Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.41
DOI: https://doi.org/10.24867/03BE23Tot

INDUSTRIJSKA IMPLEMENTACIJA MODBUS PROTOKOLA

INDUSTRIAL IMPLEMENTATION OF MODBUS PROTOCOL

Igor Tot, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U ovom radu opisani su osnovi SCADA sistema, industrijskih protokola komunikacije kao i detalji Modbus protokola. Predstavljeno je rešenje programske implementacije Modbus protokola u okviru SCADA sistema, u svrhu komunikacije sa udaljenim uređajima - koje zadovoljava realne industrijske potrebe, spram konteksta korišćenja.*

Ključne reči: SCADA, RTU, Modbus

Abstract – *This paper describes the fundamentals of SCADA systems, industrial communication protocols and specifics of the Modbus protocol. A software solution for implementing the Modbus protocol as means of communication with remote units is presented with regards to realistic industrial needs and constraints.*

Key words: SCADA, RTU, Modbus

1. UVOD

Familija Modbus protokola je namenjena za potrebe jednostavne komunikacije sa opremom za automatizaciju. Iako se može koristiti u različitim aplikacijama, najčešća primena ovih protokola je za povezivanje programabilnih logičkih kontrolera, ulazno-izlaznih modula i sl.

Ovaj rad je namenjen da ispita problematiku implementacije Modbus protokola u jedno realno industrijsko okruženje, sa ciljem predloga softverske implementacije koja je arhitekturalno dovoljno sveobuhvatna da predvidi poteškoće razvojnog ciklusa takvog sistema. Iz tih razloga se sagleda specifičnost implementacije Modbus protokola u proizvoljnom SCADA sistemu. Distribuirani SCADA sistem podrazumeva dovoljno kompleksnu softversku podršku, koja pruža mogućnost posmatranja problema implementacije Modbus protokola sa akcentom na skalabilnost, robusnost i softversku generičnost. Na temelju znanja o detaljima funkcionalnosti SCADA sistema i ulozi Modbus protokola u takvom okruženju - moguće je definisati problem i predložiti softversko rešenje implementacije Modbus protokola sa obzirom na potrebe životnog ciklusa takvog softvera.

2. SCADA SISTEM I ULOGA INDUSTRIJSKIH PROTOKOLA

Skup računarskih modula koji je prostorno distribuiran i međusobno povezan sa ciljem ostvarenja akviziciono-upravljačkih funkcija nad određenim fizičkim procesom u realnom vremenu - opisuje jedan SCADA (engl. *Supervisory Control And Data Acquisition*) sistem.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Branislav Atlagić, docent.

Ovakvi sistemi su specifične namene i strukture, i kao takvi obuhvataju širok spektar hardverske opreme i softverskih komponenti u svrhu ostvarenja tražene funkcionalnosti. Ključne komponente jednog SCADA sistema su: Udaljene RTU (engl. *Remote Terminal Unit*) ili PLC (engl. *Programmable Logic Controller*) jedinice, Nadzorno-Upravljačka MTU (engl. *Master Terminal Unit*) stanica i komunikaciona infrastruktura. Arhitektura SCADA sistema (slika 2-1) opisuje ulogu svake od ovih komponenti spram stanovišta akviziciono-upravljačke funkcije. Procesni ulazi u tom smislu podrazumevaju podatke digitalnog ili analognog tipa prikupljene putem senzora, dok procesni izlazi jesu komande nad raznim aktuatorima koji menjaju stanje sistema. Udaljeni uređaj jeste računar namenjen za rad u industrijskim uslovima (ekstremne temperature, pritisak, i sl.), dok nadzorno-upravljačka stanica kao centralna tačka SCADA sistema komunicira sa velikim brojem takvih računara posredstvom podsistema za komunikaciju. Nadzorno-upravljačka stanica je opremljena ozbiljnim PC računarom (ili grupom računara) na kojem se izvršava SCADA softver koji pruža nivo automatizacije procesa i estimaciju sistema spram obrađenih podataka sa polja.

