

بسم الله الرحمن الرحيم

قال تعالى:

﴿قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا  
إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ  
الْعَلِيمُ الْحَكِيمُ﴾

صدق الله العظيم

[البقرة: 32]

# ***Dedication***

***To my parents***

# ACKNOWLEDGMENT

First, all praise is to Allah, the Almighty, who gave me the strength, and patience to carry out this work.

My gratitude to Sudan University of Science and Technology, and the Electrical Engineering Department, for their support.

Special thanks to Dr. Eisa Bashier my supervisor, for his patient guidance and generous support.

I would like to express my great thanks to National Electricity Corporation (NEC) staff for their support and encouragement, and for sharing the wealth of information that enriched the contents of this research. I would like to thank Technical Education Corporation.

Finally, I would like to express my sincere gratitude to my mother for her continuous moral support, my father for his valuable comments, and for all family members and friends for their concern and encouragement.

# CONTENTS

SUBJECT	Page
الاية	I
DEDICATION	II
ACKNOWLEDGMENT	III
CONTENTS	IV
LIST OF FIGURES	VII
LIST OF TABLES	VIII
ABSTRACT (English)	IX
ABSTRACT (Arabic)	X
NOMENCLATURE	XI
 <b>Chapter one: Introduction and Overview of SCADA System</b>	
1.1 Introduction	1
1.2 Application process	2
1.3 Elements of SCADA system	3
 <b>Chapter Two: Remote Terminal Unit (RTU)</b>	
2.1 General	8
2.2 Communication Interface	10
2.3 Discrete control	12
2.4 Analog control	14
2.5 Pulse control	16

### **Chapter Three: Details and Comparison of SCADA Protocols**

3.1 Introduction	18
3.2 Protocol details	18
3.3 Comparison of IEC 60870-5-101/-103/-104/, DNP3, IEC 60870-6-Tase-2 with IEC 61850	25

### **Chapter Four: Hardware of RTU560**

4.1 Introduction	38
4.2 Hardware view and structure	41
4.3 Configuration type RTU560A	45
4.4 Serial line interface unit 560SLI02	47
4.4.1 CPA and CPB interface	47
4.4.2 CP1 and CP2 interface	47
4.5 Ethernet communication unit 560ETH03	50

### **Chapter five: Software**

5.1 Software view	53
5.2 RTU560 software structure	56
5.2.1 Internal communication (IC)	57
5.2.2 RTU560 system control and time Administration	57
5.2.3 Board control and diagnosis	57
5.2.4 Process Data Processing and I/O Bus Master (PDP)	57
5.2.5 Host Communication Interfaces (HCI)	58
5.2.6 Subordinate Device Communication Interfaces (SCI)	58
5.2.7 Data Base	59
5.2.8 PLC IEC 61131-3	59

5.2.9 MMI interface	59
5.3 I/O Bus Master and RTU560 Bus	60
5.4 Event flow through RTU560	61
5.4.1 SLC-IOM task	63
5.4.2 MPU	63
 <b>Chapter Six: Conclusions and Recommendations</b>	
6.1 Conclusions	64
6.2 Recommendations	64
 <b>Appendix A:</b>	65
 <b>References</b>	69

# LIST OF FIGURES

Subject	Page
Figure 1-1: A typical SCADA System Architecture	4
Figure 1-2: An RTU and its Various Connections	7
Figure 2-1: Signals Receive the RTU	9
Figure 2-2: Signals Leave the RTU	9
Figure 2-3: Expanded Black Box Description of an RTU	11
Figure 2-4: Message to RTU Calling for it to open a two-position Valve	13
Figure 2-5: Routine Reading of First Specified Register Position	13
Figure 2-6: MTU Message Calls for Analog Output Card	15
Figure 2-7: Analog Output Card	16
Figure 3-1: The Three Basic Fields in Binary Message	21
Figure 3-2: The Message Establishment Field has Two Subfields	21
Figure 3-3: Information Field	23
Figure 3-4: Message Terminator Field	24
Figure 4-1: RTU Communication Capabilities in Principle	40
Figure 4-2: RTU560 Hardware Structure in Principle	43
Figure 4-3: RTU560A (Configuration Example).	46
Figure 4-4: Block Diagram Control Unit 560SLI02	48
Figure 4-5: Board Layout 560SLI02	49
Figure 4-6: Block Diagram Control Unit 560ETH03	51
Figure 4-7: Board Layout 560ETH03	52
Figure 5-1: Software Packages of RTU560	55
Figure 5-2: Software Structure	56
Figure 5-3: Dialog RAM Array between SLC and IOC	60
Figure 5-4: Event Flow through RTU560	62

