การสร้างระบบ SCADA ที่ใช้โปรโตคอล TCP/IP และอินเตอร์เนต

Mr. Nguyen Ich Vinh

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้า

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2550

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

AN IMPLEMENTATION OF A SCADA SYSTEM BASED ON TCP/IP PROTOCOL STACK AND INTERNET

Mr. Nguyen Ich Vinh

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering Program in Electrical Engineering
Department of Electrical Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2007

Copyright of Chulalongkorn University

501838

Thesis Title	AN IMPLEMENTATION OF A SCADA SYSTEM BASED ON TCP/IP PROTOCOL STACK AND INTERNET
By	Mr. Nguyen Ich Vinh
Field of Study	Electrical Engineering
Thesis Advisor	Associate Professor. Dr. Watit Benjapolakul.
Thesis Co-advisor	Associate Professor Krisada Visavateeranon.

Accepted by the Faculty of Engineering, Chulalongkorn University in Partial Fulfillment of Requirements for Master's Degree

..... Dean of the Faculty of Engineering

(Professor Direk Lavansiri, Ph.D.)

THESIS COMMITTEE

..... Chairman

(Associate Professor. Ekachai Leelarasmee, Ph.D.)

..... Committee

(Assistant Professor. Dr. Manop Wongsaisuwan)

..... Thesis Advisor

(Associate Professor. Dr. Watit Benjapolakul)

..... Thesis Co-advisor

(Associate Professor. Krisada Visavateeranon)

##4870701621: MAJOR ELECTRICAL ENGINEERING
KEY WORDS: THE INTERNET, TCP/IP, SCADA, WEB-BASED SCADA

VINH ICH NGUYEN: การสร้างระบบ SCADA ที่ใช้โปรโตคอล TCP/IP และอินเตอร์เนต. THESIS ADVISOR: ASSOC. PROF. DR. WATIT BENJAPOLAKUL. THESIS CO-ADVISOR: ASSOC. PROF. KRISADA VISAVATEERANON. 95 + xi pp.

ปัจจุบันได้มีการนำอินเตอร์เนตมาใช้เพื่อวัตถุประสงค์ทางอุตสาหกรรมอย่างมาก ในภาคอุตสาหกรรม ระบบสกาดา (SCADA) เป็นกระบวนการที่ได้รับความนิยมมากที่สุด อย่างไรก็ตาม ปัญหาที่สำคัญที่สุดที่มีการหยิบยกขึ้นมาก็คือ ระยะทางของการสื่อสารและความเร็วในการถ่ายโอนข้อมูล ถึงแม้ว่าจะมีการเสนองานวิจัยจำนวนมาก แต่ปัญหาเรื่องความเร็วในการถ่ายโอนข้อมูล ความยืดหยุ่นของระบบและความปลอดภัยของข้อมูลยังคงไม่ได้รับการแก้ไข หรือได้รับการแก้ไขแต่ไม่สมบูรณ์ ในงานวิจัยนี้ผู้วิจัยจึงเสนอวิธีแก้ไขปัญหาบนพื้นฐานของมอดูลฮาร์ดแวร์พิเศษ ได้แก่อุปกรณ์รับ-ส่งข้อมูลผ่านอีเทอร์เนต (Ethernet IO) และการประยุกต์ใช้งานบนพื้นฐานของเว็บ การต่อร่วมเข้าไปเพื่อใช้งานซอฟต์แวร์ประยุกต์ใช้งานของระบบ สามารถเข้าถึงได้ในรูปแบบของเว็บไซต์โดยใช้อินเตอร์เนตเป็นโครงข่ายสื่อสาร งานวิจัยนี้ครอบคลุมถึงหน้าที่มูลฐานสองประการของระบบสกาดาทุกระบบซึ่งได้แก่ การได้มาซึ่งข้อมูลและการควบคุมดูแล (Data Acquisition and Supervisory Control) การใช้อินเตอร์เน็ตและอุปกรณ์รับ-ส่งข้อมูลผ่านอีเทอร์เนตทำให้ระบบที่เสนอสามารถมีหน้าที่การทำงานเพิ่มเติมได้ดังที่ได้แสดงไว้อย่างละเอียดในเนื้อหาของการวิจัย อุปกรณ์ฮาร์ดแวร์ในระบบได้รับการจำลองแบบโดยใช้ภาษา Visual C# และแมตแลบ วิธีแก้ปัญหาที่เสนอยอมให้ผู้ใช้ระบบกระทำกิจกรรมร่วมกับระบบโดยการใช้อินเตอร์เนตบราวเซอร์ ผ่านทางอินเทอร์เน็ตได้ทุกเวลาและทุกสถานที่ ผลการทดสอบแสดงให้เห็นว่า หน้าที่การทำงานของระบบทั้งหมดบรรลุวัตถุประสงค์กล่าวคือ ผู้ใช้สามารถเฝ้าตรวจข้อมูลของระบบ และสามารถออกคำสั่งต่ออุปกรณ์ในแบบเวลาจริงได้ การมีอยู่ของอินเตอร์เนตเป็นการรับรองว่าวิธีที่เสนอสามารถให้คุณลักษณะเด่นด้านราคาถูก ใน ขณะที่ยังคงรับรองหัวข้อด้านการทำงานต่างๆ ของระบบ ประเด็นเรื่องความปลอดภัยของข้อมูลได้รับการพิจารณาอย่างระมัดระวัง และต้นทุนการสร้างระบบได้รับการประมาณการ งานวิจัยนี้มีขอบเขตจำกัดเพียงแบบแผนการจำลองแบบเพื่อแสดงความสามารถในการใช้ประโยชน์อินเตอร์เนตในระบบสกาดา ในส่วนท้ายของงานวิจัยนี้ ได้มีการกล่าวถึงข้อแนะนำสำหรับการนำไปประยุกต์ใช้งานและงานวิจัยในอนาคต