Slika 2-1 – Arhitektura SCADA sistema

Pored funkcionalnih zahteva akvizicije i upravljanja podacima nad posmatranim fizičkim procesom, SCADA sistem zadovoljava i par osnovnih osobina kritičnog softverskog sistema. Kritičnost znači da greške pri radu sa ovakvim sistemom mogu da imaju katastrofalne posledice, pa iz tog razloga SCADA sistem podrazumeva minimizovano srednje vreme između ispada sistema, uz replikaciju podataka - visok nivo pouzdanosti. Sa druge strane, ovaj sistem mora biti dostupan u slučaju otkaza hardverskih ili softverskih komponenti, što podrazumeva visok nivo raspoloživosti. SCADA takođe zadovoljava i princip rada u realnom vremenu - odnosno, sve akcije nad sistemom podrazumevaju pojam logičke i vremenske ispravnosti; drugim rečima, ukoliko se željene akcije nad sistemom ne izvršavaju u predodređenim vremenskim intervalima - smatramo ih neispravnim, čak iako se tražena akcija logički uspešno izvršava. Konačno, SCADA sistem mora biti prostorno distribuiran po pitanju računarskih resursa.

SCADA sistem kao distribuirani računarski sistem razmenjuje poruke vezane za nadzor i upravljanje

posmatranim fizičkim procesom. Skup pravila i procedura koje kontrolišu tok komunikacije između komponenti distribuiranog računarskog sistema definiše komunikacioni protokol. Ta pravila su vezana za format i redosled poruka koje se razmenjuju, kao i svaku akciju koja se inicira prijemom određene poruke. Osnovne funkcije komunikacionih protokola su kontrola grešaka i upravljanje tokom podataka u mreži.

Budući da telekomunikacioni sistemi imaju strogo hijerarhijsku strukturu - realizovanu kroz više slojeva, komunikacioni protokol mora odrediti nivo na kojem se izvršava. Ova slojevitost definisana je ISO/OSI (engl. *Open Systems Interconnection Basic Reference Model*) modelom.

Prvi nivo protokola je fizički, i definiše električne i mehaničke karakteristike prenosnog kanala. Iznad njega su programski slojevi protokola. Svaki od njih proširuje skup usluga, oslanjajući se u potpunosti na funkcije prethodnog nivoa. Sprega između pojedinih slojeva protokola na istoj stanici vrši se tako da viši sloj koristi isključivo usluge prethodnog nivoa. [1]

Klasa protokola specifičnih za SCADA sisteme podrazumevana je terminom industrijski protokoli i industrijske mreže. Ovaj naziv naglašava njihovu primenu u industrijskim postrojenjima i odvaja ih od protokola iz oblasti računarstva i telekomunikacija. Industrijski protokoli se mahom oslanjaju na prvi (fizički) i sedmi (aplikacioni) sloj ISO/OSI modela i orijentisani su ka zadovoljenju aplikativnih zahteva akviziciono upravljačkog sistema.

3. MODBUS PROTOKOL

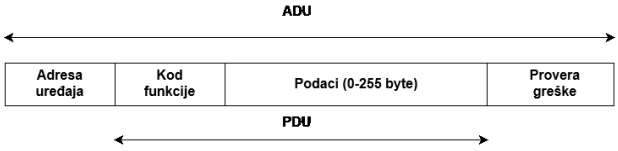
Industrijski komunikacioni protokol razvijen i predstavljen od strane kompanije Modicon (sada Schneider Electric) 1979. godine, primarno za komunikaciju sa programabilnim logičkim kontrolerima - Modbus - postao je *de facto* standardni oblik komunikacije pri povezivanju industrijskih uređaja. Modbus standard se odnosi na aplikativni sloj OSI modela i zasnovan je na klijent-server arhitekturi. Danas se koristi za komunikaciju između više uređaja iz iste mreže, gde se smatra jednostavnim za postavku i održavanje.

Modbus protokol postao je vrlo popularan usled otvorene prirode protokola i specifikacije. Od 2005. godine razvojem i usavršavanjem Modbus protokola bavi se organizacija Modbus-IDA na koju je preneta sva neophodna nadležnost. Inicijalno je Modbus protokol bio zamišljen za komunikaciju preko asinhrone serijske magistrale, ali je osposobljen i za potrebe lokalnih mreža, posredstvom TCP/IP transportnog sloja.

