International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 06, June-2015

Modelling and Analysis of Non-Critical Request Communication of DNP3 Protocol using Coloured Petri Nets Technique

Bhupendra Amrut Tare
Department of Electrical Engineering
Veermata Jijabai Technological Institute
Mumbai 400 019, INDIA

***Abstract*—Distributed Network Protocol Version 3 (DNP3) is used as Supervisory Control and Data Acquisition System (SCADA) protocol in many of control industries especially oil and gas. As these SCADA networks are continuously connected to internet, their communication becomes more susceptible to cyber-attacks. In order to identify misbehavior in communication one has to model and analyze communication flow. In this paper DNP3 protocol non-critical request communication is properly modeled and analyzed using Coloured Petri Nets (CPN) and associate state space tool. CPN technique will give complete idea to understand communication flow for processing DNP3 non critical request. The state space report and their parameters achieved from tool helps us to analyze behaviour of DNP3 protocol. With this research one can validate protocol performance against communication faults.**

Keywords—Distributed Network Protocol Version3 (DNP3), Supervisory Control and Data Acquisition (SCADA), Coloured Petri Nets (CPN), State Space Report.

I. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems are designed with three sections namely Master stations, Protocols and Outstations to provide reliable solution for control of various industrial services such as power, water, electricity, oil and gas. Master station as hub communicates with other sections and devices by transmitting requests. Protocols are responsible for actual communication between master stations and outstations. It is also termed as supervisory station. Outstation consists of Intelligent Electronics Devices (IED's) and other control devices like relays, alarms to perform operations on requests and provides responses to master station [1].

SCADA systems are continuously connected to internet services so there are more chances of interruption of usual communication flow due to attacks [3], [4]. The survey report of SANS Institute also found risk to SCADA systems [5]. In order to solve these issues one has to analyze performance of system and their protocols [2].

Depending upon industry applications various SCADA protocols are used. This work is mainly on Distributed Network Protocol Version 3 (DNP3) [6], because critical and non-critical operations can be separately processed [7]. The main objective is analysis of DNP3 non-critical request communication which don't challenge authentication from outstation and its wide use in oil, gas and many control industries [6].

Coloured Petri Nets (CPN) Technique [9] is used to prepare executable model for non-critical operation of DNP3 Protocol. This Technique transforms design logic of application into linked model from which actual message and packet formation and transmission through network can be observed. The Coloured Petri Nets and its associate state space tool have been successful in modelling and security analysis of Non- Aggressive challenge response of DNP3 protocol [8] and also achieved desire results in modelling of communication and cryptographic protocols [10]. So, petri net technique is considered as successful technique.

This work focuses mainly on modelling of non-critical request communication of Distributed Network Protocol using CPN technique and its behavioral analysis using state space tool, which will further helps us to find insecure states and identify abnormal behaviour against authenticate flow.

The rest of this paper is structured as follows. Section II gives information about Distributed Network Protocol Version 3 especially non-critical request parameters. Section III presents Coloured Petri Nets technique and implementation plan and Section IV illustrates DNP3 non-critical request formation, modelling and implementation in CPN tool version 4.0.0. Section V will elaborate results and data analysis. Finally, Section VI explains conclusions and future work.

II. DESCRIPTION OF DNP3 PROTOCOL

Distributed Network Protocol version 3 (DNP3) is defined as communication protocol which forms communication link between master stations and outstations devices those are compatible with DNP3 [6]. This protocol supports various topologies like peer to peer communication, multi drop from one master and multi drop from multiple masters. As DNP3 non-critical request is modeled here to achieve communication between master station and outstation peer to peer communication topology is preferred.

International Electro-technical commission (IEC) has confirmed that DNP3 as layered architecture. This architecture consists of three main layers, namely physical

layer, data link layer, application layer. The application layer is high priority section where generation of messages and requests takes place. It also provides linked data objects to users like Human Machine Interface (HMI), Intelligent Electronics Devices (IED's) and Energy Management Systems (EMS) [6].

DNP3 application layer has security mechanism where requests and responses formation are challenged with certain authentication. In this paper our main focus is towards application layer whose security mechanism can be modeled for non-critical request communication. There are two categories with packets can be generated as critical and non-critical requests. Criticality is defined with node or state which is responsible for parameter and set point adjustments included as control operations. Non critical operation is a two way communication where non critical request is sent from master station and relevant standard response is sent from outstation to master station [7].

A. DNP3 Message Parameters

The function code, object header and application control field are three main fields associated with DNP3 requests and responses and internal indicator as one additional field associated with DNP3 responses only [6].

