Razvoj oddaljene telemetrijske enote na 4G

Marko Udovič[1], Jaka Fritz[1], Igor Steiner[1], Marjan Golob[2]
[1]Inea d.o.o., Stegne 11, 1000 Ljubljana
[2]Univerza v Mariboru, FERI, Koroška cesta 46, 2000 Maribor
marko.udovic@inea.si, jaka.fritz@inea.si, marjan.golob@um.si, igor.steiner@inea.si

Development of a Remote Telemetry Unit on 4G

The purpose of this paper is to present project results of development of a new expansion module – remote telemetry unit (RTU). RTUs provide connectivity of remote field devices (sensors, actuators or PLCs) with the control centre via the 4G mobile network. The LTE communication expansion module uses the IEC 60870-5-104 standard and DNP3 protocols, which are specially adapted for transmitting data between distributed processes.

Main features and implementation benefits of the mentioned telemetry protocols are presented. Basic functionality of the expansion module and different communication possibilities between PLC (Programmable Logic Controller) units, expansion module and remote controlling stations are presented.

The work was carried out in the framework of the GOSTOP programme, which is partially financed by the Republic of Slovenia – Ministry of Education, Science and Sport, and the European Union – European Regional Development Fund.

Kratek pregled prispevka

Cilj prispevka je predstaviti rezultate projekta razvoja novega razširitvenega modula – oddaljene telemetrijske enote (Remote Telemetry Unit - RTU). RTU omogočajo povezljivost oddaljenih naprav (senzorjev, aktuatorjev ali PLK-jev) z nadzornim centrom prek mobilnega omrežja 4G. LTE komunikacijski razširitveni modul uporablja standard IEC 60870-5-104 in protokol DNP3, ki ***s***ta posebej prilagojena za prenos podatkov med porazdeljenimi procesi.

Predstavljene so glavne značilnosti omenjenih protokolov in prednosti njihove uporabe v industriji. Predstavljene so osnovne funkcionalnosti razširitvenega modula in različni načini komunikacije med PLK (Programirljivi Logični Krmilnik) enoto, razširitvenim modulom in nadzornimi sistemi.

Delo je bilo izvedeno v sklopu programa GOSTOP, ki ga delno financirata Republika Slovenija – Ministrstvo za izobraževanje, znanost in šport ter Evropska Unija – Evropski sklad za regionalni razvoj.

1 Uvod

Pri izvedbi sodobnih distribuiranih sistemov vodenja je ključnega pomena učinkovita in zanesljiva izmenjava informacij. Digitalna transformacija sistemov vodenja v smislu paradigme Industrija 4.0 [1] predpostavlja komunikacijske tehnologije kot ključen podporni element sistema vodenja. Pri krajevno porazdeljenih sistemih vodenja, kot so na primer komunalni, energetski in logistični sistemi, imajo pomembno vlogo brezžične komunikacijske tehnologije, kot je omrežje 4G LTE (Long Term Evolution) in prihajajoča tehnologija 5G. V raziskavi [2] avtorji predstavijo stanje na področju uporabe 4G LTE tehnologije v industrijskih aplikacijah s poudarkom na varnem prenosu podatkov. Ključno vlogo pri zagotavljanju varnosti prenosa podatkov imajo protokoli in sistemska programska oprema komunikacijskih modulov. Podjetje INEA ima dolgoletne izkušnje z razvojem strojne in programske opreme industrijskih komunikacijskih modulov, izvedenih kot razširitveni komunikacijski moduli PLK, ali kot samostojne RTU enote. RTU enota je običajno od centralnega sistema vodenja krajevno oddaljeno naprava in opravlja funkcije zajemanja procesnih podatkov preko bodisi fizičnih vhodno-izhodnih signalov ali katerega izmed industrijskih komunikacijskih vodil. Naloga RTU je varen in zanesljiv prenos podatkov od oddaljenega procesa v centralni nadzorni sistem vodenja. Aplikacije in storitve, ki se uporabljajo v centralnih sistemih vodenja za namene vodenja in nadzora procesov so poznane pod imenom SCADA sistemi (Supervisory Control and Data Acquisition). Z razvojem komunikacijskih tehnologij se razvijajo tudi SCADA sistemi. Danes govorimo o četrti generaciji SCADA sistemov, ki temelji na internetnih tehnologijah, kot sta internet stvari (Internet of Things - IoT) in računalniške storitve v oblaku (Cloud Computing) [3]. Skupaj z razvojem SCADA sistemov in komunikacijskih RTU enot so se nenehno razvijali standardi in komunikacijski protokoli.

