Зборник радова Факултета техничких наука, Нови Сад

UDK: 004.4
DOI: https://doi.org/10.24867/15BE30Vasiljevic

FILE TRANSFER ФУНКЦИОНАЛНОСТ DNP3 ПРОТОКОЛА И ЊЕГОВА ПРИМЕНА У *DSCADA* СОФТВЕРСКОМ СИСТЕМУ

FILE TRANSFER FEATURE OF DNP3 PROTOCOL AND ITS APPLICATION IN *dSCADA SOFTWARE SYSTEM*

Немања Васиљевић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *У овом раду описан је DNP3 протокол и његова конкретна имплементација у dSCADA софтверском систему са нагласком на пренос датотека (File transfer), функционалност коју, као опцију, имају само протоколи новије генерације. У самом стандарду, конкретна примена File transfer-а није специфично описана и дефинисана, што омогућава разноврсну примену ове функционалности у реалном раду. Једна од могућих примена је описана у овом раду, која омогућује упис специфичних догађаја који су се десили у процесном систему и аквизицију истих путем File transfer-а, чиме се омогућује накнадна детаљна анализа тих догађаја.*

Кључне речи: *SCADA, DNP3 протокол, File transfer*

Abstract – *This paper describes DNP3 protocol and their concrete usage in dSCADA software system with accent on File transfer functionality. File transfer is advance functionality supported only by newer generation protocols. Concrete usage of File transfer functionality is not specifically described and defined, which enables various usage of this functionality in real work. One of the usages is described in this paper, and it enables the recording of specific events occurring in the system being monitored, later File-transfer acquisition and detailed post-mortem analysis of recorded events.*

Keywords: *SCADA, DNP3 protocol, File transfer*

1. УВОД

Технолошки напредак у области микроелектронике и информационих технологија, омогућио је убрзани развој система за управљање индустријским процесима и постројењима уз помоћ рачунара. Тако су аутоматизована производна постројења почела да се развијају у раној фази развоја рачунарства, средином шездесетих година, и представљала су електромеханичке системе са рачунарским управљачким језгром. Овакви системи, специфичне намене и структуре у литератури се најчешће означавају термином SCADA (*Suervisory Control And Data Acquisition*) [2].

SCADA системи постали су изузетно важни за већину индустрија широм света јер контролишу критичне инфраструктуре [1] као што су електричне мреже, водоводи, гасоводи…

File transfer је једна од функционалности подржаних у DNP протоколу која омогућава пренос фајлова између SCADA сервера (*master*) и процесног контролера (*slave*).

2. *SCADA*

SCADA (Supervisory Control And Data Acquisition) подразумева надзор, контролу и прикупљање података.

SCADA систем је аквизиционо-управљачки систем. Аквизиција података подразумева добављање вредности са дигиталних и аналогних мерних уређаја из поља. Аквизиција је неизоставан процес у свим SCADA системима јер се све одлуке доносе на основу прикупљених и обрађених података [2].

Појавом дигиталних рачунара створила се могућност да се комплексност система далеко лакше савлада, развојем програма који ће прикупљати мерне податке, моделовати реално стање индустријског постројења и обезбедити квалитетнији надзор и управљање системом.

Традиционални системи су се састојали од једног *PLC-a* који је контролисао индустријско постројење [2]. Временом се јавила потреба за управљањем системима са дистрибуираним ресурсима па је SCADA прерасла у дистрибуирани систем. Данас су SCADA системи присутни у скоро свим критичним инфраструктурама [1].

3. ИНДУСТРИЈСКИ ПРОТОКОЛИ

Индустријски протоколи представљају групу комуникационих протокола за *SCADA* системе. Традиционално индустријски протоколи су често везани за специфичну област примене, још чешће за произвођача опреме [2].

У Америци је доминантан *DNP3* протокол, док су у Европи *IEC 60870-5-101* и *IEC 6087-5-104* [3]. У старијим системима још увек се користе *Modbus, Fieldbus,* као и многи други власнички протоколи [3].