3.1 FORMAT MODBUS PORUKE

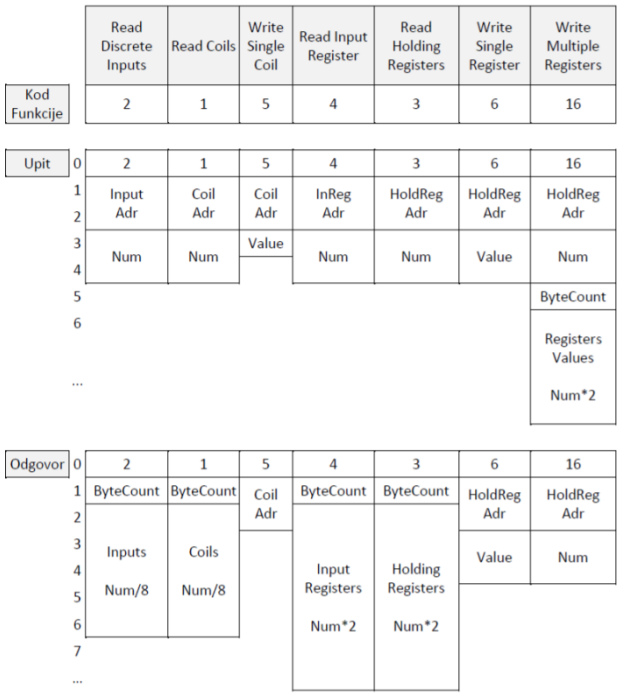
Modbus je tipičan nebalansirani protokol, gde sa ugla akviziciono-upravljačkih sistema: PLC igra ulogu servera (engl. slave) koja na upit SCADA klijenta (engl. master) šalje odgovore u vidu željenih poruka. Opšti format poruke definisan je Modbus protokolom kao aplikativna jedinica podataka (engl. *Application data Unit - ADU*) čije jezgro definiše jednostavan jedinični podatak protokola (engl. *Protocol Data Unit - PDU*) koji je uvek prisutan nezavisno od varijante Modbusa. Na slici 3.1-1 je prikazan sadržaj Modbus ADU-a. [2]

Adresa uređaja može biti u opsegu 1-247, dok je 0 rezervisana za *broadcast* poruke koje prima i obrađuje svaka stanica - bez da šalje povratnu poruku kao odgovor. Master uređaj sa druge strane, po pravilu nema svoju adresu. Kod funkcije je enkodiran u jedan bajt, pa raspolaže opsegom 1-255, gde su vrednosti opsega 128-255 rezervisana za odgovore grešaka. Svrha koda funkcije jeste da pri komunikaciji, master saopšti serveru koju akciju treba da izvrši. Podaci PDU-a, sa druge strane sastoje se od dodatnih informacija koje server koristi pri izvršenju akcije koju diktira kod funkcije.



Slika 3.1-1 Opšta struktura poruke Modbus protokola [2]

Na slici 3.1-2 je predstavljen bazni skup poruka neophodan za uspešnu komunikaciju sa udaljenim uređajem posredstvom Modbus protokola. Vertikalno posmatrano svaki od upita ima odgovarajući odgovor, gde su isti grupisani u PDU jedinice. Poruke se sastoje iz dva glavna dela: koda funkcije i podataka sadržanih u upitu - odnosno odgovoru. Prva 4 bita upita i odgovora su uvek rezervisana za kod funkcije, dok su narednih 16 pri upitima uvek rezervisana za adresu registra (registara) koji je neophodan (su neophodni) za izvršenje akcije. *Read* upiti (funkcije 1, 2,3 i 4) narednih 16 bitova rezervišu za broj registara koje treba pročitati, dok komandni (*write)* zahtevi iste rezervišu za vrednost koju treba upisati. [1]



Slika 3.1-2 Bazni skup Modbus poruka [1]

3.2 MODBUS MODEL PODATAKA

Model podataka je u jezgru svakog protokola. On određuje tipove podataka i aplikativne funkcije koje

protokol podržava. Kao takav on predstavlja spoljnu sliku uređaja koji ga implementira. Sa obzirom da je Modbus dizajniran krajem 1970-ih, u svrhu komunikacije sa PLC-ovima, tipovi podataka kojima barata protokol su ograničeni na one koje su PLC-ovi tada razumeli. [3]

Modbus logički model (po specifikaciji *Modbus Register Map*) podrazumeva četiri grupe registara, dužine 1 ili 16 bita. Oni predstavljaju najvažnije PLC podatke - sa stanovišta SCADA sistema: vrednosti procesnih ulaza/izlaza analognog odnosno digitalnog tipa. Ovi registri su prikazani slikom 3.2-1 gde se vide dozvoljene operacije komandovanja odnosno čitanja svakog od njih.

