na Ethernetu i pruža veću brzinu, veću propusnost i veću veličinu poruke od Profibusa. Profibusu nedostaje provjera autentičnosti i omogućuje lažnim čvorovima da lažno predstavljaju matične čvorove.

Profibus je terenski komunikacijski standard za tehnologiju automatizacije. Promovirao ga je 1989. godine njemački odjel za obrazovanje i istraživanje, a prvi put ga je koristio Siemens. To je protokol serijske komunikacije pomoću kabela RS-485 ili optičkog vlakna. Postoje dvije inačice Profibusa: Profibus DP i Profibus PA.

Profibus DP se široko koristi u usporedbi s Profibus PA. To je zato što Profibus PA ovisi o aplikaciji, dok se Profibus DP koristi u opće svrhe. Profibus PA označava automatizaciju procesa i široko se koristi za nadzor mjerne opreme. Profibus DP znači decentralizirana periferija, a koristi se i za nadzor mjerne opreme. Sam Profibus DP ima tri varijante: Profibus DP-V0, DP-V1 i DP-V2.

Profibus je protokol u kojem glavni uređaji upravljaju robovima za prijenos podataka između dva ili više robova. Također podržava više glavnih čvorova, a to se upravlja korištenjem dijeljenja tokena. Jednom kada gospodar nadgleda žeton, može komunicirati sa svojim robovima. Robovi također mogu započeti komunikaciju s glavnim ili drugim robovima pod određenim uvjetima. Obično je glavni voditelj PLC (Programabilni logički kontroler) ili RTU (Uređaj za daljinski terminal), a podređeni je motor i senzor.

Profibusu nedostaje provjera autentičnosti, omogućujući tako bilo kojem spoofed čvoru da lažno predstavlja glavni čvor koji pruža kontrolu nad svim robovima u mreži. Profibus je također osjetljiv na DoS napad; stoga ga treba izolirati od preostalih komponenata unutar mreže.

Profinet je Ethernet implementacija Profibus protokola. Profinet radi na Ethernetu kao fizičkom sučelju i široko se koristi u industrijskim aplikacijama za automatizaciju za obavljanje zadataka poput razmjene podataka, alarma i dijagnostike s PLC-ima i kontrolorima automatizacije. Kao i Profibus, Profinet također koristi dijeljenje tokena za prijenos podataka i komunikaciju. Profinet koristi tri komunikacijska kanala za razmjenu podataka s PLC-ovim i drugim uređajima:

- TCP / IP kanal: Ovaj kanal koristi se za acikličke operacije čitanja / pisanja, konfiguraciju i parametriranje.
- Kanal u stvarnom vremenu: ovaj se kanal koristi za standardni ciklički prijenos podataka i alarma.
- Izohronski kanal u stvarnom vremenu: Ovaj se kanal koristi za aplikacije za kontrolu kretanja i provodi se pomoću ASIC (integriranih krugova specifičnih za aplikaciju.

Budući da je Profinet napredna implementacija Profibusa, pruža brojne prednosti u odnosu na Profibus. Neke od važnih prednosti Profineta su:

- Rad velike brzine
- Podrška vremenski kritičnim i kontrolama pokreta
- Kratko vrijeme pokretanja
- Jednostavan za instalaciju i integraciju
- Manje vremena za komunikaciju i inženjersku podršku

Profinet klasificira uređaje u tri vrste. Oni su kako slijedi:

- IO kontroleri: Ovi uređaji izvršavaju programe automatizacije. IO kontroleri razmjenjuju podatke s IO uređajima. Kontrolor je odgovoran za mapiranje IO podataka s IO uređaja u

procesnu sliku i te vrijednosti podataka koriste upravljački programi. Tipični IO kontroleri podržavaju sljedeće vrste usluga:

1. Ciklička razmjena podataka: razmjena podataka između IO uređaja i IO kontrolera
2. Aciklička razmjena podataka: razmjena konfiguracijskih i dijagnostičkih podataka
3. Alarmi: razmjena podataka alarma s IO uređaja na IO kontroler
4. Kontekstno upravljanje: obrada veze

- IO uređaji: Ovi su uređaji povezani s IO kontrolerom preko Etherneta. Ti su uređaji obično senzori / aktuatori
- IO nadzornici: Ovi uređaji su HMI računala, uređaji za dijagnostičku analizu ili nadzor. Slični su Profibusovim masterima i koriste se u puštanju u rad i prikupljanju dijagnostičkih podataka

Profinetu nedostaje provjera autentičnosti, omogućujući tako bilo kojem spoofed čvoru lažno predstavlja glavni čvor koji osigurava kontrolu nad svim robovima u mreži. Za provjeru autentičnosti komponenata u mreži potrebno je koristiti različite metode autentifikacije.

Profibus i Profinet čine izvrstan industrijski protokol za automatizaciju i komunikaciju na više uređaja. Prema korištenju i implementaciji, oni se mogu koristiti. Uz potrebne sigurnosne probleme, Profibus / Profinet može biti sveobuhvatan protokol koji zadovoljava većinu potreba u automatizaciji procesa.

**Slika 2.3**. Primjer tipičnih konektora za povezivanje Profibus uređaja [3]

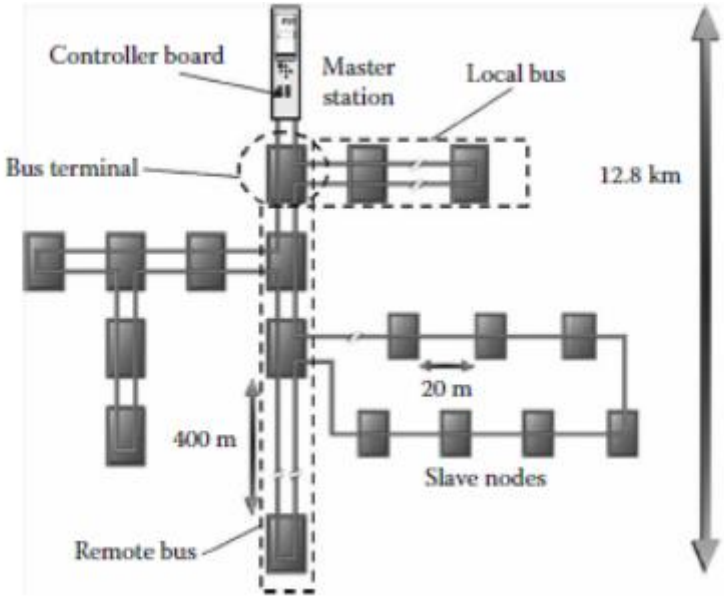
## 2.3. INTERBUS

Sabirnica INTERBUS nastaje u tvrtki Phoenix Contact 1987. godine. Kao i ostale sabirnice, zamišljena je kao brza sabirnica za prijenos podataka između senzora i aktuatora te općenito razmjenu podataka u industrijskim pogonskim okruženjima. Normirana je zajedno s ostalim normama u IEC 61158. U odnosu na ostale sabirnice, ova je specifična po svojoj topologiji i protokolu koji omogućava vrlo brz, ciklički i vremenski determiniran prijenos podataka, a omogućava samostalnu dijagnostiku i time jamči dobru robusnost.

INTERBUS ima prstenastu topologiju, dakle svi su uređaji međusobno povezani u zatvoreni krug, no podatkovne linije povezuju sve uređaje istim kabelom, pa topologija nalikuje otvorenom stablu. Ovo je bitna razlika u odnosu na ostale slične topologije, a ujedno ga čini vrlo prilagodljivim i lako proširivim. U ovu je sabirnicu moguće spojiti do 512 uređaja na 16 mrežnih razina.

Druga važna osobina svojstvena je načinu na koji se čvorovi adresiraju te na koji se način podaci prenose kroz prsten. Za razliku od drugih sustava u kojima se podaci prenose zadavanjem adrese svakog pojedinog uređaja na sabirnici i potom putuju u posebnim podatkovnim okvirima, u sustavu INTERBUS podaci se automatski šalju uređajima temeljem njihove fizičke lokacije u

sustavu. Sve informacije za sve uređaje prenose se kroz jedan zajednički okvir nazvan "okvir zbrajanja" (engl. summation frame). Ovu značajku omogućuje fizička izvedba sustava koja se može vidjeti kao dugački, raspodijeljeni registar pomaka (shift registar, SR) sa mogućnošću serijskog/paralelnog ulaza/izlaza sastavljenog od nekoliko malih registara, pri čemu svaki pripada jednom čvoru.




**Slika 2.4.** Fleksibilnost INTERBUS topologije i način ožičenja uređaja [4]

Kako bi INTERBUS radio, potrebno je upotrijebiti razne elemente sabirnice, a kao što je prikazano na slici 2.4.

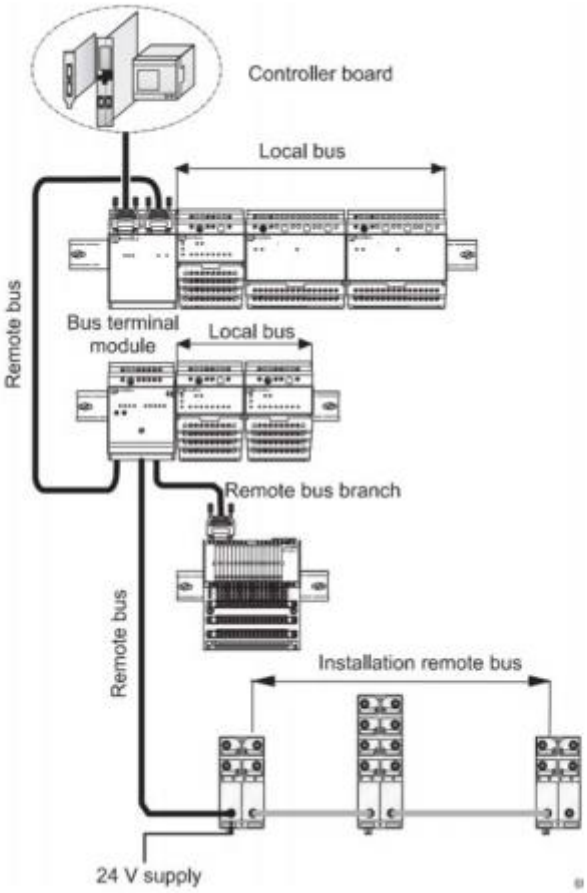
Nadzornik ili glavni upravljač sabirnice (engl. bus master) upravlja svim sabirničkim aktivnostima. On prenosi izlazne podatke na odgovarajuće čvorove, zaprima ulazne podatke i nadzire prijenos podataka. Pored toga, prikazuje dijagnostičke poruke, a poruke o pogreškama prenose se u nadređeni sustav. Kontroler ili upravljač je odgovoran za pripremu jedinstvenog „zbrojnog“ okvira koji omogućuje raspodjelu podataka među čvorovima.