4. DNP3

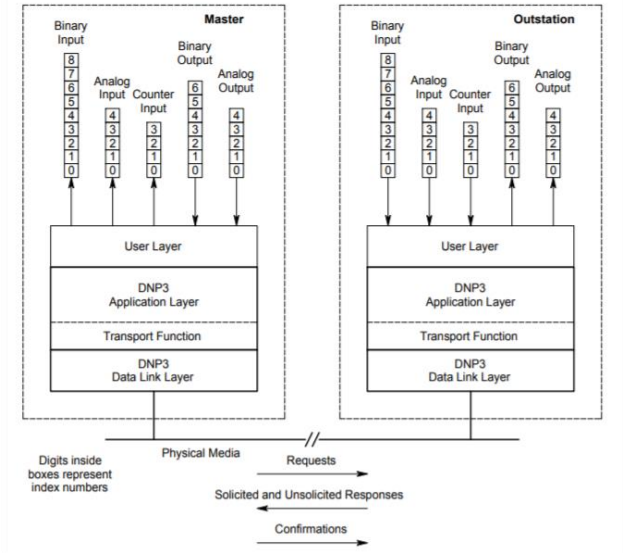
DNP3 (*Distribution Network Protocol*) представља сет комуникационих протокола који се користе за размену информација између компоненти у системима за аутоматизацију процеса. Његова главна

НАПОМЕНА:
овај рад проистекао је из мастер рада чији ментор је био проф. др Драган Кукољ.

улога је у употреби у компанијама које поседују системе као што су системи за дистрибуцију електричне енергије и водоснабдевања. Развијен је за комуникацију између различитих врста опреме за прикупљање и контролу података. Овај протокол игра главну улогу у SCADA системима, где се користи за комуникацију између MASTER станица и RTU-ова и интелигентних електронских уређаја (IDEs).

DNP3 протокол је иницијално настао док су интернет протоколи и сам ISO-OSI скуп протокола био у развоју, када није постојала адекватна мрежна инфраструктура и сам мрежни слој. Зато је изворни DNP3 протокол користио редуковани ISO-OSI модел, такозвани EPA (*Enhanced Performance Architecture*) модел са циљем да се одржи висок степен сигурности у преносу података.

Овај модел се састоји од 3 слоја: апликационог слоја, слоја канала и физичког слоја. Овакав модел комуникације код DNP3 протокола приказан је на слици 4.1.

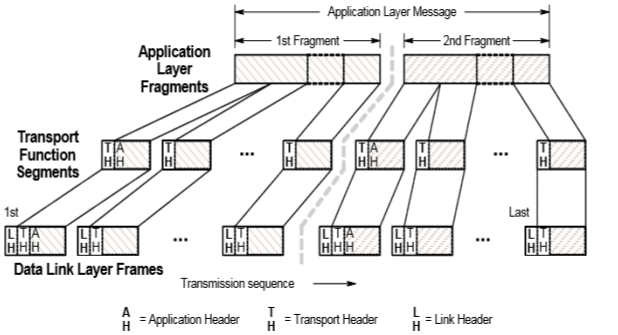


Слика 4.1 Master – Outstation модел комуникације DNP3 протокола

Сваки слој обезбеђује скуп функција које обезбеђују комуникацију са слојем на истом нивоу уређаја са којим се комуницира, при томе ослањајући се на нижи слој у обављању више примитивних функција [4].

4.1 Сегментација поруке

Слика 4.2 приказује фрагментовану поруку апликационог слоја по транспортној функцији, као и енкапсулацију података од апликационог слоја до слоја података. Такође приказује релативне положаје заглавља апликационог слоја, заглавља транспортне функције као и заглавља слоја. Сваки од горе наведених слојева енкапсулира податке добијене од слоја који се налази изнад њега и на добијену поруку лепи заглавље које носи информације које омогућавају правилну обраду поруке на слоју истог нивоа на пријемној страни.