Oznaka	Dužina	Pristup	Opis
Discrete Outputs (Coils)	1 bit	Read/Write	Digitalni izlazi
Discrete Inputs	1 bit	Read	Digitalni ulazi
Input Registers	16 bit	Read	Analogni ulazi i Brojači
Holding Registers	16 bit	Read/Write	Analogni izlazi

Slika 3.2-1 Modbus model podataka

Format podataka u registrima vidljivim klijentu je binaran, neoznačen i po pravilu - *big endian*. Budući da Modbus usled inicijalnog dizajna predviđa prenos sirovih podataka u praksi potrebno primeniti rešenja koja odstupaju od osnovnog standarda kako bi se preneli 32-bitni integer, float ili string tipovi podataka. Oni se smeštaju korišćenjem dve lokacije u zoni internih registara. Podatak se deli na dva dela od po 16 bita i smešta na dve uzastopne adrese.

3.3 VARIJANTE MODBUS PROTOKOLA

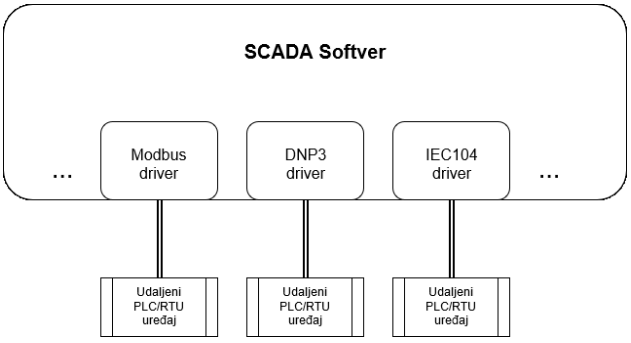
Prva verzija Modbusa bila je dizajnirana kao tekstualni protokol, za rad preko serijskog UART kanala - Modbus ASCII. Tekstualni format nije optimalan spram vremena prenosa i dužine poruke, pa je zamenjen binarnom verzijom koja je i dan danas aktuelna - Modbus RTU. Ova varijanta protokola je orijentisana ka telemetrijskim sistemima i RTU kontrolerima. Obe verzije protokola imaju istu logičku strukturu poruke, ali razlikuju se po pitanju kodiranja sadržaja (ASCII ili binarno).

Kodiranje Modbus ASCII podataka pri prenosu se svodi na slanje dva ASCII znaka, od kojih svaki predstavlja jednu heksadecimalnu cifru (0..9, A..F). Prednost ASCII formata se ogleda u tome da postoji mogućnost vizuelne kontrole, što je nekada bilo od koristi u praksi. Modbus ASCII poruka započinje znakom :, a završava slanjem CRLF sekvence (engl. *carriage return-line feed*). RTU varijanta protokola binarnim kodiranjem svodi poruku na minimalan obim podataka kako bi ostvario maksimalnu efikasnost pri brzini prenosa podataka preko sporih analognih modemskih veza brzine 600 - 2400 bit/s. Obe varijante Modbus protokola definišu poruke koje završavaju redundantnom proverom - mehanizmom kojim se utvrđuje ispravnost prenetog sadržaja.

Modbus TCP je mrežna varijanta Modbus protokola. Slično Modbus RTU varijanti - koristi binarno kodiranje podataka, ali i TCP/IP mehanizam za pouzdan prenos poruka u okviru mreže. Modbus TCP je konekcijski orijentisan protokol, što znači da su moguće istovremene veze sa više slave uređaja (ili više veza sa istim uređajem). Slično RTU varijanti: TCP/IP *Timeout* je karakteristika TCP verzije protokola koja definiše vreme u slučaju neuspešnog prenosa, nakon kojeg se veza zatvara i ponovo otvara u cilju uspešnog nastavka komunikacije. Budući da ova varijanta protokola uvodi mogućnost komunikacije sa više servera, potrebno je voditi računa o integritetu upravljačkog sistema. [2]

4. KONCEPT REŠENJA

Implementacija Modbus protokola u SCADA sistem podrazumeva realizaciju softverske podrške komunikacionog podsistema, u cilju komunikacije sa udaljenim uređajima posredstvom Modbus protokola. Programsko rešenje opisano u ovom radu nastoji da zadovolji karakteristike modernog SCADA sistema, pa je od izrazite važnosti osmisliti adekvatnu arhitekturu softverske podrške. SCADA softver jednog modernog SCADA sistema uslove generičnosti i skalabilnosti zadovoljava programskim komponentama koje se najčešće nazivaju rukovaocima (engl. *driver*). Ideja je da svaka rukovaoc komponenta ima odgovornost upravljanja perifernim jedinicama, prenosa poruka konstrukcije paketa i obrade grešaka - gde svaki od njih komunicira sa udaljenim uređajima po unapred definisanom protokolu (slika 4-1).



