

# آيَةٌ

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

وَلَوْلَا فَضْلُ اللَّهِ عَلَيْكَ وَرَحْمَتُهُ لَهَمَتْ طَائِفَةٌ مِّنْهُمْ أَنْ يُضْلِلُوكَ وَمَا  
يُضْلُلُونَ إِلَّا أَنفُسَهُمْ وَمَا يَضُرُّونَكَ مِنْ شَيْءٍ وَأَنَزَلَ اللَّهُ عَلَيْكَ  
الْكِتَابَ وَالْحِكْمَةَ وَعَلِمَكَ مَا لَمْ تَكُنْ تَعْلَمُ وَكَانَ فَضْلُ اللَّهِ عَلَيْكَ  
عَظِيمًا

صدق الله العظيم

سورة النساء

الآية 113

# DADICATION

To my dear mother, I am still remembering all you did for us since my father passed away.

Abdullah

2008

## ACKNOWLEDGEMENT

I would like to express my appreciation to Assoc.Prof.Abdalla Salih Ali, University of Karary for his supervision and guidance through the research period, and to Eng.Tarig Khalifa Gaffar co-supervisor for his continuous efforts so as to fulfill the technical requirements of this research, and finally my best wishes to the center for technical and engineering studies (CETS) and all the staff

# ABSTRACT

In the last few decades, a new market appears as new horizon in the industrial field, “Automation” Understanding this subject is based on the data communication and related subjects, understanding Supervisory Control and Data Acquisition (SCADA) as an automation system need good knowledge of protocols that used for data exchange between different system terminals. Unfortunately SCADA protocols are so complex and need analytical mind to evaluate system performance, system behavior beside error handling .It is also difficult to answer the question of “which SCADA protocol to choose for a specific SCADA system”. In this research an analytical approach was employed to answer the most common questions regarding this subject where two dominant SCADA protocols are analyzed as master-to-substation protocol and one famous remote terminal unit (RTU)-intelligent electronic device (IED) protocol as an example. The researcher found that each protocol has an advantages and weak points for example at the time that DNP3 has more data objects IEC101 has more addressing capability, while DNP3 has more efficient security but the price is using about 11% of the link frame for security, at the same time IEC has less security method for only 0.4% of the total frame length. Information object addressing was also different between DNP3 and IEC101, while IEC101 uses an application level address, DNP3 do not, but this point makes analysis of DNP3 message difficult task, in practice this is a weak point.

It was obvious that field bus protocol (MODBUS) requires only little group of data object.

## المستخلص

# TABLE OF CONTENTS

آية قرانية	i	
Dedication	ii	
Acknowledgement	iii	
Abstract	iv	
المستخلص	v	
Table of contents	vi	
List of tables	viii	
List of figures	x	
List of abbreviations	xii	
<b>Chapter one: Introduction to SCADA</b>		
1.1	Introduction to SCADA systems	1
1.2	Problem statement	1
1.3	Research objectives	1
1.4	Research methodology	1
1.5	Expected results	1
1.6	How this thesis organized	2
<b>Chapter two: Background.</b>		
2.1	Background	3
2.2	Evolution of SCADA systems	4
2.3	SCADA components	8
<b>Chapter three: SCADA protocols.</b>		
3.1	Open System Interconnection(OSI) and SCADA protocols.	11
3.1.1	OSI reference model	11
3.1.2	SCADA protocols	15
3.2	IEC60870-5-101 standard.	15
3.2.1	IEC60870-5-101(IEC101) protocol	17
3.2.2	IEC60870-5-104 protocol.	43
3.2.3	Similarities and differences between IEC101 and IEC104	48
3.2.4	Distributed Network Protocol(DNP3)	49
3.2.5	DNP3 data link layer frame format	53
3.2.6	DNP3 network operation	72

3.2.7	DNP3 subset level	74
3.2.8	Field bus protocols	74
3.2.9	Exception response	82
<b>Chapter four :Comparison between IEC101,DNP3 and MODBUS</b>		
4.1	Comparison between IEC101,DNP3and MODBUS	83
<b>Chapter five: Conclusions and recommendations</b>		
5.1	Conclusions	88
5.2	Recommendations	89
	References	90
	Appendix A	91
	Appendix B	95

## LIST OF TABLES

Table NO	Table title	PAGE NO
3.1	Main parts of IEC60870-5 standard	16
3.2	Selection of IEC60870-5	17
3.3	Companion Standards of IEC60870-5	17
3.4	function code for primary station	27
3.5	function codes for secondary station	28
3.6	control field bits of the balanced mode	32
3.7	7function codes from primary station	33
3.8	function code of the secondary station	33
3.9	IEC60870-5 data link frame format	34
3.10	type of codes of IEC60870-5-101	36
3.11	code reference defined by IEC60870-5-101	37
3.12	Standard causes of transmission.	40
3.13	SDU s used with global address	41
3.14	Structure of the information object	42
3.15	DNP3 request functions	59
3.16	DNP3 control functions	60
3.17	Freeze function	60
3.18	DNP3 Application control functions	61
3.19	configuration functions	61
3.20	Time synchronization functions	61
3.21	File functions	62
3.22	response functions	62
3.23	DNP3 data object groups.	65
3.24	index cod	66
3.25	DNP3 Qualifier codes	67
3.26	MODBUS architecture	74
3.27	MODBUS data types	78
3.28	Exception codes	81
4.1	Comparison of IEC60870-5-101,DNP3 and MODBUS.	86