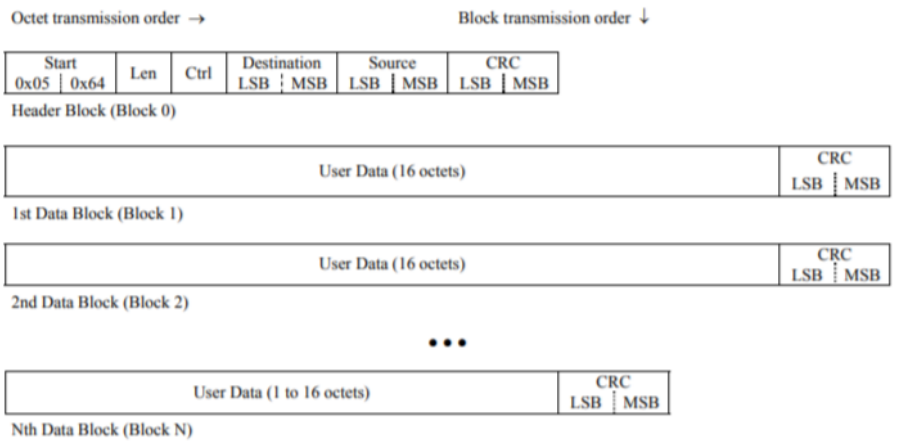


Слика 4.2 *Поступак сегментирања поруке*

4.2 Сегмент слоја података везе (Data Link Layer Frame)

Слој података везе пружа интерфејс између подслоја транспортне функције и апликационог слоја и физичког медија за пренос података или мрежног слоја. Главни допринос фрагмента слоја података је могућност адресирања удаљених станица и могућност откривања грешке. Протокол је дизајниран да делује и у бајтовском режиму рада и у пакетско орјентисаним мрежама где је основна јединица преноса података пакет, као што су *TCP/IP, UDP/IP*.

Оквир везе података има заглавље фиксне дужине, иза кога следе опциони блокови података. Блокови података су дужине 16 бајтова иза сваког блока следи 16-битно поље које садржи CRC код за откривање грешке у преносу података (Слика 4.3).

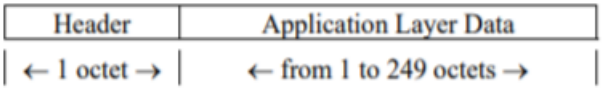


Слика 4.3 *DNP3 формат оквира података*

4.3 Сегмент транспортне функције (Transport Function Segment)

Величина DNP3 фрагмента поруке апликационог нивоа може бити већа од дозвољеног броја октета дозвољеног у једном оквиру слоја везе. Стога сврха транспортне функције је да фрагмент апликационог слоја растави на јединице података (Transport Segments) које су погодне за пренос са предајне стране и на исти начин на пријемној страни састави све пристигле фрагменте у оригиналну поруку.

На месту предаје информације, подаци са апликационог нивоа су растављени на мање делове којима се додаје заглавље транспортне функције (Transport header). Заглавље транспортне функције и подаци са апликационог слоја заједно чине фрагмент података транспортне функције (Слика 4.4), који се прослеђује слоју података.

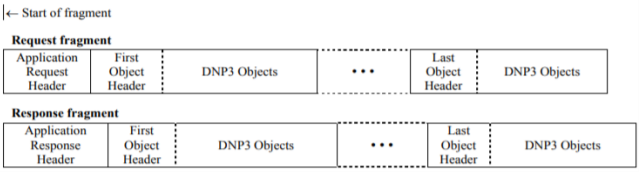


Слика 4.4 Фрагмент података транспортне функције

4.4 Сегмент апликационог слоја (Application Layer Fragment)

Фрагмент је блок узастопних осмобитних вредности (у даљем тексту октета), који садрже информације захтева или одговора који се размењују између мастер стране и удаљене станице.