V nadaljevanju članka so najprej opisane značilnosti protokolov DNP3 in IEC 60870-5. V tretjem poglavju je predstavljena oddaljena telemetrijska enota ME-RTU 4G. V četrtem poglavju pa je predstavljen demonstracijski set, ki je namenjen testiranju in predstavitvi enostavnih aplikacij prenosa podatkov med PLK in ME-RTU enoto, kakor tudi med ME-RTU enoto in SCADA nadzornim sistemom vodenja.

2 Odprti protokoli

Na tržišču nadzornih sistemov sta prisotni dve glavni skupini sistemov: *splošni* (angl. *open*) in *namenski* (angl. *proprietary*). Prvi nadzorni sistemi so bili razviti z uporabo namenskih protokolov s strani podjetij, kot del namenskega sistema, da služijo specifičnemu potrebam določene industrije. Podjetja takrat niso imela druge izbire, saj primerni odprti protokoli takrat še niso obstajali. Glavni problem namenski sistemov sta odvisnost in vezanost na proizvajalca sistema. Ravno zaradi tega problema in splošnega povečanja uporabe nadzornih protokolov, se je pojavila potreba po odprtih protokolih. Iz te potrebe se je razvilo sodelovanje več podjetij in držav. Kljub temu je bil razvoj splošno sprejetih protokolov počasen.

Glavna prednost odprtih protokolov je kompatibilnost. To pomeni, da so sistemi sposobni usklajenosti in združevanja opreme različnih proizvajalcev. To lahko prinese veliko takojšnjih in dolgoročnih koristi [4].

Takojšnje koristi so:

- kompatibilnost več različnih naprav,
- manj potrebnih protokolov za podporo sistema,
- manj stroškov za programsko opremo,
- manj testiranja, vzdrževanja in izobraževanja,
- enostavnejša dokumentacija,
- večja ponudba produktov.

Dolgotrajne koristi:

- enostavna in fleksibilna nadgradnja sistema,
- dolga življenjska doba sistema,
- hitrejša prilagoditev novim tehnologijam,
- večji prihranki pri obratovanju.

Zaradi potrebe po standardnih odprtih SCADA komunikacijskih protokolih, so v preteklih letih organizacije za standardizacijo izvedle več aktivnosti za razvoj le-te. Kot posledica tega sta se v devetdesetih letih oblikovala dva protokola: protokol DNP3 in protokol IEC 60870-5. To sta odprta komunikacijska protokola, ki zagotavljata kompatibilnost med sistemi in trenutno tekmujeta za prevlado na trgu. DNP3 je močno podprt v Severni in Južni Ameriki, Južni Afriki, Aziji in Avstraliji, IEC 60870-5 pa prevladuje v Evropi [4].

2.1 Protokol DNP3

Protokol DNP3 je bil zasnovan specifično za aplikacije SCADA, ki se uporabljajo za nadzor in vodenje procesov. Te aplikacije vključujejo pridobitev informacij in pošiljanje nadzornih ukazov med fizično ločenimi napravami. Protokol DNP3 je namenjen prenosu relativno majhnih paketov podatkov na zanesljiv način v deterministčnem zaporedju. V tem se razlikuje od nekaterih bolj splošnih protokolov, ki so zmožni pošiljanja velikih količin podatkov ampak na način, ki načeloma ni primeren za nadzorne sisteme.