Udaljena sabirnica (engl. remote bus): Upravljačka elektronika (engl. controller board) nadzornika povezana je s uređajima sabirnice preko udaljene sabirnice. Ogranak ili rukavac ove veze naziva se udaljeni ogranak sabirnice. Prijenosni (fizički) medij mogu biti bakreni vodovi (standard EIA-485), optička vlakna, infracrvene podatkovne veze te ostali prijenosni mediji (npr. radijske veze). Kao uređaji na udaljenoj sabirnici mogu se koristiti posebni ulazno/izlazni moduli

te uređaji poput robota, motori ili aktuatori. Svaki od njih ima lokalno napajanje i galvanski odvojen podatkovni priključak. Pored vodova za prijenos podataka, u instaliranom se kabelu sabirnice također mogu nalaziti i vodiči za napajanje modula i senzora. Priključni modul sabirnice (engl. bus terminal module): Priključni modul sabirnice povezuje ulazno/izlazne module preko INTERBUS mreže na udaljeni sabirnik.

Priključni modul sabirnice dijeli sustav na pojedine segmente, omogućavajući uključivanje / isključivanje pojedinih grana uživo, tijekom rada. Priključni modul sabirnice također pojačava podatkovni signal (engl. repeater, ponavljač) i galvanski izolira pojedine segmente sabirnice.

Lokalna sabirnica (engl. local bus): lokalna sabirnica odvaja se od udaljene sabirnice preko spojnice sabirnica (engl. bus coupler) i povezuje sve uređaje na lokalnoj sabirnici. Na ovoj razini nisu dopuštena grananja. Napaja se preko priključnog modula. Uređaji lokalne sabirnice u pravilu su U/I moduli.

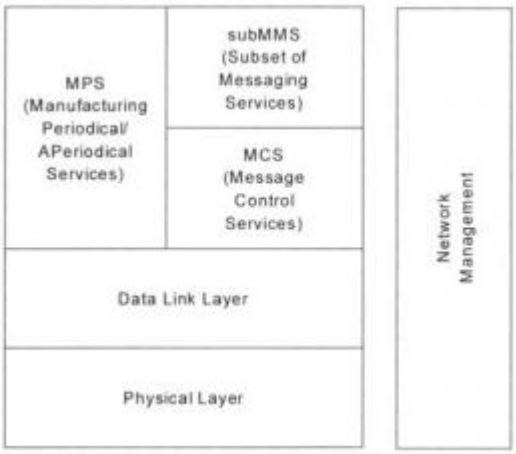



**Slika 2.5**. Primjer povezivanja različitih INTERBUS uređaja [5]

Brzine na sabirnici kreću se od 500 kib/s do 2 Mib/s. Od dijagnostičkih funkcija, sabirnica može samostalno detektirati prekide i kratke spojeve u vodovima, smetnje ili kvarove pojedinog uređaja te sporadične smetnje u komunikaciji (često uslijed EM smetnji).

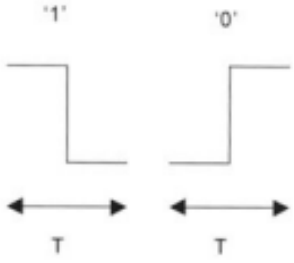
## 2.4. WorldFIP

WorldFIP protokol je otvoreni sustav, međunarodni standard sabirnice polja (EN50170) i koristi se za spajanje nulte razine (senzori i aktuatori) i razine jedan (PLC-ovi, kontroleri). Može se koristiti u raznim arhitekturama, poput centraliziranih, decentraliziranih i master-slave. Algoritam upravljanja može se nalaziti unutar jednog procesora ili se može distribuirati. Slika 2.6. prikazuje slojeve WorldFIP standarda.




**Slika 2.6.** Slojevi WorldFIP standarda [6]

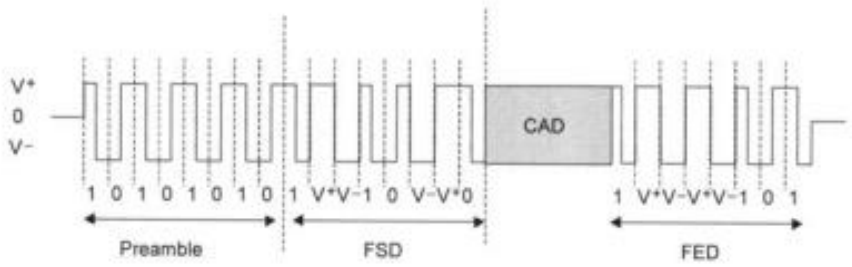
Fizički sloj osigurava prijenos bita s jednog uređaja na drugi. U glavnoj specifikaciji brzina prijenosa je 1 Mbps preko oklopljenog uvijenog para (STP) ili kabela optičkih vlakana. Tri definirane brzine su 1 USD (31,2 kbps), 2 USD (1 Mbps) i 3 USD (2,5 Mbps) i dodatna brzina od 5 Mbps (optička vlakna).Kao Ethernet, WorldFIP koristi Manchester kodiranje. To kodira '1' kao prijelaz između visokog i niskog i '0' kao niski do visoki prijelaz, kao što je prikazano na slici 2.7. Stalna visoka ili niska razina je kršenje kodiranja. Visoka razina je y +, a niska razina y. Manchester kodiranje ima prednost ugradnje podnožja u preneseni signal.




**Slika 2.7**. WorldFIP bit kodiranje [7]

Slijed pokretanja okvira (FSS) prikazan je na slici 2.8., a sadrži sljedeća polja:

- Preambula (PRE) - unaprijed definirani uzorak od 10101010. Koristi se za sinkronizaciju satova prijema.
- Razgraničivač okvira (FSD) - unaprijed definirani uzorak lVVlOv-v'O, koji definira početak polja CAD.
- Kontrola i podaci (CAD) - sadrže podatke o sloju veze podataka.
- Razdjelnik krajnjeg okvira (FED) - unaprijed definirani uzorak lVv-v'VlOl, koji definira kraj polja CAD.




**Slika 2.8**. WorldFIP okvir [8]

Sloj podatkovne veze podržava dvije vrste usluga:

- Razmjene varijabli
- Prijenosi poruka

To mogu biti ciklični ili izričiti korisnički zahtjev. Ciklička poruka je kada sustav konfigurira nazive objekata. Te se razmjene automatski šalju bez da korisnik to traži od njih. Izričiti korisnički zahtjev uključuje zahtijevanje varijabli i srodnih odgovora.

## 2.5. Foundation Fieldbus (FF)

Ova sabirnica i protokol nastaju kao nastavak razvoja WorldFIP-a, a uvelike se koristi u automatizaciji procesa. Jedno od njegovih ključnih obilježja jest potpuna raspodijeljenost upravljačkih funkcija koje se mogu izvoditi na ugrađenim računalima koja se mogu nalaziti na senzorima i aktuatorima. Svaki uređaj posjeduje vlastitu „inteligenciju“ i komunicira preko dvosmjernog serijskog sučelja.

Specifikacija za FF određuje dvije razine mreže:

- H1 - upravljačka mreža koja radi na brzini 31,25 kib/s
- HSE - brza podatkovna sabirnica na 100/1.000 Mib/s.

Razina H1 koristi prijenosnu tehnologiju MBS (Manchester bus powered, IEC 61158-2 tip 1), koristi se u pogonu, a moguće ju je koristiti i u opasnim uvjetima. Na višim razinama koristi se Ethernet pa je tako moguće povezivanje s klasičnim računalnim mrežama. HSE je normiran i u normi IEC 61158-2 označen je kao tip 5. Za HSE razinu određena su četiri razreda ili klase uređaja:

1. HD (host device) - osobna (PC) računala ili kontroleri koji imaju Ethernet priključak
2. LD (link device) - povezuje Ethernet mrežu s više segmenata H1
3. U/I pristupnici (foreign I/O gateway) - služe integraciji s drugim vrstama sabirnica
4. ED (Ethernet device) - omogućava izravno povezivanje s Ethernet mrežom.

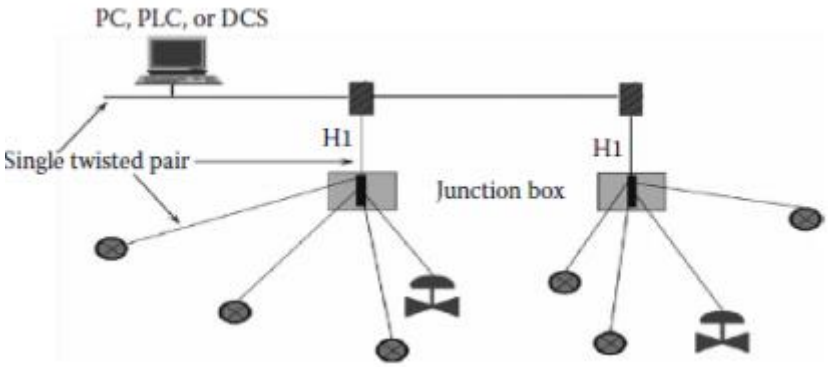
Najveća duljina jednog segmenta sabirnice je 1.900 metara bez ponavljača, a sabirnicu je moguće produljiti s najviše četiri ponavljača, pa ukupna duljina sabirnice može iznositi 9.500 metara. Podržani koncepti razmjene podataka su [FFSEG12]:

- poslužitelj/klijent - za potrebe razmjene podataka koristi se Client/Server Virtual Communications Relationship (VCR). Na sabirnici se koristi lista čekanja tj. red (engl.

queue) pa se poruke šalju i primaju redoslijedom kojim su zaprimljene ili poslane, a u skladu s njihovim prioritetima.

- izdavač/pretplatnik - koristi se za komunikaciju jedan-na-više. Koriste se među spremnici (engl. buffer) što znači da se na mreži zadržava samo zadnja verzija podataka, a novi podaci brišu prethodne.
- distribucija izvještaja (report distribution) - koristi se u slučajevima nasumične komunikacije (nije prethodno planirana, tj. nije ciklička), a pokreću je korisnici.

Svaki segment mreže za svoj rad zahtjeva dva terminatora. Terminatori odgovaraju serijskom spoju kondenzatora od 1 µF i otpornika od 100 oma. Svi su uređaji paralelno spojeni na sabirnicu, stoga u svakom trenutku samo jedan uređaj može slati podatke. Komunikacija na sabirnici odvija se na način da se svaki uređaj ponaša kao potrošač struje (current sink). Manja potrošnja struje označava logičko stanje visoko (logička jedinica), a veća potrošnja struje označava logičku nulu (potrošnja struje kreće se između 15 mA i 20 mA).