5.1	Types of monitoring direction	91
5.2	ASDU type process information in monitoring direction	92
5.3	ASDU types process information in control direction	93
5.4	ASDU types–system information in control direction	93
5.5	parameters in control direction	94
5.6	ASDU types – file transfer	94
5.7	binary input object	95
5.8	BINARY OUTPUT OBJECT	95
5.9	counter object	96
5.10	frozen counters	96
5.11	FROZEN EVENT	97
5.12	Analog input object	98
5.13	analog output object	100
5.14	time object	100
5.15	class object	101
5.16	file object/device object	101
Table 4.1	Comparison of IEC60870-5-101, DNP3 and MODBUS	86

# LIST OF FIGURES

<b>Figure NO</b>	<b>Figure Title</b>	<b>Page no</b>
<b>2.1</b>	Sensor to panel SCADA system	5
<b>2.2</b>	PLC/DCS SCADA	7
<b>2.3</b>	Modern SCADA	8
<b>2.4</b>	Typical SCADA system architecture	10
<b>3.1</b>	OSI reference model layers	11
<b>3.2</b>	Encapsulation process	14
<b>3.3</b>	EPA model	18
<b>3.4</b>	DTE-DCE interface	19
<b>3.5</b>	system topologies	20
<b>3.6</b>	variable, fixed length and single Octet frame.	21
<b>3.7A</b>	frame format for IEC101 type FT1.2	22
<b>3.7B.</b>	Physical channel format.	22
<b>3.8</b>	Primary/secondary/dual mode stations	23
<b>3.9</b>	Balanced and unbalanced communication	24
<b>3.10</b>	Unbalanced control field (primary/secondary functions)	26
<b>3.11</b>	Frame header of IEC101	29
<b>3.12</b>	Balanced control field (primary/secondary functions)	31
<b>3.13</b>	ASDU frame details for IEC60 870-5-101	35
<b>3.14</b>	Variable structure qualifier	38
<b>3.15</b>	Cause of transmission octet.	39
<b>3.16</b>	Single and double octets common address of ASDU	41
<b>3.17</b>	The networked version of the IEC60870-5-101(IEC104)	44
<b>3.18</b>	IEC104 interfaces to LAN and WAN equipments	45
<b>3.19</b>	IEC104 telegram with variable length	46
<b>3.20</b>	Information(I) format	47
<b>3.21</b>	supervisory (s) format	47
<b>3.22</b>	Unnumbered (U) format	48
<b>3.23</b>	DNP3 network topologies	50

3.24	DNP3 architecture	51
3.25	DNP3 data link header	52
3.26	DNP3 transport header	52
3.27	DNP3 application header	53
3.28	DNP3 data link frame structure	54
3.29	DNP3 message buildup	55
3.30	DNP3 control byte	56
3.31	DNP3 transport sequence	58
3.32	DNP3 application message sequence(balanced)	63
3.33	DNP3 application message sequence(unbalanced)	63
3.34	Unsolicited response message	64
3.35	DNP3 object header	65
3.36	DNP3 network operation	72
3.37	MODBUS addressing	75
3.38	MODBUS frame	75
3.39	Bit sequence in RTU mode with and without parity bit	76
3.40	RTU mode message frame	77
3.41	Bit sequence in ASCII mode with and without parity bit	77
3.42	ASCII mode message frame	78
3.43	Read coil function example	79

## LIST OF ABBRIVIATIONS

SCADA	Supervisory Control and Data Acquisition
RTU	Remote Terminal Unit
IED	Intelligent Electronic Device
DNP3	Distributed Network Protocol
IEC	International Electrotechnic Commision
PLC	Programable Logic Controller
DCS	Distributed Control System
CPU	Central Processing Unit
RAM	Random Access Memory
ROM	Read Only Memory
PID	Proportional-Integral-Derivative controller
PC	Personal Computer
GPS	Glopal Positioning System
HMI	Human Machine Interface
ISO	International Standard Organization
OSI	Open System Interconnection
TCP	Transmission Control Protocol
IP	Internet Protocol
UDP	User Datagram Protocol
FT	Frame Type
DCE	Data Communication
DTE	Data Terminal Equipment
CRC	Cyclic Redundancy Check
FCB	Frame Count Bit
FCV	Frame Count Valid
ACD	Access Demand
DFC	Data Flow Control
RES	Reserved
FC	Function Code
DIR	Direction
ASDU	Application Service Data Unit
SQ	Structure Qualifier

LAN	Local Area Network
WAN	Wide Area Network
APCI	Application Protocol Control Information
APDU	Application Protocol Data Unit
FIR	First
FIN	Final
TSDU	Transport Service Data Unit
TPDU	Transport Protocol Data Unit
LSDU	Link Service Data Unit
AC	Application Control Code
EPA	Enhanced Performance Architecture