Lastnosti protokola DNP3 [4]:

- zagotavlja časovno sinhronizacijo in dogodke (angl. events) s časovnimi značkami,
- razdeli sporočila v več podatkovnih okvirjev in s tem zagotovi optimalen nadzor napak in hitro komunikacijo,
- dovoljuje istoležno (angl. peer-to-peer) in gospodar-suženj (angl. master-slave) omrežno topologijo,
- pošilja dogodke brez izrecnega ukaza gospodarja,
- poskrbi za varno konfiguracijo in prenos datotek.

Časovna sinhronizacija

Ena od pomembnih funkcionalnosti DNP3 protokola za SCADA aplikacije je, da omogoča časovno označevanje dogodkov. Časovno označevanje dogodkov je možno z ločljivostjo do ene milisekunde. Da se dogodki ujemajo preko celotnega sistema, je potrebno zagotoviti, da se ure v vseh postajah ujemajo z uro gospodarja omrežja. Sinhronizacija ur naprav je izvedena preko pošiljanja časovnega in datumskega objekta. Med samim prenosom časovne sinhronizacije med postajami nastane zakasnitev. Če se teh zakasnitev ne upošteva pri nastavitvi ure, je čas na napravah zamaknjen za vrednost te zakasnitve. Dodatne zakasnitve lahko nastanejo v napravi zaradi procesiranja zahteve. Te dodatne zakasnitve se na podatkovnem sloju meri in odpravi.

2.2 Protokol IEC 60870-5

Protokol IEC 60870-5 je zbirka standardov, izdanih s strani Mednarodne elektrotehniške komisije (angl. International Electrotehnical Commission – IEC). Cilj razvoja teh standardov je zagotoviti odprt telemetrijski protokol za nadzor in prenos podatkov v nadzornih sistemih. Protokol se uporablja predvsem na evropskem območju.

Protokol IEC 60870-5 je strukturiran hierarhično, sestavljen iz šestih delov in dodatnih spremljevalnih standardov. Število 5 nakazuje na del 5 (protokol prenosa) standarda 60870. Protokol se je čez čas postopoma razvijal in izdajal. Glavna spremljevalna standarda sta protokol IEC 60870-5-101 in protokol IEC 60870-5-104, ki definirata dva različna prenosa sporočil [4]:

- protokol IEC 60870-5-101 omogoča serijsko povezavo in ponuja vse potrebne podatkovne objekte v aplikacijskem sloju, potrebne za SCADA komunikacijo,
- protokolu IEC 60870-5-104 je novejša verzija protokola IEC 60870-5-101, kjer je večina spodnjih slojev nadomeščena z naborom komunikacijskih protokolov TCP/IP, ki zagotavljajo prenos podatkovnih enot aplikacijskega sloja modela ISO/OSI (angl. Application Service Data Unit – ASDU).

Slika 1: Oddaljena telemetrijska enota ME-RTU 4G.

Topologija sistema

IEC 60870-5-101 podpira enotočkovno in večtočkovno povezavo, ki prenaša zaporedje bitov preko nizko pasovnih podatkovnih povezav. V protokolu je vzpostavljena hierarhična struktura. V osnovi je pri komunikaciji med dvema napravama ena nadzorna naprava in druga procesna naprava. Iz tega sta definirani dve smeri komuniciranja; smer

vodenja in smer spremljanja. Tako so opazovane vrednosti (na primer analogne vrednosti procesnih veličin) poslane v smeri spremljanja, krmilni ukazi pa v smeri vodenja. Če je postaja sposobna pošiljati opazovane vrednosti in krmilne ukaze, potem naprava deluje v dvojnem načinu.

Časovna sinhronizacija

Tako kot pri protokolu DNP3, tudi protokol IEC 60870-5 podpira časovno označevanje dogodkov. Tudi časovna sinhronizacija poteka podobno kot pri protokolu DNP3.

3 Oddaljena telemetrijska enota ME-RTU 4G

Telemetrijsko enoto ME-RTU, prikazano na sliki 1, razvijajo v podjetju INEA d.o.o. Enota predstavlja oddaljeno zaključno enoto, ki implementira odprte standardne protokole in omogoča povezljivost senzorjev, aktuatorjev, PLK-jev in drugih naprav z nadzornim centrom preko mobilnega omrežja.