**Slika 2.9.** Primjer jednostavne topologije sabirnice FF [9]

Obzirom da sabirnica FF omogućuje raspodijeljeno upravljanje i „inteligentne“ komponente (senzore i aktuatore), kako bi to zaista i radilo nužno je da svi elementi jedne upravljačke petlje (control loop) budu smješteni na isti sabirnički segment.

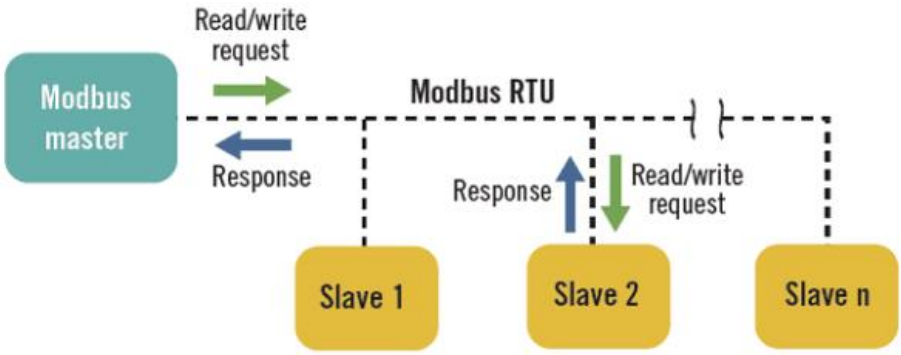
Obzirom na posebnost načina komunikacije, sabirnička razina H1 mora imati posebne jedinice za napajanje FBPS (Fieldbus Power Supply/Power Conditioner) kako bi napon sabirnice bio unutar očekivanih granica. Ovisno o veličini mreže, izlazni napon jedinice FBPS kreće se između 12 i 28 V, a najveća izlazna struja kreće se između 80 i 500 mA.

## 2.6. MODBUS

Modbus je komunikacijski protokol za prijenos informacija između elektroničkih uređaja serijskim linijama (izvorna verzija) ili putem Etherneta, a uobičajeno se koristi u automatizaciji procesa i tvornica. Iako je riječ o otvorenom protokolu i bilo tko ga može koristiti, "Modbus" je registrirani zaštitni znak tvrtke Schneider Electric USA, Inc. (trenutni vlasnik robne marke Modicon). Organizacija Modbus.org stvorena je za daljnju upotrebu Modbusa i Schneider Electric je bio partner u njemu.

Modbus.org ima opsežnu pokrivenost za Modbus, specifikacije za različite vrste Modbusa, softver, testiranje, kôd sučelja i još mnogo toga.

Modbus serijski protokol (izvorna verzija) je glavni / podređeni protokol, npr. jedan master koji upravlja transakcijama podataka Modbus s više robova koji odgovaraju na zahtjeve master-a za čitanje ili pisanje podataka u robove. Modbus TCP, također poznat kao Modbus TCP / IP, koristi arhitekturu klijent / poslužitelj. Te mrežne arhitekture prikazane su na slikama 2.10. i 2.11.



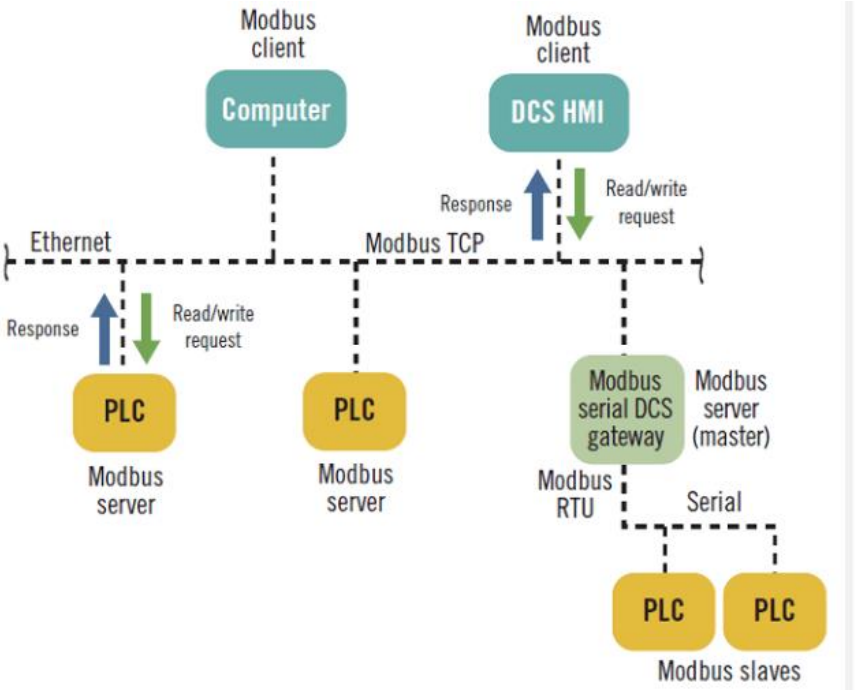

**Slika 2.10.** Modbus serijska arhitektura [10]

U standardnoj Modbus serijskoj mreži nalazi se jedan glavni i čak 247 robova, svaki s jedinstvenom adresom roba. Modbus TCP obično se implementira na Ethernet mreži, a podatkovne transakcije s Modbusovog klijenta usmjeravaju se prema Modbus poslužitelju putem IP adrese.

Modbus dolazi u nekoliko varijanti, uključujući serijski RTU, serijski ASCII, TCP / IP i UDP / IP. Modbus dijalekti, poput Enrona, Daniela i Pemex Modbusa, nastali su zbog toga što su

ljudi mijenjali standardni Modbus za obradu podataka s pomičnim zarezom, podataka s dugim cijelim brojem i drugih zahtjeva za podacima. Čitanje Modbus sučelja i dokumentacije roba ključno je za razumijevanje i implementaciju ovih vrsta Modbus mreža i za miješanje različitih proizvođača uređaja u istoj Modbus mreži, što treba pažljivo učiniti.

Modbus protokol je preteča modernih terenskih sabirnica. Popularnost Modbusa zaslužna je jednostavnošću, otvorenošću i sveprisutnom prirodom - koristi se svuda. Izdržala je test vremena i još uvijek je prisutna nakon gotovo četiri desetljeća. Modbus je izvorno objavio Modicon 1979. godine, prije svega za upotrebu s vlastitim PLC-ovima. Kad se pojavio industrijski Ethernet, razvijen je Modbus TCP, zadržavši veći dio Modbusove jednostavnosti u TCP / IP omotu.




**Slika 2.11.** Modbus TCP arhitektura [11]

Adresa modbus memorije je obično organizirana oko 16-bitnih registara koji sadrže 16 zavojnica ili stanja uključivanja / isključenja (0/1) ili cjelobrojne vrijednosti u 16-bitnim registrima (unosi / izlazi ili registar zadržavanja).

Modbusova poruka temelji se na onome što nazivamo aplikacijskom jedinicom podataka (ADU) i jedinicom podataka protokola (PDU). Modbus poruka uključuje podređenu / poslužiteljsku adresu za uključeni rob / poslužitelj, funkcijski kod, početne adrese podataka i

podatke koji se šalju (pisano) ili se vraćaju (čitaju) glavnom klijentu, s greškom kontrolnog zbroja na kraju (CRC / LRC / Checksum).

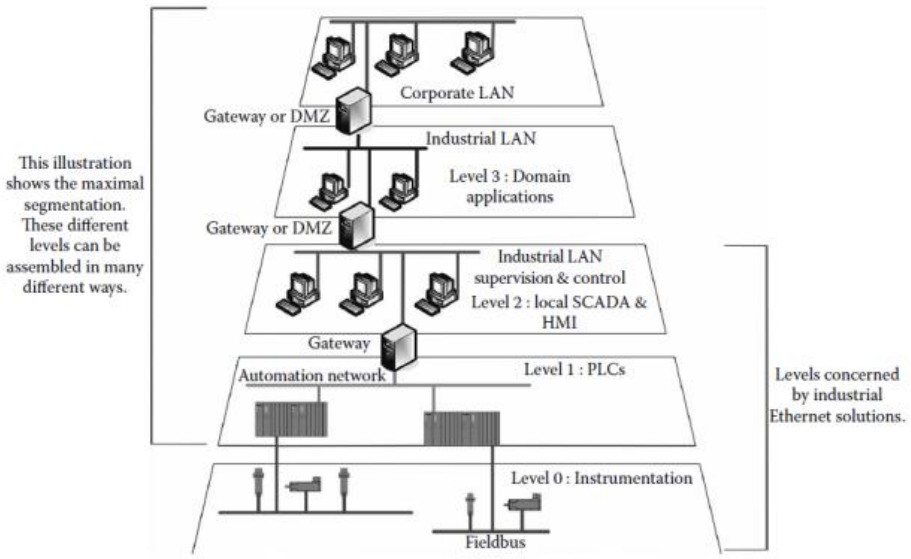
Veličina serijskog Modbus PDU ograničena je ograničenjem veličine naslijeđene od prve implementacije Modbusove serijske mreže od 256 bajtova. Adresa robova Modbusa ograničena je na 1-255. Korisnicima su dostupne adrese 1-247, a adrese 248-255 su rezervirane.

## 2.7. Industrijski Ethernet

Krajem 1970-ih ubrzano se povećava stupanj automatizacije u sustavima mjerenja i upravljanja, a prati ga pojava vlasničkih sabirničkih rješenja koja su osmišljena prema trenutnim zahtjevima pojedinih skupina tržišta (ili vrsta proizvodnih procesa).

Kako bi se osigurala interoperabilnost između različitih proizvoda različitih proizvođača, stvorena je norma IEC 61158. No, uslijed velikog pritiska proizvođača, umjesto unificirane norme nastaje samo zbirka nekoliko različitih specifikacija koje odgovaraju ponudi svakog dobavljača.

U međuvremenu se javlja Ethernet (IEEE 802.3) koji postaje standardno rješenje u računalnim komunikacijskim sustavima koji implementiraju prva dva sloja OSI modela. Protokolni složaj TCP / IP (RFC 791 i 793) istu je stvar učinio za OSI slojeve 3 i 4.