Сваки фрагмент садржи функцијски код који одређује како ће прималац обрадити пристигли фрагмент, нула или више заглавља података, објекте испуњене подацима као и информације да ли су примљени фрагменти пристигли у одговарајућем редоследу (Слика 4.5). Максимална дужина фрагмента одређује да ли ће порука која се шаље бити послата као један или више фрагмената. Мање поруке могу бити послате као један фрагмент.



Слика 4.5 *Структура фрагмента захтева и одговора*

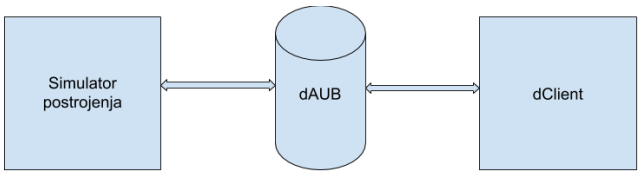
5. dSCADA СОФТВЕРСКИ СИСТЕМ

dSCADA софтвер је програмски пакет школске SCADA-е, који чине три основне компоненте приказане на слици (Слика 5.1):

Симулатор процесног контролера, за потребе развоја DNP3 протокола коришћен је DNP3 симулатор објашњен у претходном поглављу,

Аквизиционо управљачка станица – dAUB,

Клијентска радна станица са графичком спрегом ка оператеру – dClient [2].



Слика 5.1 Компоненте dSCADA апликације

5.1 Клијентска радна станица (dClient)

Клијентска радна станица dClient (оператерска конзола) је апликација која обезбеђује табеларни и графички приказ тренутног стања SCADA система, визуелизацијом оних атрибута процесних величина које су оператеру најинтересантнији.

То значи да многи елементи dSCADA модела нису доступни преко оператерске спреге, јер нису претерано важни у лабораторијској примени или су доступни на неки други начин (кроз развојно окружење).

Поред табеларног приказа, dClient апликација садржи и графички приказ процесног система. Графички приказ се састоји од технолошких дијаграма (шема) процесног система на којима су приказани технолошки елементи постројења. Елементи система повезани са SCADA системом се динамички освежавају, што значи да се њихово стање мења у виду промене боје, додавање текста и променом графичког облика. Остатак дијаграма као технолошка подлога графичког приказа постројења, је непроменљив по иницијалном исцртавању на екрану [2].

5.2 Аквизиционо управљачки блок (dAUB)

Аквизиционо управљачки блок dAUB је централна програмска компонента dScada система која врши функцију SCADA сервера у реалном времену. Иза dAUB апликације стоји слојевита програмска подршка, која прати основне функционалне целине SCADA аквизиционо управљачке станице. Централни део dAUB софтвера представља меморијска база података у реалном времену, која чува променљиве dSCADA модела процеса и све остале структуре података неопходне за рад [2].

5.3 Симулатор постројења (simPLC)

RTU симулатор је програмска компонента, део dSCADA софтверског система чији је задатак да замени физички процесни контролер уз обезбеђење идентичне комуникационе спреге [2].

Суштински задатак SCADA симулатора јесте динамичка симулација окружења SCADA система, тачније процесног окружења које одређује понашање SCADA надзорно управљачке станице [2].

Симулација RTU уређаја има два важна аспекта: симулацију комуникације и симулацију понашања [2].

Симулација комуникације је релативно једнозначан, што не значи и једноставан задатак. Потребно је реализовати RTU станицу неког индустријског протокола, инверзну у односу на протокол који користи SCADA станица.

Стандардно RTU симулатор прима упите SCADA станице, анализира их и шаље адекватне одговоре [2].

Симулација понашања RTU уређаја је, у ствари, симулација постројења иза њега. Промене у постројењу настају као последица одвијања технолошког процеса, или као реакција на управљачке команде SCADA система [2].