# LIST OF TABLES

Subject	Page
Table (3-1): General issue.	28
Table (3-2): Process data description.	30
Table (3-3): Operational services.	31
Table (3-4): Self description services.	32
Table (3-5): Online configuration.	33
Table (3-6): Offline configuration.	34
Table (3-7): Integration into application.	35
Table (3-8): Architecture and communication stacks.	36
Table (4-1): RTU560 A/C board.	41



# ABSTRACT

In controlling complex and large systems remotely always, there will be two units namely: Master control units and remote control units.

The first one known as master terminal units (MTU) which may be located away from the system under control, while the second unit known as remote terminal units (RTU) connected through I/O channel to the field device using the convenient voltage and current to control the device. The RTU work under the command coming from MTU using same protocols

For controlling the system between the MTU and device, compatibility is a must.

The problem under investigation is to analyze and evaluate how the MTU and device be made compatible through another media, which is RTU560. This device is a converter which combines the two protocols used for successful control.

## الخلاصة

في انظمة التحكم الكبيرة والمعقدة التى يتم التحكم فيها عن بعد هناك وحدتان لسليقتان , وحدة التحكم الرئيسية و وحدة التحكم عن بعد .

الاولى تعرف بالوحدة الطرفية الرئيسية وهى تكون بعيدة عن المجل الذى يسلط عليه التحكم . و الاخرى تعرف بالوحدة الطرفية للتحكم عن بعد. يتم الربط بينهما خلال قنوات دخل وخرج جهدية وتيارية .  
الوحدة الطرفية للتحكم عن بعد تستقبل الاوامر وترسل الاشارات من و الى الوحدة الطرفية الرئيسية بوسطة مجموعة من القوانين تعرف بالبروتوكولات .يجب ان تكون هناك موائمة بين الاجهزة الموجودة في الحقل والوحدة الطرفية الرئيسية .  
في هذا البحث تم لستعرض وتحليل كيفية عمل نظام التحكم اذا كن هناك اختلاف في البروتوكولات المستخمة في النظام بين الاجهزة ووحدة التحكم الرئيسية خلال جهاز وسيط اخر هو (RTU560) هذا الجهاز يعمل علي الموائمة بين البروتوكلين لإنجاح عملية التحكم.

## NOMENCLATURE

BCU: Bus Connection Units.

CMU: Communication Units.

CP: Controls Process.

CPU: Central Process Unit.

CRC: Cyclic Redundancy Code.

DCF77: Deutschland Long wave signal Frankfurt 77.5KHz.

GPS: Global Positioning System.

HCI: Host Communication Interface.

IC: Internal Communication.

IEC: International Electro technical Commission.

IED: Intelligent Electronic Device.

I/O: Input Output.

IOM: Input/Output Master.

IOC: Input Output Microcontroller.

IP: Internet Protocol.

LAN: Local Area Network.

MMI: Man Machine Interface.

MPU: Main Processing Unit.

MTU: Master Terminal Unit.

NCC: Network Control Center.

OSI: Open Systems Interconnection.

PDP: Process Data Processing.

PID: Proportional Integral Derivative.

PLC: Programmable Logic Controller.

PSU: Power Supply Unit.

RAM: Random Access Memory.

ROM: Read Only Memory.

RTU: Remote Terminal Unit.

SCADA: Supervisory Control And Data Acquisition.

SCI: Subordinate device Communication Interface.

SLC: Serial Line Controller.

STCA: Seamless Telecontrol Communication Architecture.

TCP: Transmission Control Protocol.

UART: Universal Asynchronous Receiver Transmitter.

USART: Universal Synchronous Asynchronous Receiver Transmitter.

UPS: Uninterruptible Power Supply.

UDP: User Datagram Protocol.

WAN: Wide Area Network.