**Slika 2.12.** Primjer arhitekture komunikacijskog sustava u tvornici [12]

Sve do kasnih 1990-ih Ethernet se nije mogao koristiti u industrijskim uvjetima na najnižoj razini upravljanja proizvodnim procesom isključivo zbog svoje nedeterminističke metode kontrole pristupa mediju, nazvane CSMA/CD. Iako je pojava full-duplex veza i tehnologije preklapanja od Etherneta stvorio potencijalnog kandidata za komunikaciju na razini proizvodnje, još uvijek se nije moglo zajamčiti unaprijed poznato i kratko vrijeme odziva. Razlog tome je što se Ethernet podatkovni okviri u preklopniku mogu iz niza razloga privremeno zaustaviti, pa čak izgubiti (tj. odbaciti). Takvo upravljanje podacima ne udovoljava zahtjevima sustava upravljanja i nadzora u stvarnom vremenu.

Kako bi se riješio taj problem, dobavljači su razvili nekoliko različitih rješenja koja odgovaraju uvjetima koje postavljaju proizvodni procesi. Slika 2.12. prikazuje moguću podjelu komunikacijskih mreža u informacijskom sustavu neke tvornice. Moguće je vidjeti različite vrste komunikacijskih mreža, od tzv. poslovnog LAN-a, industrijskog LAN-a, pa do posebnih podatkovnih sabirnica. Gornje dvije razine, na kojima je izveden klasični Ethernet, ne omogućavaju prijenos vremenski kritičnih podataka. Industrijska Ethernet rješenja osmišljena su posebno za potrebe povezivanja na nižim razinama, raznim podatkovnim sabirnicama koje služe automatizaciji procesa.

U domeni IKT tehnologija, Ethernet, TCP (ili UDP) te IP danas su de facto standardi. Većina protokola viših slojeva, neovisno o tome jesu li otvoreni ili vlasnički, naslanjaju se na te protokole za kontrolu pristupa, mrežne i transportne usluge. Iz tog razloga komunikacijski protokoli viših slojeva mogu bez problema koegzistirati na istoj komunikacijskog mreži.

Nadalje, mnogi uobičajeni protokoli koji rade preko TCP/IP-a, primjerice, SFTP za prijenos datoteka ili HTTPS za prijenos mrežnih stranica, koriste se za pružanje potrebnih mrežnih usluga raznim računalnim programima. Nažalost, to nije slučaj u rješenjima za industrijsko umrežavanje. Ethernet je definiran normom IEEE 802.3. On pruža većinu funkcija i usluga koji odgovaraju slojevima 1 i 2 OSI modela i dobro je poznat po svojoj metodi za kontrolu pristupa prijenosnom mediju: CSMA/CD. Međutim, kada se Ethernet povezuje s prefiksom "industrijski", tada se pojam „Industrijski Ethernet“ može imati tri različita značenja. Takav se naziv može koristiti:

- samo za uobičajene Ethernet proizvode (mrežne kartice tj. NIC, preklopnike i kablove) ili
- za LAN mrežu koja koristi uobičajene Ethernet preklopnike, ali samo određene mrežne kartice ili
- koristiti samo Ethernet kablove pri čemu je sve ostalo specifično za određenu namjenu.

Posljedica toga je da postoje različite vrste pojma „industrijskog Etherneta“, a koje nisu međusobno kompatibilne. Stoga treba imati na umu da neke izvedbe „industrijskog Etherneta“ ponekad mogu raditi na istoj mreži, ali kompatibilnosti je ovisna o konkretnim proizvodima tj. tehnologijama. Pojam "industrijski" nerijetko se i odnosi na mogućnost rada u teškim industrijskim uvjetima. Razmotrimo neka svojstva koja industrijska komunikacijska mreža temeljena na Ethernetu mora zadovoljiti:

- Konektori i sklopovlje moraju moći raditi u industrijskim uvjetima

Komunikacijska oprema (elektroničke komponente, oklapanje, zaštita sklopovlja i konektori) mora biti u mogućnosti ispravno raditi u industrijskim uvjetima. To podrazumijeva, primjerice, potvrđivanje IP6x, korištenje raznih konektora otpornih na habanje i prašinu, potvrđivanje EMI i IECEx

- Jamstvo usluge

Obzirom da Ethernet koristi mehanizam za upravljanje pristupom mediju CSMA/CD, nemoguće je jamčiti ni dolazak podatkovnog okvira niti vrijeme njegovog prijenosa. Da bi ih se koristilo na razini proizvodnih procesa, industrijska Ethernet rješenja moraju udovoljiti nizu ovdje opisanih zahtjeva.

Jedan od takvih zahtjeva je i zajamčeno trajanje vremena prijenosa. Upravljački sustavi su redovito sustavi koji rade u stvarnom vremenu, pa se informacije moraju prenositi bez gubitaka i uz malo kašnjenje. Međutim, Ethernet ne može jamčiti malo kašnjenje paketa. Za multimedijske primjene ovaj je problem riješen zahvaljujući prioritizaciji protoka i korištenja virtualnih LAN-ova (VLAN), prema normama IEEE 802.1Q i IEEE 802.1D. Ovo rješenje omogućuje smanjenje jittera i jamči vrijeme prijenosa na oko 10 ms (za promet visokog prioriteta). Međutim, to su srednje vrijednosti vremena prijenosa.

## 2.8. EtherCAT

Ethernet za tehnologiju automatizacije upravljanja (EtherCAT) razvio je Beckhoff. Temelji se na CANopen protokolu i na Ethernetu, ali se razlikuje od internetske i mrežne komunikacije po tome što su posebno optimizirane za industrijsku kontrolu automatizacije. Standardi su definirani i održavani u EtherCAT tehnološkoj grupi.

Koristeći mrežni model OSI, Ethernet i EtherCAT oslanjaju se na iste fizičke i podatkovne slojeve veze. Dalje od toga, dvije se mreže razlikuju po dizajnu jer su optimizirane za različite zadatke. Tako je, na primjer, Ethernet dizajniran za slanje velikih količina podataka kroz mnogo različitih čvorova. Podatke može usmjeriti prema milijardama zasebnih adresa i sa njih, omogućavajući komunikaciju na ogromnim mrežama.

EtherCAT je brza i determinirana mreža i obrađuje podatke koristeći namjenski hardver i softver. Koristi puni dupleks, glavno-slave konfiguraciju i prilagođava bilo kojoj topologiji. U 30 mikrosekundi može obrađivati 1.000 I / O točaka i komunicirati sa 100 servo osi u 100 mikrosekundi. Osi primaju zadane vrijednosti i upravljačke podatke i izvještavaju o stvarnom položaju i stanju. Osovine se sinkroniziraju pomoću tehnike raspodijeljenog sata koja je jednostavna verzija IEEE 1588 i smanjuje podrhtavanje na manje od 1 mikrosekunde.

EtherCAT protokol omogućuje brzi protok jer se poruke obrađuju u hardveru prije nego što se proslijede na sljedeći slave. Robovi čitaju relevantne podatke dok im prolazi okvir podataka i u pokretu ubacuju nove podatke u isti tok podataka. To ne ovisi o vremenu izvođenja skupa protokola, pa odgoda obrade obično iznosi samo nekoliko nanosekundi.

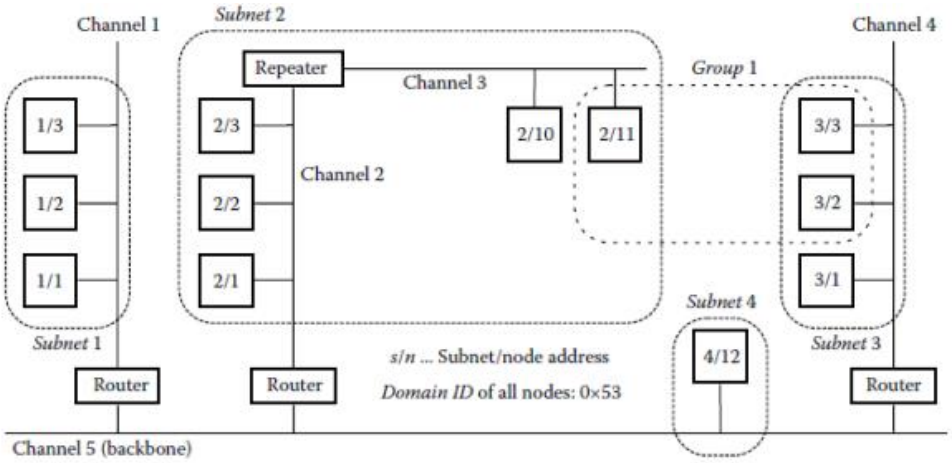
## 2.9. LonWorks

LonWorks stvorio je Echelon Corp 1988. LonWorks je vodeće mrežno rješenje za automatizaciju zgrada. Procjene za broj instaliranih čvorova širom svijeta kreću se u milijunima. Udruga za interoperabilnost LonMark s preko 300 tvrtki članica odražava snagu koju LON sada ima na tržištu automatizacije.

Kad se koristi u industrijskom okruženju, rješenje tvrtke LonWorks vrlo se razlikuje od mreža otvorenih uređaja poput DeviceNet, Profibus i Modbus koji se obično nalaze na tvorničkim podovima. Prvo za razliku od ovih popularnih sabirnica uređaja LonWorks je potpuno jednaka mreža. Umjesto da se podaci prebacuju preko „glavnog“ uređaja, bilo koji uređaj može razmjenjivati podatke s bilo kojim drugim uređajem LonWorks u mreži. Drugo, LonWorks nije vezan ni za jedan fizički komunikacijski sloj. Ako je DeviceNet ograničen na CAN, a Profibus i Modbus su ograničeni na RS485, LonWorks može koristiti upleteni par, Ethernet ili čak mrežu napajanja kao svoj komunikacijski kanal. Konačno, mrežni podaci koji se razmjenjuju na LonWorksu konfiguriraju mrežni alat za konfiguraciju. Ova operacija koja se naziva "vezanje"

povezuje ulaz jednog uređaja s izlazom drugog uređaja neovisno o radu ili aplikacijskom softveru na bilo kojem uređaju.

LonWorks je standardna tehnologija za mnoge svjetske organizacije za standarde, uključujući ASHRAE, IEEE, ANSI, SEMI i mnoge druge. Zapravo, sposobnost LonWorksa preduvjet je za sudjelovanje u sve većem broju projekata automatizacije. LonWorks postaje glavni mrežni standard na tržištu poslovnih zgrada s velikim brojem dobavljača sustava za automatizaciju građevina koji se standardiziraju na LON, uključujući Siemens Building Systems i Honeywell. Za profit na ovom tržištu važno je podržati LON.