The application control field is used to combine multiple message components. The function code explains actual purpose of message formation. It consists of three commands namely "0x01", "0x02", "0x81" for different operations. The command "0x01" is referred as "Read Function" Command used for non-critical operation. "0x02" command is used as "Write function" command and termed it as critical operation command. The standard response generated at outstation is represented with "0x81" command where criticality is not applicable [8].

The object header fields are incorporated in packet formation to indicate type and format of data in which master station is expecting response from outstation. The commands "g20v1/g20v7" commands are used to represent object headers. If these commands are assigned with non-critical request function codes then outstation should assign feedback in format of "xx|xx|xx". If these commands are assigned with critical request then feedback format should be "gxxx". These token values can be assign to indicate analog and binary outputs at outstation [8].

The field "Internal Indicator" is incorporated while generating responses at outstation to indicate error conditions. The command "00_IIN_1" is used with non-critical function code and "00_IIN_ 2" is used for critical function codes. The final response will consist of function code, object header and status of internal indicator [8].

B. Identification of Non Critical Request

When request from master station is received at outstation, it classifies request as non-critical and critical depending upon commands. If request consists of 1'("0x01", "g20v1") or 1'("0x01", "g20v7") packets then they are consider as non-critical requests. As non-critical request communication do not challenged authentication, requests are directly transmitted and standard response is generated as 1'("0x81", data, I). In this response ("0x81") is indication for response, "data" indicates header and letter "I" shows status for internal indicator. If outstation receives packets with command "0x02" then requests are termed as critical requests. In this paper DNP3 model created in Coloured Petri Nets, elaborates flow of non-critical request operation.

III. CPN METHODOLOGY

CPN [9] is technique used for modelling and analysis of concurrent systems. It is based on Standard Metalanguage Functions (SML). This methodology usually deals with design of petri nets, programming functions and declarations. Petri nets are used to develop states and high level language to declare data types and variables used in model. The state space tool associated with CPN makes user to identify insecure states and to validate behaviour.

Coloured Petri Nets allow user to construct models with combination of places, transitions and directed arcs. Places indicate various nodes in modelling of systems. Transition describes what type of operation is to perform and last directed arcs are used to connect places and transitions or transitions to places. Data objects and variables while modelling are defined with color sets. The color set is the type defined with declaration "color". There are various color sets are used in this application to represent various message fields of non- critical requests. The places used in model can be initialize with data values or set of data values. The values assign to place is called as "Token" and set of values refereed as "Multi-set". The functions written on an arc which connects places to transitions and transitions to places are known as "Arc Inscriptions". The variables used in arc inscriptions must be typed and declared.

After designing model in CPN tool next task is to simulate model for performance verification and further security analysis is achieved from state space report.

A. Block diagram to transfer DNP3 Non Critical Communication in CPN

The objective is to prepare executable model for DNP3 non-critical request operation in CPN tool. The block diagram shown in fig.1 will explains actual logic to understand communication flow from master station to outstation and back to master station again.

1) Master Station: The master station is control center responsible for creation of requests and to receive and display of responses. The requests are formed with token values for function code and object header. The object header data values indicates, type and format in which master station is expecting response. After processing request, responses are received back at master station itself and then at indication, operation gets highlighted.

2) Network: The requests formed at master station are transmitted through network for their operation at outstation. After processing requests responses are transmitted to master station through this network itself.

3) Outstation: The request is received at outstation and identified for non-critical operation with reference to its token value. Depending upon data objects of header respective loop is selected to process non critical operation. Finally, response is generated with token values of three parameters namely function codes, object header and internal indicator and transmitted towards master station.

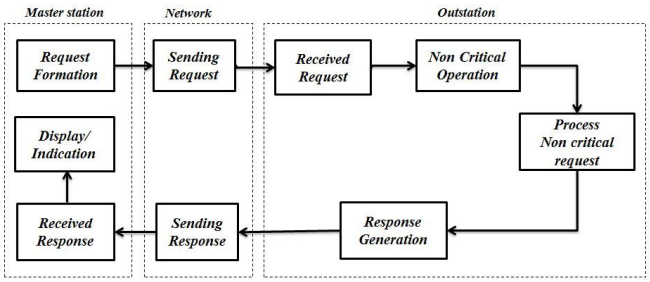

Fig. 1. Block Diagram: DNP3 Non Critical Operation to CPN Flow

The whole creation and modelling is to mimic the performance of DNP3 protocol.

B. Assumptions and Declarations to Model DNP3 Non Critical Operation in CPN

In this section, I highlighted some assumptions and declarations required to create executable model to process non-critical request operation of DNP3 protocol.