ภาควิชา วิศวกรรมไฟฟ้า
สาขาวิชา วิศวกรรมไฟฟ้า
ปีการศึกษา 2550

ลายมือชื่อนิสิต.....
ลายมือชื่ออาจารย์ที่ปรึกษา.....
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม.....

##4870701621: MAJOR ELECTRICAL ENGINEERING
KEY WORDS: THE INTERNET, TCP/IP, SCADA, WEB-BASED SCADA

VINH ICH NGUYEN: AN IMPLEMENTATION OF A SCADA SYSTEM BASED ON TCP/IP PROTOCOL STACK AND INTERNET, THESIS ADVISOR: ASSOC. PROF. DR. WATIT BENJAPOLAKUL. THESIS CO-ADVISOR: ASSOC. PROF. KRISADA VISAVATEERANON. 95 + xi pp.

Nowadays, the Internet has been being in large use for industrial purposes. In the industrial sector, SCADA systems are the most popular processes. Communication range and data transfer speed have been raised as the most outstanding problems. There have been several researches proposed recently, but the problem of data transfer speed, system flexibility and security still remains unsolved or not completely solved. In this research, the proposed solution is given based on the concept of a special hardware module called Ethernet IO and a web-based application. The system application software interface is accessed as a website. Internet became the communication network. The two basic functions of every SCADA system which are data acquisition and supervisory control have been covered. The use of the Internet and the Ethernet IO board provides additional functions as discussed in details in the contents of the research. The hardware devices in the system are simulated using Visual C# and Matlab. The proposed solution allows system users to interact with the system using Internet browsers via Internet at any time and from any where. Test results have shown that all the system functionalities have been achieved in the way that users can monitor system's data and issue control commands on devices in a real-time manner. The presence of Internet promises to give a low-cost feature to the solution while still ensuring the system's criteria. The security issue is considered carefully and the implementation cost estimation is also given. This search is limited with the simulation scheme in order to demonstrate the ability of utilizing the Internet in SCADA system. Recommendations for applications and future works on this research are given in details in the last part of this research.

Department. Electrical Engineering... **Student's Signature**.....
Field of Study...Electronics..... **Advisor's Signature**.....
Academic Year...2007..... **Co-advisor's Signature**.....

ACKNOWLEDGEMENT

"If you fail to plan, you are planning to fail"

I had tried my best to make a proper working plan on the thesis, to ensure the graduation in the given time of two years.

I would never forget, and I would like to send my warmest thank to these people who had greatly contributed to my thesis completion.

1. Assoc. Prof. Dr. Watit Benjapolakul, my advisor, for his continuous attention and care as well as the very useful advices for the whole thesis period.

2. Assoc. Prof. Krisada Visavateeranon, my co-advisor, for his kindness and deep support from the very first steps to Chulalongkorn University

3. Assoc. Prof. Dr. Ekachai Leelarasmee, the committee chairman, for his kind consideration as well as his advices on my paper.

4. Assist. Prof. Dr. Manop Wongsaisuwan, the committee member, for his comments, suggestions and questions which had strengthened the content of my thesis.

5. Prof. Lien Van Nguyen and Dr. Hue Thi Phan, the two lecturers at HUT, for their recommendations to Chulalongkorn University.