**Slika 2.13.** Primjer fizičke i logičke podjele sustava temeljenog na LonWorks mreži [13]

Mreža se fizički sastoji od nekoliko kanala koji su međusobno povezani preko usmjerivača i ponavljača. Mreža je podijeljena na podmreže. Jedna domena može imati do 255 podmreža s najviše 127 čvorova, što daje najviše 32.385 čvorova po domeni. Čvorovi se mogu grupirati, a po jednoj domeni moguće je odrediti 256 grupa. Ovaj primjer sadrži jednu grupu koja se proteže na tri čvora na različitim podmrežama i kanalima.

Postoje različiti primopredajnici koji podržavaju nekoliko prijenosnih medija. Najčešći medij je upletena parica s brzinom prijenosa podataka od 78 kib/s, a signal se kodira kao razlika napona između dva vodiča. Kompatibilna inačica upletenoj parici je Link Power, koji također osigurava napajanje (42,4 V DC) za čvorove spojene preko upletene parice.

Za okosnu mrežu (engl. backbone), upletena parica može prenositi podatke brzinom do 1250 kib/s, ali s manjom udaljenošću od 130 m između čvorova. Topologija mreža koja je izvedena

upletenom paricom je slobodna (ne mora biti strogo linijska ili zvjezdasta). Mreže se mogu širiti u slobodnim topologijama s proizvoljnim granama i petljama. Pri tome treba imati na umu da se smanjuje najveća udaljenost. Primjerice, linijska sabirnica s kratkim granama omogućava maksimalnu udaljenost od 2.700 m između čvorova, dok je u slobodnoj topologiji najveća udaljenost ograničena na 500 m.

Ostali podržani prijenosni mediji su energetska mreža (brzine do 10 kib/s), optička vlakna (1,25 Mib/s), radijski prijenos (do 19,5 kib/s) te ranije spomenuti LonWorks/IP (1000 Mib/s). Za povećanje dometa LonWorks mreže mogu se koristiti ponavljači koji osvježavaju sve dolazne signale i šalju ih na drugi mrežni segment (koji mora biti isti medij i mora koristiti isto kodiranje poruka). Obzirom da LonTalk implementira OSI referentni model, LonWorks mreže se mogu povezati i na višim slojevima. Mostovi (engl. bridges) koji rade na sloju veze podataka, mogu se koristiti za povezivanje mreža koje rade na različitim medijima i koriste različita kodiranja. Oni također osiguravaju da se na drugu stranu prosljeđuju samo ispravne poruke.

## 2.10. KNX

KNX je otvoreni standard (EN 50090, ISO/IEC 14543) za automatizaciju u zgradarstvu. KNX uređaji obično služe upravljanju rasvjetom, roletama i prozorima, sustavima HVAC, sigurnosnim sustavima, upravljanjem energentima, audio video sustavima, bijelom tehnikom, ekranima, služe za daljinsko upravljanje itd.

KNX svoje korijene nalazi u tri starija standarda: European Home Systems Protocol (EHS), BatiBUS te European Installation Bus (EIB ili Instabus). Kao fizički prijenosni medij može koristiti upletenu paricu (u topologiji stabla, linije ili zvijezde), energetsku mrežu (KNX Powerline 110 ili PL 110), radio vezu (KNX-RF) te IP veze (KNXnet/IP).

Podržane topologije mreže su stablasta, linijska i zvjezdasta (prstenasta topologija nije dopuštena). Na KNX mreži moguće je povezati najviše 57.375 uređaja. U ovoj mreži povezani uređaji formiraju distribuiranu aplikaciju te tako povezani uređaji izravno komuniciraju. Za programiranje KNX sustava koriste se modeli sa standardiziranim tipovima podataka i objektima, a kroz što se stvaraju logički kanali između pojedinih uređaja. KNX uređaji u pravilu su povezani upletenom paricom, a konfiguriraju se preko kontrolera.

Sabirnica, osim za prijenos podataka, može služiti i za napajanje svih povezanih uređaja. Postoje četiri vrste uređaja:

- senzori (tipke, prekidači, termostati, anemometri, detektori pokreta) koji prikupljaju podatke i šalju ih preko sabirnice u formi telegrama,
- aktuatori (dimeri rasvjete, ventili, zasloni, ekrani, displeji)
- kontroleri (za nadzor temperature, upravljanje roletama itd.)
- sistemski uređaji i komponente

KNX RF podržava radijske veze koje su kompatibilne s bežičnim M-Bus-om, europskim standardom za mjerne uređaje, pa je tako moguća integracija s drugim uređajima. KNX RF radi na središnjoj frekvenciji 868,3 MHz, a koja se nalazi u opsegu rezerviranom za SRD (uređaje kratkog dometa). U području 868.0–868.6 MHz primjenjuje se ograničenje ciklusa emitiranja na manje od 1%. Podaci se prenose brzinom od 16,4 kib/s pomoću modulacije FSK i Manchester kodiranja. Format okvira za KNX RF temelji se na opisu u IEC 60870-5.

KNX Powerline 110 (PL110) koristi prijenos podataka i napajanje uređaja preko gradske mreže 230 V/50 Hz. Podržana je dvosmjerna half-duplex komunikacija. Podaci KNX moduliraju se koristeći SFSK modulaciju sa središnjom frekvencijom od 110 kHz. Signal se ubacuje između faznog i nul-vodiča te se modulira sinusoidalni napon mreže. Fizička topologija mreže nema ograničenja.

Moguće je instalirati ponavljače u trofazne mreže. Zbog relativno loših prijenosnih svojstava mrežne mreže, brzina prijenosa podataka ograničena je na 1200 bit/s. Svaki je oktet podataka kodiran u 12-bitni znak (8-bitni podaci, 4 bita za ispravljanje pogreške).

Upravljanje pristupom mediju temelji se na tehnici vremenskih odsječaka, a kako bi se smanjila vjerojatnost kolizije. Nakon što protekne minimalno razdoblje tišine između dva podatkovna okvira, dva su vremenska odsječka rezervirana za čekanje na prijenos visokog prioriteta, a slijedi ih još sedam koje čekaju čvorovi s potrebnom za standardnim prijenosom (bez prioriteta) te potom nasumično biraju nasumično početno vrijeme slanja.

Što se tiče prijenosa KNX telegrama preko IP mreža, KNXnet/IP (ranije poznat kao EIBnet/IP) trenutno se omogućava središnje i daljinsko upravljanje. KNXnet/IP navodi nekoliko kategorija usluga. KNXnet/IP temeljne usluge definiraju strukturu paketa i metode potrebne za otkrivanje i samoopisivanje KNXnet/IP poslužitelja te za postavljanje i održavanje komunikacijskog kanala između klijenta i poslužitelja

# 3. UZROCI SMETNJI U INDUSTRIJSKIM MREŽAMA

Industrijski komunikacijski sustav mora udovoljiti određenom podskupu sigurnosnih ciljeva ovisno o njegovoj specifičnoj funkciji te okruženju u kojem se nalazi.

Namjerno kršenje sigurnosnih ciljeva smatra se napadom. Napadi su u osnovi sve aktivnosti koje su usmjerene na ugrožavanje sigurnosti podataka, računalnih sustava i komunikacijskih mreža. Napade mogu pokrenuti osobe (ili drugi sustavi) izvan postrojenja ili sami zaposlenici tj. osobe (ili drugi sustavi) unutar postrojenja. Razlikujemo ciljane i nasumične napade. Ciljani napadi usmjereni su nanošenju štete određenom sustavu ili vrsti sustava (primjerice s ciljem industrijske špijunaže, ratnih sukoba ili terorizma). Nasumični napadi ugrožavaju i štete svakom ranjivom sustavu do kojeg je moguće doći. Ciljanim napadima neizbježno prethodi prikupljanje informacija o cilju napada (primjerice korištenje svih javno dostupnih, ali i specifičnih informacija o ciljanom sustavu te korištenje namjenskih alata za otkrivanje ranjivosti sustava koji je na komunikacijskoj mreži).

Najčešće vrste napada i smetnji su:

- DoS (Denial of service): Napad uskraćivanjem resursa. Cilja napadača je smanjiti dostupnost sustava kako ne bi obavljao svoj zadatak.
- Prisluškivanje (Eavesdropping): Cilj napadača je narušiti povjerljivost komunikacije, primjerice prisluškivanjem paketa (engl. packet sniffing) na lokalnoj mreži ili presretanjem bežične komunikacije.
- MITM (man-in-the-middle) napad: U ovoj vrsti napada napadač djeluje istodobno prema oba kraja komunikacije, te se tako ponaša kao sudionik razmjene podataka. Uz to što je narušena povjerljivost komunikacije, ovo također omogućuje promjenu razmijenjenih podataka pa tako narušava i cjelovitost (integritet) komunikacije. Pomoću ove vrste napada moguće je pronaći i iskoristiti slabosti u izvedbi nekog komunikacijskog protokola (primjerice u razmjeni ključeva za šifriranje podataka) ili primjeni autentikacijskih protokola, a kako bi se nadziralo i upravljalo šifriranom razmjenom podataka.
- Neovlašteni ulazak (provala) u sustav: Narušavanjem autentikacije i kontrole pristupa napadač stječe mogućnost kontrole nad komunikacijskih sustavom i povezanim sustavom, a tako može zaobići i ciljeve povjerljivosti i cjelovitosti. Provala u sustav podrazumijeva penetraciju u veći broj podsustava i postepeno neovlašteno povećavanje ovlasti napadača u napadnutom sustavu.

- Virus: Napadi temeljeni na virusima manipuliraju legitimnim korisnikom kako bi zaobišli mehanizme provjere autentičnosti i kontrole pristupa, a s ciljem izvođenja zlonamjernog koda koji je napadač ubacio u sustav. U praksi se virusni napadi često šire nenamjerno i među ranjivim sustavima i korisnicima. Ovakvi napadi izravno ili neizravno smanjuju dostupnost inficiranih sustava trošeći preveliku snagu procesiranja računala na kojem se izvode ili zauzimaju previše mrežne propusnosti (bandwidth).
- Trojan: Trojan je posebna vrsta programa u kojem se zlonamjerna aktivnost skriva iza željene funkcionalnosti programa. Najčešće ga korisnici sami postave na računalni sustav i pokreću, pri čemu su nesvjesni njegove stvarne prirode. Trojanci se koriste kako bi se zaobišla povjerljivost i kontrola pristupa.
- Crv (worm): Crv je zlonamjerni program čiji se mehanizam širenja oslanja na automatsko istraživanje i iskorištavanje ranjivosti u ciljanom sustavu. Pri tome ne ovisi o ljudskoj aktivnosti. Infekcije crvima često nisu ciljane (ili zbog svoje prirode izmaknu kontroli i prošire se izvan eventualno ciljanog sustava), a svojom aktivnošću stvaraju probleme s dostupnošću pogođenih sustava. Crv u sebi može sadržavati zlonamjerni kod za pokretanje distribuiranog ciljanog napada sa svih zaraženih računala.