Zadnja verzija ME-RTU ima vgrajen 4G LTE komunikacijski modem, ki zagotavlja povezavo med nadzornim centrom in oddaljenim sistemom preko mobilnega omrežja. Uporablja se predvsem kot razširitvena enota za PLK enote podjetja Mitsubishi Electric. Z dodajanjem ME-RTU se razširi funkcionalnost sistema PLK v smislu [5]:

- možnih več načinov povezave na PLK enoto za spremljanje in programiranje (preko lokalnega ali mobilnega omrežja),
- komunikacija s SCADA sistemi preko DNP3 ali IEC 60870-5 komunikacijskih protokolov,
- nadzora preko spletnega uporabniškega vmesnika,
- komunikacije po mobilnem omrežju – za zaščito prenosa podatkov se lahko vzpostavi povezava preko navideznega zasebnega omrežja (angl. Virtual Private Network – VPN),
- SMS sporočanja operaterjem in vzdrževalcem.

Vse te funkcionalnosti močno olajšajo delo operaterjem in vzdrževalcem, ki skrbijo za nadzor in delovanje celotnega sistema. Z integracijo enote ME-RTU pridobijo možnost daljinskega dostopa do PLK in procesa.

3.1 Komunikacija

Nadzorna naprava (SCADA) in PLK enota komunicirata preko TCP/IP omrežja, ki je neodvisno od fizičnega sloja. Naloga ME-RTU razširitvene enote je zagotoviti spremljanje procesnih podatkov in omogočiti možnost programiranja PLK enote. ME-RTU deluje kot komunikacijski prehod, ki zahteve iz nadzorne naprave posreduje PLK enoti, odgovore iz PLK enote pa posreduje nadzorni napravi. Za lažje razumevanje si podrobneje poglejmo kako ME-RTU komunicira s PLK in kako z nadzornim SCADA sistemom.

Komunikacija PLK – ME-RTU

ME-RTU lahko s PLK enotami, odvisno od družine PLK enot, komunicira preko dveh vmesnikov:

- namenski vmesnik ASIC (Application Specific Integrated Circuit),
- Ethernet vmesnik (komunikacija preko vtičnikov).

ASIC vmesnik omogoča izmenjavo podatkov med ME-RTU in FX3 družino PLK enot. S takim načinom komunikacije, je PLK enota dostopna preko programskega orodja za programiranje PLK enot na osebnem računalniku.

Komunikacija med ME-RTU in iQ-F družino PLK enot poteka preko Ethernet vmesnika in temelji na komunikaciji preko vtičnikov. Omenjenim PLK enotam vmesnik omogoča dostop do notranjega vmesnega pomnilnika (angl. Buffer Memory – BFM) ME-RTU enote. Komunikacija preko ASIC vmesnika z iQ-F družino PLK enot je možna z uporabo FX5-CNV-BUS(C) modula za pretvorbo vodila.

Komunikacija ME-RTU – nadzorni sistem

ME-RTU komunicira z nadzornimi sistemi preko:

- Ethernet vmesnika,
- mobilnega omrežja,
- radijskega modema.

Ethernet vmesnik je ob komunikaciji z iQ-F družino PLK namenjen tudi za komunikacijo z nadzornimi napravami, ki lahko komunicirajo z ME-RTU preko DNP3 ali IEC 60870-5-104 komunikacijskega protokola. Za varen prenos podatkov, se lahko vzpostavi VPN povezava.

Mobilni vmesnik omogoča dostop do internetnega omrežja preko GPRS povezave. Za mobilni vmesnik skrbi poseben komunikacijski modem. Preko mobilnega vmesnika lahko nadzorne naprave dostopajo do ME-RTU preko DNP3 ali IEC 60870-5-104 komunikacijskega protokola.

ME-RTU vsebuje tudi USB vhod, na katerega se lahko priključi primeren radio modem. Če modem ni združljiv z USB, se vhod lahko uporabi za priklop serijskega pretvornika. S tem lahko ME-RTU komunicira z nadzornimi napravami preko serijskega vmesnika.