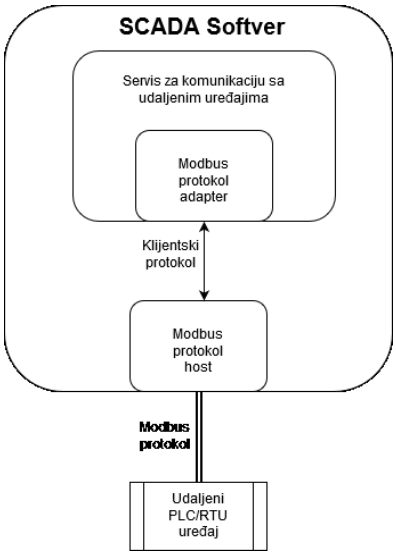
Slika 4-1 Generičnost rešenja

Predloženo rešenje se konceptualno sastoji od dve ključne komponente: servis za komunikaciju sa udaljenim uređajima i Modbus protokol host. Servis za komunikaciju da udaljenim uređajima je nezavisan od konkretnog protokola komunikacije i kao takav sadrži Modbus protokol adapter koji servisu omogućuje komunikaciju sa Modbus protokol hostom. Protokol host se direktno povezuje sa udaljenim uređajima sa kojima i komunicira putem Modbus protokola. Protokol host i protokol adapter komponente su zamišljene kao servisi koji komuniciraju putem nekog klijentskog protokola što istovremeno omogućava podizanje Modbus protokol hosta na različitom računaru. Arhitektura ovog koncepta je prikazana slikom 4-2.

Servis za komunikaciju sa udaljenim uređajima korisniku omogućava da preko konzole izda naredbe, odnosno očita vrednosti sa udaljenog uređaja nezavisno od industrijskog protokola na jedinstven i konzistentan način. Pored toga što komunicira sa modulom korisničkog interfejsa sa jedne strane, ovaj servis sa druge strane posredstvom odgovarajućeg adaptera obezbeđuje komunikaciju sa protokol hostovima. Servis iz biblioteke adaptera dobavlja Modbus protokol adapter, koji ostvaruje komunikacionu spregu sa Modbus protokol host-om. Dve ključne komponente ovog modula jesu Akviziciono-upravljački servis i Dispečer zahteva. Posredstvom ovih komponenti

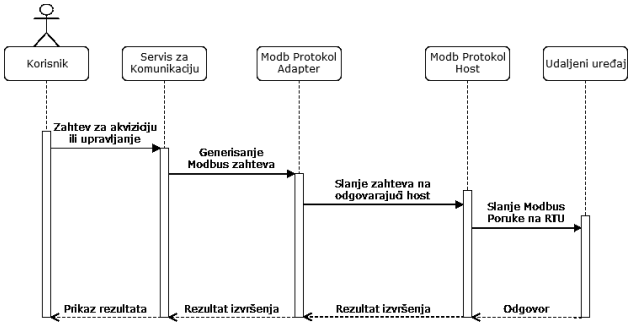
ostvaruje se generisanje zahteva za akviziciju, odnosno generisanje komandi - spram prethodno učitane konfiguracije i dospelog ulaza sa korisničkog interfejsa.

Modbus protokol host je komponenta koja direktno komunicira sa udaljenim uređajima po Modbus protokolu. Broj senzora i aktuatora na udaljenim uređajima potencijalno može biti velik sa porastom samih uređaja u sistemu. To znači da komunikacioni podsistem potencijalno mora da podrži prenos izrazito velikog broja poruka u određenom trenutku, pa je potrebno da SCADA softver omogući konkretnom protokol adapteru komunikaciju sa više protokol hostova kako bi se izbeglo zagušenje komunikacije. Teoretski, predloženo rešenje ima mogućnost skalabilnosti po pitanju broja protokol hostova, ali je zarad jednostavnosti realizovan i opisan samo jedan Modbus protokol host kako bi se sagledala suština te komponente.



