آيـة

بسم الله الرحمن الرحيم

"وَلَوْلاَ فَضْلُ اللّهِ عَلَيْكَ وَرَحْمَتُهُ لَهَمَّت طَّآئِفَةٌ مُّنْهُمْ أَن يُضِلُّوكَ وَمَا يُضِلُّونَ إِلاَّ أَنفُسَهُمْ وَمَا يَضُرُّونَكَ مِن شَيْءٍ وَأَنزَلَ اللّهُ عَلَيْكَ الْكِتَابَ وَالْحِكْمَةَ وَعَلَّمَكَ مَا لَمْ تَكُنْ تَعْلَمُ وَكَانَ فَضْلُ اللّهِ عَلَيْكَ عَظِيمًا"

صدق الله العظيم

سورة النساء

الاية 113

DADICATION

To my dear mother, I am still remembering all you did for us since my father passed away.
Abdullah
2008

ACKNOWLEGEMENT

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

LIST OF TABLES

LIST OF FIGURES

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