3.2 Shranjevanje in tok podatkov

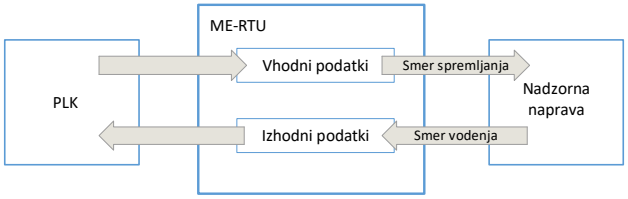
ME-RTU shranjuje podatke v svoji notranji podatkovni bazi. Podatkovna baza shranjuje in spremlja nadzorne podatke, protokolno specifične podatke, časovne značke, itd. Ti podatki se izmenjujejo med nadzorno napravo in PLK enoto. Podatki v bazi so lahko osnovnega tipa ali strukturirani. Struktura notranje podatkovne baze je za uporabnika skrita in direktni dostop do nje onemogočen. Uporabnik lahko dostopa do notranje baze podatkov preko vmesnika medpomnilnika iz PLK enote ali preko protokolnih podatkov (npr. DNP3 podatkovni objekti) iz nadzorne naprave [6].

Podatki so razdeljeni v dve skupini, kot je prikazano na sliki 2 in sicer na:

- vhodne podatke in
- izhodne podatke.

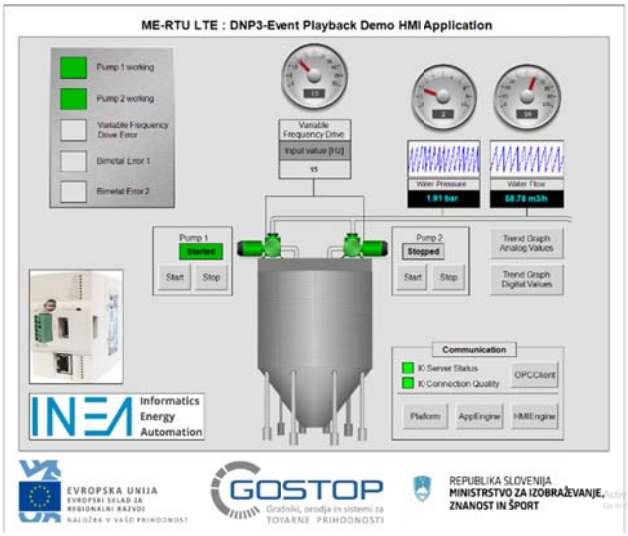
Vhodni podatki predstavljajo podatke iz procesa do nadzorne naprave. Ti podatki so za nadzorno napravo označeni samo za branje. Z vidika telemetrijskega protokola rečemo, da poteka tok vhodnih podatkov v smeri spremljanja (angl. monitoring direction).

Izhodni podatki predstavljajo podatke iz nadzorne naprave do procesa. Ti podatki so za nadzorno napravo označeni samo za pisanje. Z vidika telemetrijskega protokola rečemo, da poteka tok izhodnih podatkov v smeri vodenja (angl. controlling direction).



Slika 2: Pretok podatkov.

ME-RTU ima možnost označevanja vrednosti vhodnih podatkov s časovno značko. Te časovne značke so dostopne samo s strani telemetrijskih protokolov DNP3 in IEC 60870-5. V notranjem medpomnilniku (BFM) pa so prikazani samo trenutni (statični) podatki.



Slika 3: Glavni zaslon SCADA aplikacije za nadzorne sisteme.

3.3 Časovna sinhronizacija

Časovna sinhronizacija ME-RTU se lahko izvede iz treh različnih virov [5]:

- iz PLK enote,
- is strežnika SNTP,
- iz nadzornega sistema (SCADA).

Za pravilno delovanje vseh funkcij, mora biti ME-RTU časovno sinhroniziran. Ena od teh funkcij je samodejno pošiljanje podatkov s časovno značko takoj ob spremembi vrednosti podatka, brez izrecnega ukaza iz nadzorne naprave. Ta funkcija prinese naslednje prednosti:

- nadzorna naprava ne rabi pošiljati zahtev za podatke, oziroma to počne z manjšo frekvenco – s tem se zmanjša obremenitev omrežja in poraba zakupljenih podatkov,
- nadzorna naprava takoj (oz. z zakasnitvijo v omrežju) pridobi informacijo o spremembi vrednosti podatka.