Slika 4-2 Arhitektura rešenja

Na slici 4-3 prikazana je razmena poruka između prethodno opisanih komponenti u slučaju akvizicije odnosno upravljanja udaljenim uređajem.



Slika 4-3 – Tok komunikacije pri akviziciono-upravljačkom procesu

5. IMPLEMENTACIJA REŠENJA

Programsko rešenje razvijeno je u programskom jeziku *C#*, pomoću *Microsoft*-ovog *Visual Studio 2015* razvojnog okruženja. Korišćen je *.NET 4.6.2 framework* pri razvoju rukovaoca, a za potrebe komunikacije je simuliran RTU uređaj pomoću Modbus PLC Simulatora [4].

Pokretanjem procesa Servisa za komunikaciju, korisniku će se prikazati upravljačka konzola gde je moguće izdati neku od mogućih naredbi akvizicije odnosno upravljanja. Pri pokretanju servisa vrši se konfiguracija modela podataka SCADA sistema. Po izdavanju zahteva za akviziciju, odnosno upravljanje – proces se oslanja na model podataka sistema kako bi odredio o kojem protokolu je reč, u svrhu dobavljanja adekvatnog Protokol Adaptera. Adapter komponenta je pomoću MEF (engl. *Managed Extensibility Framework*) tehnologije enkapsulirana i izmeštena u zasebnu biblioteku u svrhu postizanja modularnosti. Izdati zahtev se prenosi ka Modbus Protokol Hostu, koji na osnovu njega kreira odgovarajuću Modbus poruku kako bi iskomunicirao zahtev sa simulatorom. Simulator vraća odgovor i odgovarajuće podatke koji se nakon ažuriranja u *Redis* in-memory bazi podataka Protokol Hosta šalju nazad ka servisu za komunikaciju. Korisnik spram prikaza na konzoli nije svestan detalja komunikacije, te bi prikaz bio isti u slučaju implementacije nekog drugog protokola i simulatora. Servis za upravljanje sa udaljenim uređajem i protokol host realizovani međusobno komuniciraju posredstvom WCF (engl. *Windows Communication Foundation*) tehnologije. Modbus PLC Simulator je javno dostupan simulator PLC uređaja koji podržava RTU i TCP varijante Modbus komunikacije. Iskorišćen je u svrhu simulacije udaljenog uređaja sa Modbus protokol host komponentom, kako bi se adekvatno sagledala funkcionalnost programskog rešenja.

7. ZAKLJUČAK

Tematika problema implementacije Modbus protokola u SCADA sistem je dovoljno kompleksna, a rešenje dovoljno jednostavno da se dočara jasna slika o detaljima problema uvođenja protokola komunikacije u jedan ovakav sistem. Rešenje podrazumeva slanje zahteva za akviziciju i upravljanje nad pojedinačnim tačkama Modbus PLC simulatora. Arhitekturalno, rešenje je zamišljeno sa idejom proširivosti, tako da bi eventualan dalji pravac razvoja pokrio preostale Modbus funkcije koje je teoretski moguće izvršiti nad udaljenim uređajem. Takođe, moguće su izmene na postojećoj arhitekturi u cilju uvođenja manuelnog konfigurisanja sistema, izmeštanja konzolne aplikacije u zaseban WCF servis, kao i poboljšanje performansi komunikacionih kanala u slučaju uvođenja više udaljenih uređaja.

8. LITERATURA

[1] Branislav Atlagić, Softver sa kritičnim odzivom, Fakultet tehničkih nauka, Novi Sad, 2015

[2] MODBUS Application Protocol Specification, Version 1.1b3, 2012

[3] https://en.wikipedia.org/wiki/Modbus

[4] https://sites.google.com/site/plcsimulator/

Kratka biografija:

Igor Tot rođen je 14.05.1993. u Novom Sadu gde je i završio Gimnaziju „Jovan Jovanović Zmaj'' 2012. godine. Upisao je osnovne akademske studije Računarstva i Automatike na Fakultetu Tehničkih Nauka iste godine. Po završetku osnovnih studija, 2017. upisao je master akademske studije Primenjenog Softverskog Inženjerstva na istom fakultetu.