6. Mr. Dao Quang Minh, an IT expert, for his significant help in designing and implementing the application software.

7. AUN/SEED-NET JICA Project, the scholarship management board, for the full financial support in the whole study.

8. My parents and my three elder sisters, for their endless love and care which raised the motivation in me during the hard study.

9. All friends in IIRL and from other research laboratories, for their helps and supports.

CONTENTS

Page

Abstract (Thai) ..... **iv**

Abstract (English) ..... **v**

Acknowledgement ..... **vi**

Contents ..... **vii**

List of Tables ..... **ix**

List of Figures ..... **x**

Chapter I Introduction **1**

1.1. Motivation 1

1.2. Objectives 4

1.3. Scope of Thesis 5

1.4. Methodology 5

1.5. Contributions 7

Chapter II Literature Review **8**

Chapter III Proposed System **18**

3.1. System's Features 18

3.2. Basic Technologies 19

3.3. General System Architecture 25

Chapter IV System Implementation **28**

4.1. Tentative Architecture 28

4.2. Implementation Details 29

4.2.1. Hardwares 29

4.2.2. Software Tools and Modules 31

A. Database 33

Page

B. Application Software 46

C. Device Simulator 54

4.3. Testing Results 62

4.3.1. Getting Started 62

4.3.2. Detailed Operation 65

1. User Management 65

2. Device and Data Management 67

3. Event Log 73

4. Security Management 74

5. Device Simulator Operation 77

4.4. Cost Estimation 80

4.4.1 From the Developer Side 80

4.4.2 From the Customer Side 82

Chapter V Conclusion 83

5.1. Summary 83

5.2. Recommended Applications 85

5.3. Recommendation for Future Works 86

5.3.1. Improvements on the testing system 86

5.3.2. Recommendations on newly-built systems 90

References 94

Biography 95

LIST OF TABLES

Table		Page
4.1	Event Log Type	52
4.2	Matlab Product Price	80
4.3	.NET Programming Products	81
5.1	Gateway	91

List of Figures

Figure		Page
2.1	SCADA System Architecture proposed by [1]	8
2.2	SCADA System Architecture proposed by [2]	9
2.3	SCADA System Architecture proposed by [3]	10
2.4	SCADA System Architecture proposed by [4]	11
2.5	SCADA System Architecture proposed by [5]	12
2.6	SCADA System Architecture proposed by [6]	13
2.7	SCADA System Architecture proposed by [7]	14
2.8	SCADA System Architecture proposed by [8]	15
3.1	Internet Architecture	20
3.2	General System Architecture	25
4.1	Tentative Implementation Architecture	29
4.2	Server Computer	30
4.3	Client Computer	30
4.4	DS Computer	30
4.5	Router + Modem	31
4.6	Testing System	32
4.7	Connecting to MySQL	35
4.8	MySQL Workspace	35
4.9	ODBC Architecture	48
4.10	Data Management Principle from Server Side	49
4.11	Data Management Principle from Client Side	50
4.12	Device Control Principle	51
4.13	Physical Model of DC Motors	55
4.14	Mathematical Model of DC Motors	55
4.15	DS Operational and Interface Diagram	57
4.16	PID Block Diagram	59
4.17	DC Motor with PID Controller Block Diagram	60
4.18	Welcome Page	63
4.19	Login Page	64
4.20	Home Page	64
4.21	Server Idle time	64

Figure Page

4.22 User Management Page 65
4.23 Edit User 66
4.24 Locked Users 66
4.25 Add New User 66
4.26 Connection Speed and Variance Time 69
4.27 System Time and History Time 69
4.28 Historical Angular Speed 69
4.29 Historical Control Signal 70
4.30 Historical Armature Current 70
4.31 Step Response of DC Motor under no Controller 71
4.32 Response Speed of DC Motor under PID Controller 71
4.33 Device Management Page 72
4.34 Event Log Page 73
4.35 Router Configuration Page 74
4.36 Outbound Services Settings 75
4.37 Inbound Services Settings 75
4.38 User Authentication Tool 76
4.39 IP Approval Tool 76
4.40 User Permission Tool 77
4.41 DS Specifications 78
4.42 DS Operation under WithoutPID scheme 78
4.43 DS Operation under WithPID scheme 79
5.1 DS and SCADA interface at the same time operating 82
5.2 DS Interface with 0 points 86
5.3 MD5 Operation 88
5.4 Un-smooth Data Graphs 89
5.5 Industrial Server 91
5.6 Monitoring by Location 91
5.7 Monitoring by System 92
5.8 Suggested System Architecture for Further Study 92