1) Assumptions: Master station and outstation are aware of command for non-critical operation. I concentrated only on application layer, all the other layers are considered reliable. Time fragments formation for responses and requests are single fragment.

2) Declarations: A CPN declaration manages DNP3 codes and headers into CPN programming language. The declarations required for modelling non critical operation are shown in fig.2. There are various color sets are defined to represent data types of places used. DNP3 function code and object header are declared with "function" and "object" color sets. The "main" and "data" are two variables are used to assign token values for function code and object header. The status of internal indicator is represented by color set "Indicator". The variable "I" belongs to color set "Indicator" is used for assigning status of indicator in response fragment. The requests formed at master station are defined by color set "Request". Similarly, DNP3 responses are calculated in combination with function codes, headers and internal indicator those are indicated by color set "Response". Color set "common" is used to represent dynamical states like Process, Critical, END while modelling DNP3 non-critical operation.

There are two functions namely "Selection" and "Internal" are used for enabling places for analog and binary outputs and status of internal indicator. According to function token values respective set and place gets enabled. For non-critical operation token values "00 _IIN_1" is selected as indicator status.

```
▼DNP3_NEW.cpn
   Step: 0
   Time: 0
  ▶Options
  ▶History
  ▼Declarations
    ▼DNP3 Declarations
      ▼colset function=string;
      ▼var main:function;
      ▼colset object=string;
      ▼var data:object;
      ▼colset Request=product function*object;
      ▼val Respvalue=("0x81");
      ▼colset Indicator=string;
      ▼var I:Indicator;
      ▼colset Response=product function*object*Indicator;
      ▼colset common= with Process|Critical|END;
      ▼fun Selection(main:function, data:object)=
        let val(ff)=main val(ohh)=data
        in if main="0x01" andalso data="g20v1" then 1`("00|00|01")
        else if main="0x01" andalso data="g20v7"
        then 1`("111101")else empty end;
      ▼fun Internal(main:function)
        =let val(ff)=main
        in if main="0x01" then 1`("00_IIN_1")
        else if main="0x02" then 1`("00_IIN_2") else empty end;
    ▶Standard declarations
  ▶Monitors
   DNP3
```

Fig. 2. CPN Declarations for DNP3 Non Critical Operation

IV. DNP3 NON CRITICAL OPERATION MODEL IN CPN TOOL

The CPN tool Version 4.0.0 is used to model DNP3 non-critical request communication to depict normal behaviour as shown in fig.3. The detail structure and its operation is explained in following sections.