# 4. ULOGA INDUSTRIJSKIH MREŽA U INDUSTRIJSKIM SUSTAVIMA

Gdje protokoli za industrijsku automatizaciju uključuju pitanje sigurnosti, isti uglavnom i rješavaju pitanje kontrole pristupa subjektima koji su definirani u pripadnom standardu/normi. Sustav automatizacije mora imati odgovarajuće alate za upravljanje vlastitim sigurnosnim postavkama. Za kontrolu pristupa moraju se definirati grupe korisnika i njihove uloge, a dopuštene operacije moraju biti predodređene i mora postojati mogućnost njihova finog podešavanja. Također je nužno moći konfigurirati popise kontrola pristupa. U nastavku se razmatraju sigurnosne funkcije određene nekim čestim normama ili preporukama za industrijske komunikacijske protokole.

OPC: OPC je specifikacija aplikacijskog sloja za komunikaciju između programskih komponenti industrijske automatizacije. OPC definira standardizirana sučelja kroz koja OPC klijenti pristupaju objektima na OPC poslužiteljima. Radne stanice operatora obično su OPC klijenti koji pristupaju OPC poslužiteljima koji djeluju kao pristupnici (gateway) komponentama za automatizaciju.

OPC standardno sučelje skriva složenost komunikacijskih protokola koji su ovisni o pojedinom uređaju te tako jamči otvorenu povezanost [i interoperabilnost] u industrijskoj automatizaciji i sustavima. OPC nadograđuje Microsoftov komponentni objektni model (COM), tako da su implementacije OPC-a u praksi ograničene na platforme koje podržavaju COM. Specifikacija OPC pristupa podacima (OPC data access, OPC DA) određuje standardizirane operacije čitanja za prijenos procesnih podataka u stvarnom vremenu. Ti se podaci zajedno s oznakom vremena i informacijama o statusu šalju s uređaja za automatizaciju (kao što su PLC-ovi) u aplikacije više razine (kao što su razni nadzornici procesa i sustavi vođenja proizvodnje).

Ostale specifikacije OPC definiraju alarme i obavijesti o događajima, razmjenu podataka između komunikacije poslužitelj-poslužitelj preko Ethernet mreža, pristup pohranjenim povijesnim podacima i ostale funkcije. Novije verzije OPC specifikacije koriste format XML za određivanje pravila i formata za predstavljanje i objavljivanje podataka iz postrojenja. Primjena formata XML jamči neovisnost platforme OPC. OPC sigurnosna specifikacija definira neobavezna sigurnosna sučelja OPC objekata. Specifikacija se bavi kontrolom pristupa i temelji se na sigurnosnom modelu koji se koristi na platformi Microsoft Windows. Principali (definirani kao osobe ili računalni procesi) prilikom pristupa sigurnosnom objektu moraju predstaviti svoje vjerodajnice (pristupni token) preko zaštićenog komunikacijskog kanala. Referentni nadzornik

provjerava vjerodajnice prema podacima na popisu kontrole pristupa (ACL) povezanim s objektom, te u skladu s tim daje ili uskraćuje pristup.

Tamo gdje je dostupno, primjerice u Windows domeni, OPC poslužitelji koji imaju implementirane sigurnosne elemente koristit će Windows / Kerberos vjerodajnice i uslugu referentnog nadzornika pripadnog COM middleware softvera.

Vjerodajnice se moraju generirati i za ovjerene korisnike i procese te se potom pohranjuju (spremaju u pred memoriju, cache) na način koji jamči njihovu zaštitu. Autentifikacija korisnika u praksi je prepuštena postupku prijave u sustav Windows. U slučaju da Windows vjerodajnice nisu dostupne, (primjerice ako se OPC poslužitelju pristupa s neke druge domene ili s Interneta), OPC poslužitelji moraju dodijeliti i upravljati vlastitim „privatnim“ vjerodajnicama, kao što su određene kombinacije korisničkih ID-ova i lozinki. OPC poslužitelj je zadužen koristiti mehanizme koji sprečavaju kompromitiranje ovih vjerodajnica, a što se izvodi na neki od ranije opisan način (korištenje hasheva, kriptiranih podataka itd.). OPC poslužitelj može implementirati jednu od tri razine sigurnosti:

- Ne primjenjuje se sigurnost.
- DCOM sigurnost: Dozvole za pokretanje i pristup OPC poslužitelju ograničene su na odabrane klijente. Ovo je predefinirana razina sigurnosti koju pruža distribuirani COM (DCOM; vidi dolje) i obično se upravlja pomoću DCOM alata za konfiguraciju sigurnosnih parametara.
- OPC sigurnost: OPC poslužitelj služi kao referent i nadzornik za kontrolu pristupa sigurnosnim objektima koji su karakteristični za isporučitelja sustava (vendor-specific), a koje je izložio OPC poslužitelj. U implementaciji se koristi programska sigurnost DCOM-a. Standard ne propisuje ili ne sugerira koje objekte treba osigurati. Ako se implementira OPC sigurnost, DCOM sigurnost mora biti konfigurirana za omogućavanje pristupa sučeljima poslužitelja.

OPC sigurnosna specifikacija pokriva samo kontrolu pristupa poslužitelju / objektu, ali se ne bavi povjerljivošću i integritetom tijekom prijenosa. U distribuiranim konfiguracijama u kojima se OPC klijenti i poslužitelji nalaze na različitim domaćinima/računalima (hosts), DCOM se obično koristi umjesto COM-a.

Mjere sigurnosti nad mrežom prebačene su na DCOM. Izvedbe OPC-a mogu koristiti COM, a umjesto DCOM-a implementirati vlastiti mrežni softver (middleware). Neke se izvedbe proširuju na DCOM servise u smislu rješavanja otpornosti na pogreške i redundanciju.

Bilo koja alternativna izvedba komunikacije za OPC trebala bi ponuditi slične usluge kao što su DCOM usluge opisane u nastavku, posebno u kontekstu mrežne sigurnosti. Kao što je već spomenuto, nove OPC-XML specifikacije zamjenjuju DCOM usluge jednostavnijim i platformski neovisnim komunikacijskim protokolom SOAP (Simple Object Access Protocol).

SOAP uglavnom radi na protokolu HTTP, a u tom se slučaju može vrlo lako zaštititi kriptografskim mehanizmom na transportnom sloju (TLS, ranije i SSL). Premda je riječ o tehnologiji koja svoj početak ima u prvoj polovici 1990-ih godina, podrška za DCOM se proteže sve do MS Windows Server 2016, a postoje i alternativne implementacije na Linux platformi, poput TangramCOM. Više se neće ulaziti u detalje sigurnosti DCOM-a obzirom da materija nadilazi opseg ovog predmeta. MMS: Ranije spomenuti MMS je preporuka za razmjenu poruka između raznih komponenti automatizacije i PLCova, a djeluje na aplikacijskom sloju. MMS je definiran 1980-ih i tako je prethodio OPC-u. Danas se MMS uvelike koristi u automobilskoj industriji, a osnova je i za skup normi IEC 61850. MMS definira samo generičke/općenite usluge i objekte (varijable) te njihovo adresiranje.

Za definiranje posebnih objekata konkretne aplikacije potrebno je koristiti posebne dodatne standarde. MMS ne obuhvaća samo komunikaciju između klijenta i poslužitelja, već i partnersku komunikaciju (engl. peer-to-peer network) u distribuiranim mrežama. MMS određuje neke značajke kontrole pristupa na temelju jednostavne provjere autentičnosti zaporke. Ne nudi usluge osiguranja povjerljivosti i neporecivosti.

Početni MMS zahtjev za pridruživanje (engl. association request) postavlja MMS okruženje između klijenta i poslužitelja, tj. stvara polutrajne komunikacijske veze i razmjenjuje informacije o mogućnostima koje nudi poslužitelj. Zahtjev za pridruživanje ima neobavezni parametar provjere autentičnosti (lozinku), a koji klijent treba uručiti poslužitelju. Ova provjera autentičnosti koristi se za kontrolu pristupa MMS objektima.

Objekti sadrže popise kontrola pristupa (ACL) koji navode uvjete pod kojima su usluge tražene od nekog objekta dopuštene. Uvjeti su identitet korisnika (aplikacije) i / ili lozinka, dok usluge uključuju stvaranje, čitanje, pisanje, izvršavanje, brisanje ili izmjenu. Uvjeti se mogu odrediti zasebno za pojedinačne objekte ili za sve objekte. MMS pretpostavlja da je Ethernet LAN temeljna komunikacijska mreža između klijenata i poslužitelja. Izvorna specifikacija opisala je skup protokola prema ISO-u, ali danas se većina implementacija temelji na skupu protokola TCP/IP.

U slučaju implementacije na TCP/IP-u, preslikavanje MMS-a na TCP definira preporuka RFC 1006 , a pri čemu se određuje format podataka, složaj okvira te broj porta. U slučaju potrebe za korištenjem sigurne komunikacijske veze, ista se može realizirati korištenjem uobičajenih protokola IPSec ili TLS.

IEC 61850: Riječ je o novijem skupu protokola za komunikaciju između digitalnih releja te za cjelokupni SCADA sustav na razini trafostanice. IEC 61850 određuje programske cjeline, modele podataka, usluge, protokole i formate podataka za automatizaciju trafostanica (općenito podstanica) elektroenergetske mreže. Od posebne su važnosti za informacijsku sigurnost mogućnosti kontrole pristupa i preslikavanje protokola komunikacije, a što određuje sigurnosna obilježja mreže.

IEC 61850 propisuje da čvorovi (eng. nodes) moraju osigurati kontrolu pristupa temeljenu na identifikaciji čvorova (u slučaju komunikacije M2M tj. stroj-stroj) te na provjeri autentičnosti korisnika i kontrole pristupa sustavu (u slučaju korisnika HMI-a tj. sučelja čovjek-računalo). Korisnici moraju biti prepoznati kao operatori, administratori itd. te dobiti odgovarajuće privilegije pristupa za najčešće operacije stvaranje / pregled / izvršavanje itd. Pri početnom pridruživanju klijent bi trebao poslati parametre provjere autentičnosti (dakle korisnički ID + traženi prikaz + lozinka) na poslužitelj. Kontrola pristupa koju obavlja poslužitelj ograničava prikaze (dostupni skup objekata koji je će prikazati na sučelju HMI), a na temelju identiteta (ID-a) klijenta.

