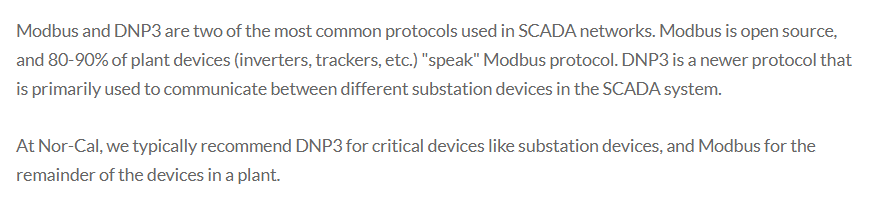
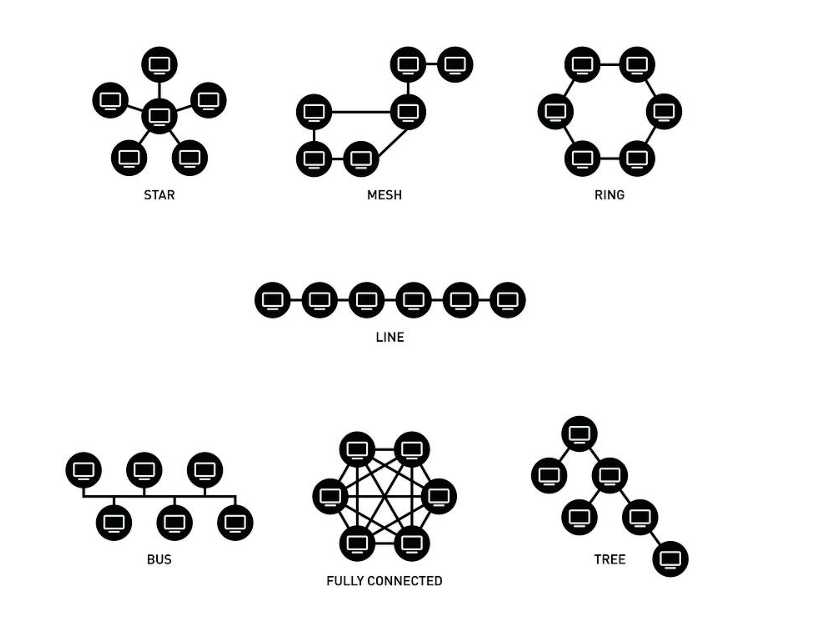
U istraživanju sam saznao da razni SCADA sustavi koriste različite protokole i problem nastaje kada se ti protokoli ne održavaju i ostavljaju zastarjeli. Tada napadači mogu koristiti upravo njih kao vektor napada.



<https://blog.norcalcontrols.net/scada-networking-protocols-and-basics>

u ovom clanku je razradeno kako debuggati ako nesto ne radi u SCADA sustavima od aolikacijskog sloja prema nizim slojevima

takoder su razradene strukture mreze koju SCADA sustavi mogu imati



te je objasnjeno koje su prednosti i nedostatci odredenih odabira

<https://forumautomation.com/t/different-types-of-scada-protocols/4194> (jos detaljnije o protokolima sa objasnjenjima gdje se koristi)

## IEC 60870-5

* IEC 104

## DNP3 Protocol

## Modbus

## MODBUS X

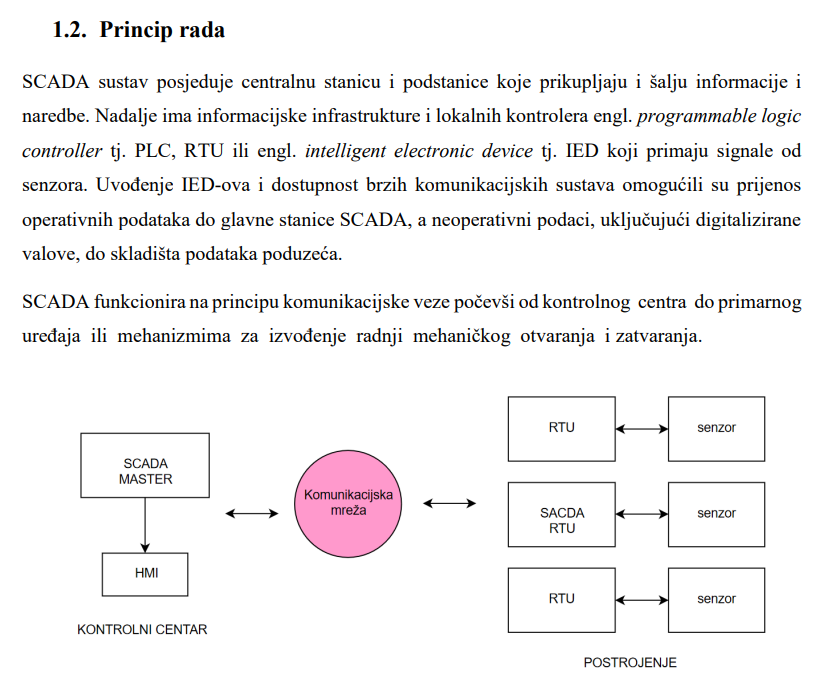
## DNP (Distributed Network Protocol)