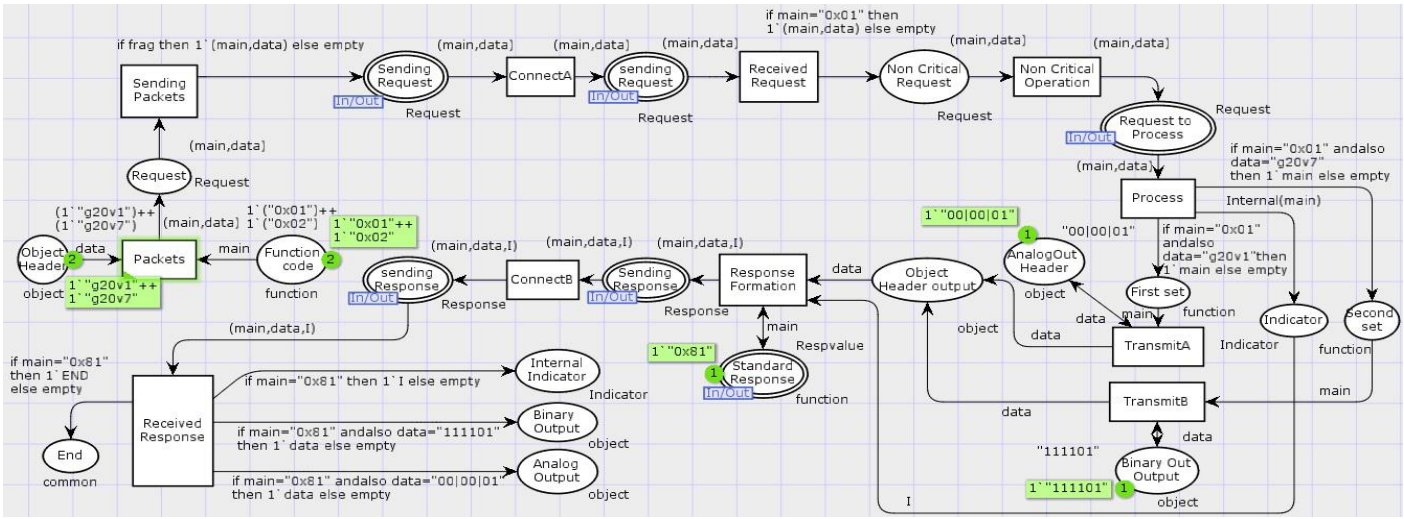

Fig. 3. CPN Model for DNP3 Non Critical Request Operation

A. Design of Model

DNP3 model is designed to process non critical requests operation with flow of packets from master station to outstation. Master station uses three places namely "Function code", "Object Header" and "Request" to create message packets and two transitions namely "Packets" and "Sending Packets" to transmit data packets towards network. The token values 1‘("0x01") and 1‘("0x02") are assigned to function codes. 1‘("g20v1") and 1‘("g20v7") are reference commands and token values used for headers. The requests which are formed with above token values are transmitted through out network in pair of (main, data).

The network section is formulated with "Sending Request" and "Sending Response" places with respective color sets Request and Response. The requests are sent in form of (main, data) and responses are received with (main, data, I) through the network.

The received request section of outstation is modeled with two transitions namely "Received Request" and "Non critical operation" and also one place "Non Critical Request".

The process section at outstation is arranged for two outputs namely "Analog" and "Binary". Depending upon combination of token values two sets are formed for analog and binary operations. These sets are defined with color set "function". 1‘("00|00|01") and 1‘("111101") are markings for analog and binary output header. With received packet combination anyone of the two transitions "TransmitA" and "TransmitB" gets activated to provide object header for final response. One place is also located at process to manage status of internal indicator .At outstation the transition "Response Formation" is used to create standard response with token value 1‘("0x81"). The received response section of master station is design with four places namely "Analog Output", "Binary Output", "Internal Indicator" and "End" for final indication and one transition "Received Response".

B. Operation

Considering the communication link for operation in fig. 3, the first step is to create requests at master station. These requests are created at "Packets" transition with token values of codes and headers. The set (main, data) is form of packet represents token values of both fields. These requests are transmitted through network after enabling transition "Sending Packets". After receiving at outstation non critical request with token values 1‘("0x01") is identified because arc is in-scripted in way for non-critical token value. Now this request with respective data object is further pass to non-critical operation at process end of outstation.

In next step, Place "Request to Process" gets activated to transmit request for processing non critical request. As object header has two token values 1‘("g20v1") and 1‘("g20v7") so with one non critical token 1‘("0x01") two sets are possible. Depending upon packet received at place "Process" respective arc inscription gets enabled to fire their relevant transition. The transition TransmitA gets enabled for analog output header with request 1‘("0x01", "g20v1"). The transition TransmitB gets enabled for binary output header with request 1‘("0x01","g20v7"). While processing non critical request, function "Internal" assigns value ("00_ IIN_ 1") with variable I as status of internal indicator. The place "Object Header output" is used to provide data object marking for selected set by enabling transition either for analog and binary output.

Further , outstation response is created with standard response token value 1‘("0x81"), status of object header ("data") and internal indicator ("I").The transition "Response Formation" gets fired with response (main, data ,I). It is then passed over network to received response section of master station at place "Received Response" where token values for respective object header gets highlighted by enabling respective place node and arc inscription. Three separate places namely 'Internal Indicator", "Binary output" and "Analog output" used to represent final marking status. The place "END" with "common" color set gets activated only for

data value 1‘(‘0x81”), that means standard response is received at station. Thus above operation gives complete link of communication from master station to outstation.

V. RESULTS AND DATA ANALYSIS

In this section, results and data analysis of state space report for CPN model of DNP3 non critical request are described. With this work we had verified the performance of DNP3 protocol for non-critical communication. The state space report terminologies listed in Table. I and their interconnection explain normal behaviour of DNP3 non critical operation.

TABLE I. STATE SPACE REPORT

State Space Nodes	118
State Space Arcs	230
SSC Graph Nodes	118
SSC Graph Arcs	230
Home Markings	None
Dead markings	3
Dead Transitions	None
Live Transitions	None

Table I show state space report analysis of CPN model (fig.3) of DNP3. The State space nodes and state space arcs are terminologies related to number of states or nodes and directed arcs used for operation of CPN model. Strongly connected components (SCC) graph nodes, arcs are used to check reachable states. SSC node can be defined as node reachable from every other node [9]. As state space nodes data matches with SCC graph nodes and report values of state space arcs and SCC graph arcs are same, means every state or node in system is reachable from at least one other node or state. And also indicates that no loops are present in model. Home markings status helps to check finite operation means whether communication is entering in infinite loop or not. As no any home markings are observed, our model has termination point and it is not entering into infinite loop.