6. FILE TRANSFER ФУНКЦИОНАЛНОСТ

File transfer функционалност подразумева пренос комплетних датотека, односно читање и писање датотека између *master* и *slave* станице од почетка датотеке па све до краја.

File transfer увек иницира *master* што подразумева могућност читања и писања фајлова само на удаљеној станици, али не и обратно. У dSCADA софтверском систему имплементирана је функционалност читања фајлова са удаљене станице.

Читање датотека путем DNP3 протокола састоји се од следећих трансакција:

- Опционална аутентификација
- Отварање фајла који читамо
- Један или више захтева за читање фајла
- Затварање фајла

Ако систем захтева кључ за потзврду идентитета за отварање датотеке, мастзер издаје захтев за потврду идентитета.

Отварање датотеке, читање и затварање захтева враћање објекта догађаја од удаљене станице. Ако удаљена станица може одмах да одговори, она враћа одговарајући објекат, у супротнм ако удаљена станица не може одмах да пошаље одговор, она одговара са поруком која не садржи објекте података.

6.1 *Save event* функционалност

Конкретна примена File transfer функционалности није специфично описана и дефинисана, што омогућава разноврсну примену ове функционалности у реалном раду.

Једна од примена која је имплементирана у dSCADA софтверски систем јесте чување специфичних догађаја који су од интереса за перзистенцију у фајл на удаљеној стани. То омогућава прикупљање тих фајлова са свих удаљених станица које надзиремо и њихову детаљну реконструкцију анализу.

Од конкретне имплементације симулатора удаљене станице односно од конфигурације стварног RTU уређаја зависи који догађаји су од интереса да се перзистирају у фајл.

У случају dSCADA система кроз конфигурациони параметар (SAVE_EVENT 1) је могуће омогућити или онемогућити креирање фајла за упис догађаја, као и упис догађаја у исти.

7. ЗАКЉУЧАК

Основна замисао овог рада била је имплементација напредних функционалности DNP3 протокола, међу којима је *File transfer* и њена реална примена. Функционалност је имплементирана и на *master* станици као и на симулатору.

За реализацију рада било је неопходно детаљно упознавање свих функционалности DNP3 протокола, њихову имплементацију, као и упознавање архитектуре dSCADA софтверског система.

За саму имплементацију протокола коришћени су алати *Outstation DNP Simulator* и *Cliet DNP Simulator* као референтни алати за развој, како би поруке које се размењују биле у потпуности у складу са захтевима протокола.

Наставак и унапређење dSCADA софтверског система била би развој алата који би олакшао анализу фајлова са удаљених станица односно анализу забележених догађаја.

8. ЛИТЕРАТУРА

[1] Kyle Coffey, Richard Smith, Leandros Maglaras and Helge Janicke, *Vulnerability Analysis of Network Scanning on SCADA Systems*, 2018

[2] Branislav Atlagić, *Softver sa kritičnim odzivom, projektovanje SCADA sistema*, 2015

[3] Frances Cleveland, *IEC TC57 Security Standards for the Power System's Information Infrastructure – Beyond Simple Encription*, 2006

[4] *Никола Живковић – Једно решење имплементације ДНП3 протокола, 2011*

[5] *DNP_SpecificationDocuments_20100223*

[6] *G.Clarke, D.Reynders, E.Wright, Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems, Elsevier 2004.*

[7] *S.Boyer, SCADA: Supervisory Control and Data Acquisition, ISA, 2009.*

[8] *D.Bailey, E.Wright, Practical SCADA for Industry, Elsevier, Burlington 2003.*

[9] *J.F.Kurose, K.W.Ross, Computer Networking: A Top-Down Approach, Pearson Education, Boston 2010.*

Кратка биографија:

Немања Васиљевић рођен је 1996. године у Ужицу. Завршио је Средњу Техничку школу у Ужицу 2014. године. Исте године уписао је Факултет Техничких наука у Новом Саду. Дипломски рад под називом *Имплементација DNP3 протокола у dSCADA софтвер* одбранио је 2019 године.