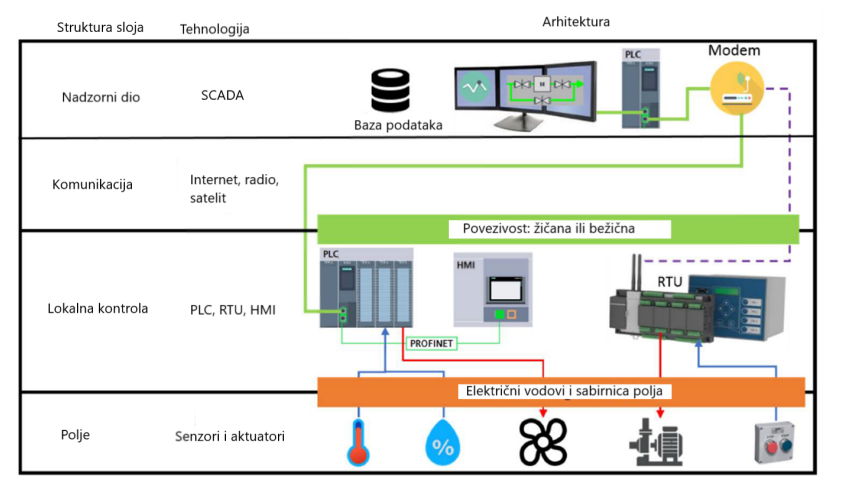
## ASCII

## IEEE 60870

<https://repozitorij.etfos.hr/islandora/object/etfos%3A3520/datastream/PDF/view>

studentski zavrsni rad o SCADA sustavima





skopovska arhitektura jednog scada sustava

Kroz istrazivanje sam takoder saznao da je dobra praksa izolirati mrezu na kojem se vrti SCADA sustav tako da i da se dogodi proboj ne može se toliko brzo prosiriti

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8672892>

zanimljiv clanak u kojem sam saznao da je PCOM protokol lako exploitable i dane su neke ideje što bi napadac mogao uciniti da nade neki propust koji ovaj protokol nudi.

Sljedeće pitanje je koje su prednosti i nedostatci SCADA sustava ( jako dobre informacije o ovome sam pronašao u studentskom zavrsnom radu kojeg sam linkao u ovom dokumentu)

Jedna od najvecih prednosti je da se svi podatci biljeze i to znaci da operator ne mora svaki dan provjeravati je li sve u redu i moze se vracati na prosle dane i sakupljati informacije

takoder se automatizira taj proces gdje se operatora ubavjestava ako neki podatci nisu u skladu s ocekivanjima (to je jako vazno npr. u uklearnim elektranama i drugim proizvodnjama visokog rizika)

neki od nedostataka su

Kako bi se osjetljivi pogoni zastitili moramo dodavati firewall na SCADA sustave

SCADA-ini sustavi su manje pouzdani od distribuiranih sustava upravljanja (eng. DCS) i sustava zasnovanih na programibilnom logičkom kontroleru (eng. PLC) jer se sustavi ažuriraju prilično često kako bi se dodale ili promijenile oznake, mjerne jedinice, skripte, alarmi i sinoptički podatci što znači da se SCADA programi moraju često ponovno pokretati.

Još jedan problem o kojem se mora razmisliti je da SCADA oprema neće vječno trajati. To znači da će proizvođači sustava morati zaustaviti proizvodnju i prestati pružati podršku za takvu opremu kad u rad dođu nove verzije.