U operativnim kontrolnim radnjama, poput naredbi poslanih na prekidače u trafostanici, objekt treba provjeriti ovlaštenja klijenta prije izvođenja tražene operacije. Pridruživanje prema IEC 61850 izravno je mapirano na zahtjev za pridruživanje MMS-a. Kao što je ranije opisano, MMS se dalje preslikava na TCP/ IP na Ethernetu. Uređaji za automatizaciju trafostanica pokreću algoritme za zaštitu električne elektroenergetske mreže gdje je presudno osigurati prijenos podataka s vrlo malim kašnjenjem (latencijom), pa je tako, primjerice, potrebno osigurati da se određena radnja dovrši u vremenu do najviše 300 milisekundi.

Za brzi prijenos vremenski kritičnih podataka za općeniti skup događaja u trafostanici (GSE), poput aktiviranja zaštitnih prekidača elektroenergetske mreže ili za brzu distribuciju uzorkovanih izmjerenih vrijednosti struja i napona (SMV), IEC 61850 definira izravno mapiranje jednostavnih paketa podataka na Ethernet pakete. Distribucija podataka prema načelu peer-to-peer i podrška kocepta izdavač-pretplatnik (publisher-subrscriber) koristi Ethernet okvire broadcast i multicast.

Usmjeravanje na IP sloju se zaobilazi zbog problema kašnjenja. To je primjenjivo na terenskim ili upravljačkim mrežama za brzi prijenos sirovih, neobrađenih podataka s terenskih uređaja na kontrolere trafostanica. Za segmentiranje prometnog opterećenja te za osiguravanje brzog prijenosa mogu se koristiti VLANovi (IEEE 802.1Q) te postavljanje prioriteta na mreži (primjerice koristeći QoS). Važno je razumjeti kako se IEC 61850 ne bavi sigurnom komunikacijom, već se umjesto toga naslanja na aktivnosti koje obavlja druga IEC radna skupina. Aktualna norma koja pokriva sigurnost u ovom području je IEC 62351. IPSec je primjenjiv tamo gdje je komunikacija temeljena na protokolima TCP/IP. Međutim, na Ethernet sloju u principu ne postoje sigurnosni standardi tako da ni ne postoje tipizirani alati za zaštitu prijenosa GSE i SMV podataka. Primatelji identificiraju podatke koristeći MAC adrese izvora, ali to pruža relativno slabo jamstvo autentičnosti, jer je MAC adrese lako lažirati. Također se mogu koristiti i VLAN-ovi za ograničavanje distribucije podataka na određene mrežne segmente, no ni to nije dovoljna sigurnosna mjera.

# 5. INDUSTRIJSKI PROTOKOLI U PRIMJENI KOD FREKVENCIJSKIH PRETVARAČA

U ovom dijelu završnog rada ukratko je objašnjeno što su to frekvencijski pretvarači a kao primjer dan je frekvencijski pretvarač VLT® EtherNet/IP MCA 121.

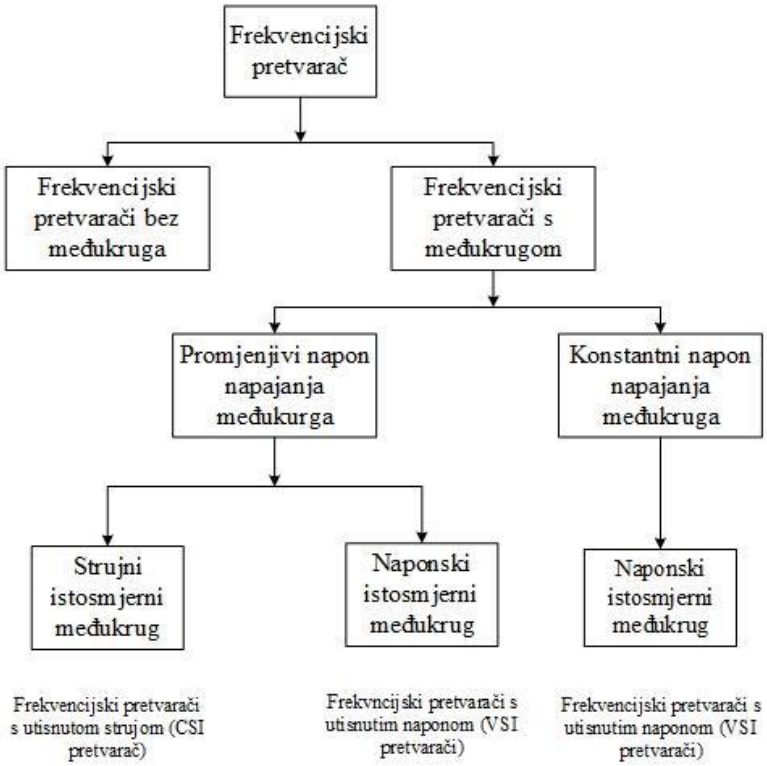
S obzirom da postoji velika potreba za uređajima koji povećavaju stupanj automatizacije proizvodnih procesa, tj. povećanje učinkovitosti proizvodnje, ona potiče razvoj frekvencijskih pretvarača kojima se upravlja brzinom vrtnje izmjeničnih motora.

Frekvencijski pretvarači su elektronički uređaji. Pomoću njih se izmjenični napon konstantne vrijednosti i frekvencije pretvara u napon promjenjive vrijednosti i frekvencije. Pomoću ovih uređaja je moguće kontinuirano upravljati brzinom vrtnje izmjeničnih motora.

U današnjoj industriji najčešće se upotrebljavaju trofazni asinkroni motori, dok je upotreba jednofaznih asinkronih motora gotovo zanemariva. Frekvencijskim pretvaračima mogu se pogoniti i trofazni i jednofazni asinkroni motori.

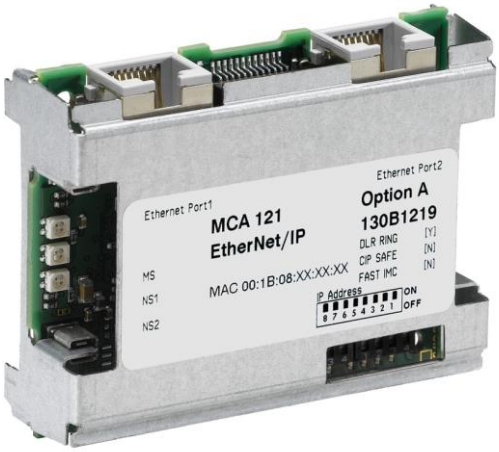
Frekvencijski pretvarači koji se koriste u industriji za regulaciju brzine vrtnje ili upravljanje trofaznih izmjeničnih motora rade na dva osnovna načina:

- Frekvencijski pretvarači bez istosmjernog međukruga (izravni frekvencijski pretvarači)
- Frekvencijski pretvarači s istosmjernim međukrugom (neizravni frekvencijski pretvarači)




**Slika 5.1.** Podjela frekvencijskih pretvarača [14]

Frekvencijski pretvarač VLT® EtherNet/IP MCA 121 je uzet kao primjer jer se povezuje s motorom putem Etherneta. U sljedećem tekstu prikazane su osnovne karakteristike uređaja.




**Slika 5.2.** Frekvencijski pretvarač VLT® EtherNet/IP MCA 121 [15]

Uređaj VLT® EtherNet/IP MCA 121 nudi opciju uključi i radi (plug and play) te mogućnost spajanja s EthetNet/IP osnovnim mrežama, kao što su Rockwell PLC sustavi preko CIP (Common Industrial Protocol) protokola.

Uređaj može podnijeti jednu EthetNet/IP vezu sa zahtjevom intervala paketa (RPI-Requested Packet Interval) od 1 ms u oba smjera. To ga čini jednim od EthetNet/IP uređaja s najboljom izvedbom na tržištu.

Uređaj ima ugrađen 2-portni prekidač koja olakšava tradicionalne linije mreže ili prstenastu topologiju (DLR- Device Level Ring). Prstenasta topologija na MCA 121 je bazirana na Beacon tehnologiji, kako bi postigla najbrže otkrivanje kvarova s vremenom oporavka od 3 ms. Ova topologija eliminira potrebu za kompliciranim kablovima i skupim industrijskim Ethernet prekidačima, koji se koriste u zvjezdastoj topologiji.

**Druge značajke:**

- Ugrađeni web poslužitelj za daljinsku dijagnozu i čitanje dijagnoze osnovnog diska.
- Može se konfigurirati E-mail notifikator za slanje poruka putem e-maila na jedan ili više prijemnika ukoliko se pojavi određeno upozorenje, alarm ili čišćenje.
- Dodavanje uputa (AOI- Add On Instruction) koje smanjuju vrijeme, napor i troškove uključene u razvoj PLC programa. Upute sadrže popis unaprijed definiranih oznaka koje se koriste za kontrolu diska.
- Brza integracija PLC alata za konfiguriranje putem EDS datoteke.

Primjena protokola:

- EtherNet/IP (industrijski protokol) za postavke upravljanja i parametara.
- CIP (Common Industry Protocol) za komunikacija s PLC-om.
- HTTP (Hypertext Transfer Protocol) za dijagnozu putem ugrađenog web poslužitelja.
- SMTP (Simple Mail Transfer Protocol) za e-mail obavijesti.
- DHCP (Dynamic Host Configuration Protocol) za konfiguraciju automatske IP adrese.
- Podržava vezu s VLT® alatom za kontrolu pokreta MCT 10 preko TCP/IP-a.
- Podržava čitanje / pisanje razbacanih parametara diska.

| Značajka | Korist |
|---|---|
| Povezivanje s mrežama temeljenim na EtherNet/IP | Povezuje se s Rockwell PLC sustavom putem CIP (Common Industry Protocol) |
| Zahtjev intervala paketa (RPI) od 1 ms | Visoke performanse |
| Ugrađeni web-poslužitelj | Daljinska dijagnoza i čitanje osnovnih parametara diska |
| E-mail notifikator | Obavijesti ako se pojave upozorenja ili alarmi |
| Dva Ethernet priključka s ugrađenim prekidačem | Jednostavno spajanje<br>Nema potrebe za skupim prekidačima ili čvorištima |
| Temelji se na CIP protokolu | Ponovna uporaba PLC programa prilikom migracije s DeviceNet na EtherNet/IP ili podržava obje tehnologije |
| Podržava tehnologiju Device Level Ring (DLR) | Greška u jednom od Ethernet kabela ili jednom od uređaja u prstenu, neće dovesti do gubitka komunikacije na svim uređajima |

Opcija VLT® EtherNet/IP MCA 121 brzo se integrira u PLC alat za konfiguraciju, putem datoteke EDS.