Further analysis is performed with dead markings and dead transitions status in report. Dead markings represents markings in the model which does not contain token. Dead transitions are defined as, the transitions from which no path can be drawn from reachable state in model. Live transitions are defined as, transition with which we can find occurrence sequence from any path of reachable state in model [9]. As dead and live transitions are null, each transition is getting triggered at least once during operation. The close inspection of state space report concludes that dead markings observed were expected and with home markings status as none our operation flow is terminating well as expected.

The designed model is simulated using single step debugging in CPN tool to observe actual packet formation and transmission through each node. While simulating no any errors are observed. From above data analysis, normal behaviour of non-critical request operation is achieved. As data values for state space and SCC graph nodes and arcs makes every node reachable. Home markings give final location and as all transitions are getting enabled means no communication fault with none insecure states. If there is any insecure state means abnormal behaviour that can be identified with decrease in state space and SCC graph nodes and arcs as well dead markings. The list of dead transition is also generated while misbehavior or else communication get interrupted in between.

VI. CONCLUSION AND FUTURE WORK

I presented that CPN methodology with its design constraints and programming technique can be used to model and implement non critical request communication of DNP3 protocol. Data packets formation and transmission is observed
by simulating model in CPN tool version 4.0.0. With associated state space tool, I concluded about performance analysis of DNP3 with parameters involved in generated state space report. As while simulating no any errors and communication faults are observed and also normal and expected operation is supported by data analysis. we can conclude that non critical requests are processed well as per demand of master station and responses are indicated at received response section.

The work which combines non-critical request operation with critical indication using CPN technique is in progress. I am also planning to represent normal and abnormal behaviour of DNP3 protocol graphically using “Probability Distribution Functions”(PDF). Data required to present PDF is collected by performing various experiments with initial CPN model of DNP3 and generated state space report. The future work also involves modelling of DNP3 critical request, formation and transmission with Hash Message Authentication Code (HMAC) generation to complete the operation.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of Center of Excellence in Complex and Non-Linear Dynamical Systems (CoE-CNDS), VJTI, Mumbai, India for providing research facilities.

REFERENCES

[1] K. Stouffer, J. Falco, and K. Scarfone, “Guide to Industrial Control Systems (ICS) Security,” NIST Special Publication, vol. 800, p. 82, 2008.

[2] Brian Prince, “U.S. Critical Infrastructure Cyber attack Reports Jump Dramatically,” Published Article on Dark Reading,Available at http://www.darkreading.com/attacks-breaches/us-critical-infrastructurecyberattack-r/240003029 [Retrived on 11th March 2014].

[3] V. M. Igure, S. A. Laughter, and R. D. Williams, “Security issues in SCADA networks, ” Computers and Security, vol. 25, no. 7, pp. 498506, 2006.

[4] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, “SCADA security in the light of Cyber-Warfare,” Computers and Security, vol. 31, no. 4, pp. 418436, June 2012. [Online]. Available:http://dx.doi.org/10.1016/j.cose.2012.02.009;http://www.sciencedirect.com/science/article/pii/S0167404812000429.

[5] Matthew E. Luallen, “SANS SCADA and Process Control Security Survey,” Available at https://www.sans.org/reading-room/ analysts. ../sanssurvey-scada-2013.

[6] "IEEE Standard for Electric Power Systems Communications-DistributedNetwork Protocol (DNP3)," IEEE Std 1815-2012, no. 1815-2012(Revision of 1815-2010), pp. 1866, 2012.

[7] G. Gilchrist, "Secure authentication for DNP3," in Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, IEEE, 2008, pp. 13.

[8] R.Amoah,S.Suriadi,S.Camtepe,E.Foo, "Security analysis of Non-Aggressive Challenge Response of the DNP3 Protocol using CPN Mode," In IEEE International Conference on Communications(ICC 2014) , 10-14 June 2014, Sydney, NSW.

[9] K. Jensen, L. Kristensen, and L. Wells, "Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems," International Journal on Software Tools for Technology Transfer (STTT),vol. 9, no. 3, pp. 213254, 2007.

[10] I. A1-Azzoni, D. G. Down, and R. Khedri "Modeling and Verification of Cryptographic Protocols using Coloured Petri Nets and Design/CPN," Nordic Journal of Computing, vol. 12, no. 3, p. 201, 2005.