4 Demonstracijske aplikacije

Programske rešitve omenjenih načinov komunikacije med PLK enoto, ME-RTU in nadzornimi sistemi, so prikazane v obliki dveh demonstracijskih aplikacij. V aplikacijah so uporabljeni ME-RTU, PLK enote z razširitvenimi moduli proizvajalca Mitsubishi Electric in programske opreme za SCADA sisteme MAPS (Mitsubishi Adroit Process Suite) in Wonderware InTouch. Demonstracijske aplikacije so dostopne na [7].

V preprostih demonstracijskih aplikacijah so uporabljene kombinacije digitalnih in analognih vhodov ter izhodov. Namenjene so predvsem prikazu načina prenosa podatkov med PLK enoto, ME-RTU in nadzorno napravo za potrebe spremljanja in vodenja procesov.

V prvi aplikaciji je izvedena komunikacija s PLK enoto preko ASIC vmesnika. V drugi aplikaciji je izvedena komunikacija preko Ethernet vmesnika in temelji na komunikaciji preko TCP vtičnikov. V obeh aplikacijah je komunikacija z nadzorno napravo izvedena preko DNP3 protokola. Za prenos podatkov lahko izberemo Ethernet vmesnik ali mobilno omrežje. Za prikaz delovanja sistema smo v SCADA programu izdelali preprost uporabniški vmesnik, prikazan na sliki 3, ki omogoča testiranje sistema.

5 Zaključek

V prispevku smo predstavili rezultate raziskav in razvoj nove oddaljene telemetrijske enote, ki omogoča povezljivost oddaljenih naprav z nadzornim sistemom vodenja preko 4G LTE omrežja. Za končno uporabnost naprave je bistvena pravilna izbira in izvedba odprtih komunikacijskih protokolov, kot sta DNP3 in IEC 60870-5-104. Nova oddaljena telemetrijska enota ME-RTU omogoča komunikacijo med PLK in nadzornim centrom prek mobilnega omrežja LTE, Ethernet povezave, ali USB radijskega modema. Izvedene testne aplikacije so potrdile uporabnost razvitih komunikacijskih pristopov.

Zahvala

Delo je bilo izvedeno v sklopu programa GOSTOP, ki ga delno financirata Republika Slovenija – Ministrstvo za izobraževanje, znanost in šport ter Evropska Unija – Evropski sklad za regionalni razvoj.

6 Literatura

[1] K. Bauer in drugi, MCP - Mobil Controlled Production/5G for Digital Factories, Plattform Industrie 4.0, 2019, Berlin, Nemčija. Dostopno na: https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/mobil-gesteuerte-produktion.pdf?__blob=publicationFile&v=6 (Dostopno: 1.3.2019)

[2] A. Ray, J. Akerberg, M. Bjorkman, R. Blom, M. Gidlund, Applicability of LTE Public Key Infrastructure based device authentication in Industrial Plants, IEEE 39th Annual International Computers, Software & Applications Conference – COMPSAC, Taichung, Taiwan 2015, str. 510–515.

[3] A. Sajid, H. Abbas, K. Saleem, Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges, *IEEE Access*, 4, 2016, str. 1575-1384.

[4] G. R. Clarke, D. Reynders, in E. Wright, *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Oxford ; Boston: Newnes, 2004.

[5] INEA, *Remote Terminal Unit ME-RTU User's Manual*, 3.0.4. Ljubljana, 2018.

[6] J. Dolinar, „RAZVOJ KOMUNIKACIJSKEGA PREHODA S PODPORO MODERNIH PROTOKOLOV ZA SISTEME SCADA“, teza, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, 2016.

[7] „Inea“. [Na spletu]. Dostopno na: http://www.inea.si/telemetrija-in-m2m-produkti/mertu/. [Pridobljeno: 17-mar-2019].