VLT® disk podržava ODVA i FC profile za objekte U/I (Ulaz/Izlaz) sklopa. Isto tako, on također podržava:

- CIP objekte, uključujući U/I (Ulaz/Izlaz) za pet različitih sklopova objekata (AO) za prilagodbu komutacije za optimalne performanse.
- Objekt AC diska.
- Ostale objekte za jednostavnu podršku konfiguracije i integracije s PLC-ovima koji podržavaju EtherNet/IP.

**Preuzimanja**

Ove datoteke su besplatno dostupne u području za preuzimanje softvera na drives.danfoss.com.

# 6. ZAKLJUČAK

Nagli razvoj računala omogućuje njihovu primjenu u različitim ljudskim djelatnostima i potrebu povezivanja različitih računalnih sustava radi brže razmjene podataka i lakšeg upravljanja. Računalne komunikacijske mreže pojedinih proizvođača opreme nisu bile kompatibilne s mrežnom opremom drugih proizvođača. Iz tog razloga proizvođači su se morali okrenuti normiranim i otvorenim tehnološkim rješenjima.

Komunikacijska mreža je skup dva ili više povezanih računala. Računala su povezana ukoliko mogu razmjenjivati informacije. Međusobna komunikacija između čvorova računalne mreže odvija se pomoću komunikacijskih protokola. Komunikacijski protokol je skup pravila pomoću kojih dolazi do razmjene informacija. Neke od najpoznatijih komunikacijskih mreža koje se koriste u industrijskim sustavima su: CAN (Controller Area Network), Profibus, PROFInet, INTERBUS, WorldFIP, Foundation Fieldbus, MODBUS, Industrijski Ethernet, EtherCAT, LonWorks i KNX.

# LITERATURA


1. [BiVan96] S. Biegacki, D. VanGompel. The application of deviceNet in process control. ISA Transactions, 35:169–176, 1996.
2. [CANW19] Web stranica „Controller Area Network (CAN bus)“, https://en.wikipedia.org/wiki/CAN_bus, svibanj 2020.
3. [CIA02] Grupa autora, CANopen application layer and communication profile, version 4.02. CiA (CAN in Automation), Nuremberg, Germany, 2002. EN 50325-4 Standard.
4. [CCERT05] Grupa autora, Nacionalni program informacijske sigurnosti u RH, http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-04-110.pdf, svibanj 2020.
5. [CVJ07] S. J. Cvjetković, Telekomunikacije u elektroenergetskim sustavima, Sveučilište u Splitu, 2015.
6. [FFSEG12] FOUNDATION™ Fieldbus System Engineering Guidelines (AG-181), Revision 3.2.1, Fieldbus Foundation, Austin, Texas 78759-5316 SAD, rujan 2012.
7. [IEC61850] Grupa autora, IEC 61850, dostupno na: https://en.wikipedia.org/wiki/IEC_61850, svibanj 2020.
8. [ISO11898] International Standards Organisation. ISO 11898. Road vehicles—Interchange of digital information—Controller area network (CAN) for high speed communication. ISO, Geneva, Switzerland, 1993.
9. [ISOCAN01] ISO. Road vehicles—Controller area network (CAN)—Part 4: Time triggered communication. ISO, Geneva, Switzerland, 2001.
10. [Kon19] Končar INEM, Tehnička dokumentacija sustava INEMATIC 300, Končar - Elektronika i informatika d.d., 2004.
11. [MMS03] ISO, Industrial Automation Systems—Manufacturing Message Specification (MMS), ISO 9506-1:2003, 9506-2:2003, 9506-5:1999, 9506-6:1994, 2003.
12. [RB1991] R. Bosch. CAN specification version 2.0. BOSCH, Stuttgart, Germany, 1991.
13. [MTK19] Grupa autora, Tehnička dokumentacija sustava mrežnotonfrekventnog upravljanja, INŽENJERING ZA MTK d.o.o., 2009.
14. [OLS14] J. Olsson, 6LoWPAN demystified, Texas Instruments, Dallas, Texas, SAD, 2014.
15. [OPCF] Grupa autora, Open Platform Communications Foundation, https://opcfoundation.org/about/what-is-opc/, svibanj 2020.

16. [OSIIICCP] Grupa autora, Inc., Inter-Control Center Communications Protocol, Open systems International, web stranica https://www.osii.com/fr/files/product_pdf/OpenICCP1p_DD_3.0.pdf, svibanj 2020.
17. [SNMP] Grupa autora, Simple Network Management Protocol, https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol, svibanj 2020.
18. [Sucic09] S. Sučić, Sustavi upravljanja, Sigurnosni komunikacijski protokoli u elektroenergetskom sustavu, FER i Končar inženjering za energetiku i transport, Zagreb, 2009.
19. [VLANCARNET] Eldis Mujarić, Računalne mreže - Virtualna lokalna mreža (VLAN), web stranica sys.portal Carneta, https://sysportal.carnet.hr/node/671, svibanj 2020.
20. [DANFOSS98] Danfoss, Najvažnije o frekvencijskim pretvaračima, Graphis Zagreb, http://www.graphis.hr/news/danfoss/danfos_web_72dpi.pdf, 1998.
21. [VLTMCA121] Danfoss, Fact Sheet, VLT® EtherNet/IP MCA 121
22. [Bencic09] Benčić Z., Najvažnije o frekvencijskim pretvaračima, GRAPHIS Zagreb, 2009., ISBN: 978-953-279-019-1

Izvori slika

1. Slika 2.1. CAN mreže značajno smanjuju ožičenje [https://www.ni.com/en-rs/innovations/white-papers/06/controller-area-network--can--overview.html]
2. Slika 2.2. primjer napona koji se javljaju na CAN sabirnici [BiVan96 S. Biegacki, D. VanGompel. The application of deviceNet in process control. ISA Transactions, 35:169–176, 1996.]
3. Slika 2.3. Primjer tipičnih konektora za povezivanje Profibus uređaja [Wikipedia]
4. Slika 2.4. Fleksibilnost INTERBUS topologije i način ožičenja uređaja [FFSEG12] FOUNDATION™ Fieldbus System Engineering Guidelines (AG-181), Revision 3.2.1, Fieldbus Foundation, Austin, Texas 78759-5316 SAD, rujan 2012.]
5. Slika 2.5. Primjer povezivanja različitih INTERBUS uređaja [Phoenixcontact]
6. Slika 2.6. Slojevi WorldFIP standarda [Springer]
7. Slika 2.7. Slojevi WorldFIP kodiranje [Springer]
8. Slika 2.8. WorldFIP okvir [Springer]

9. Slika 2.9. Primjer jednostavne topologije sabirnice FF [CIA02 Grupa autora, CANopen application layer and communication profile, version 4.02. CiA (CAN in Automation), Nuremberg, Germany, 2002. EN 50325-4 Standard.]
10. Slika 2.10. Modbus serijska arhitektura [Kon19 Končar INEM, Tehnička dokumentacija sustava INEMATIC 300, Končar - Elektronika i informatika d.d., 2004.]
11. Slika 2.11. Modbus TCP arhitektura [Kon19 Končar INEM, Tehnička dokumentacija sustava INEMATIC 300, Končar - Elektronika i informatika d.d., 2004.]
12. Slika 2.12. Primjer arhitekture komunikacijskog sustava u tvornici [CIA02 Grupa autora, CANopen application layer and communication profile, version 4.02. CiA (CAN in Automation), Nuremberg, Germany, 2002. EN 50325-4 Standard.]
13. Slika 2.13. Primjer fizičke i logičke podjele sustava temeljenog na LonWorks mreži [Sucic09 S. Sučić, Sustavi upravljanja, Sigurnosni komunikacijski protokoli u elektroenergetskom sustavu, FER i Končar inženjering za energetiku i transport, Zagreb, 2009.]
14. Slika 5.1. – Podjela frekvencijskih pretvarača [Bencic09 Benčić Z., Najvažnije o frekvencijskim pretvaračima, GRAPHIS Zagreb, 2009., ISBN: 978-953-279-019-1]
15. Slika 5.2. - Frekvencijski pretvarač VLT® EtherNet/IP MCA 121 [Digiconsolutions]

## SAŽETAK

Rane 1970-te godine donijele su nagli razvoj računala koja su nalazila svoju primjenu u različitim ljudskim djelatnostima, čime se javlja i potreba povezivanja različitih računalnih sustava s ciljem brže razmjene podataka i lakšeg upravljanja. Razvoj tih ranih računalnih komunikacijskih mreža uglavnom se naslanjao na mnogobrojna vlasnička tehnološka rješenja (engl. proprietary solutions) pojedinih proizvođača opreme. Svako od tih rješenja bilo je izvedeno prema vlastitim specifikacijama te gotovo u pravilu nije bilo kompatibilno s mrežnom opremom drugih proizvođača, što znači da se komunikacijske mreže različitih dobavljača nisu mogle jednostavno povezivati. Kako su se takve mreže širile, problemi su postajali sve očitiji. Proizvođači su ubrzo uvidjeli da se moraju odmaknuti od dotadašnje prakse i okrenuti normiranim i otvorenim tehnološkim rješenjima.



**Ključne riječi:** Industrijske mreže, Industrijska komunikacija, komunikacija u industriji 4.0.


# TYPES OF INDUSTRIAL NETWORKS AND THEIR ROLE IN INUSTRIAL SYSTEMS


## ABSTRACT

The early 1970s brought the rapid development of computers that found their application in various human activities, thus creating the need to connect different computer systems with the aim of faster data exchange and easier management. The development of these early computer communication networks mainly relied on numerous proprietary solutions of individual equipment manufacturers. Each of these solutions was performed according to its own specifications and was almost as a rule not compatible with the network equipment of other manufacturers, which means that the communication networks of different suppliers could not be easily connected. As such networks expanded, the problems became increasingly apparent. Manufacturers soon realized that they had to move away from previous practices and turn to standardized and open technological solutions.



**Key words:** Industrial Networks, Industrial Comunication, communication in INDUSTRY 4.0.

# ŽIVOTOPIS

Goran Horvat rođen je 15.07.1992. godine u Našicama. Školovanje započinje 1999. godine u osnovnoj školi u Đurđenovcu gdje ide na razna natjecanja iz matematike. 2007. godine upisuje Opću gimnaziju u Našicama. Upisuje preddiplomski sveučilišni studij Elektrotehnike smjera Elektroenergetika na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku 2011. godine, a kasnije se prebacuje na stručni studij.