

# CONTENTS

|                                                      |      |
|------------------------------------------------------|------|
| Abstract .....                                       | i    |
| Abstract (Arabic) .....                              | ii   |
| Dedication .....                                     | iii  |
| Acknowledge .....                                    | iv   |
| Table of contents.....                               | v    |
| List of tables.....                                  | viii |
| List of figures.....                                 | ix   |
|                                                      |      |
| chapter One -- Introduction                          |      |
| 1.1 Statement of the problem .....                   | 1    |
| 1.2 Subject significance .....                       | 1    |
| 1.3 Project objective .....                          | 2    |
| 1.4 Approaches .....                                 | 2    |
| 1.5 Thesis layout .....                              | 3    |
|                                                      |      |
| Chapter Two -- Theory of IEC60870-5-101 protocol     |      |
| 2.1 Introduction.....                                | 5    |
| 2.2 Reference model for communication networks ..... | 7    |
| 2.3 Message structure .....                          | 9    |
| 2.3.1 Start frame .....                              | 10   |
| 2.3.2 Data Unit Identifier .....                     | 16   |
| 2.3.3 Information Object .....                       | 20   |
| 2.4 Station initialization .....                     | 22   |
| 2.5 Application functions .....                      | 24   |

|                                                          |    |
|----------------------------------------------------------|----|
| 2.5.1 Station interrogation -----                        | 24 |
| 2.5.2 Cyclic data transmission -----                     | 25 |
| 2.5.3 Background scan -----                              | 26 |
| 2.5.4 Acquisition of events -----                        | 26 |
| 2.5.5 Clock synchronization -----                        | 27 |
| 2.5.6 Command transmission -----                         | 27 |
| 2.5.7 Reverse direction -----                            | 28 |
| 2.6 Example of the use of IEC 60870-5-101 protocol ----- | 29 |

### Chapter Three -- Simulation of a telecontrol outstation

|                                                 |    |
|-------------------------------------------------|----|
| 3.1 Basis of the simulation -----               | 30 |
| 3.2 Main procedures -----                       | 31 |
| 3.2.1 Transfer_click procedure -----            | 31 |
| 3.2.2 Primary_Request_Status proprocedure ----- | 33 |
| 3.2.4 Secondary_Receive procedure -----         | 35 |
| 3.2.4 Primary_Reset_Status procedure -----      | 38 |
| 3.2.5 Second_send_ASDU procedure -----          | 41 |
| 3.2.6 Prim_receive_ASDU procedure -----         | 43 |

### Chapter Four -- Results

|                              |    |
|------------------------------|----|
| 4.1 Program interfaces ----- | 46 |
|------------------------------|----|

### Chapter Five – Hardware and Simulation

|                              |    |
|------------------------------|----|
| 5.1 Hardware and design----- | 50 |
| 5.2 Design steps-----        | 53 |

### Chapter Six – Conclusion and Comments

|                      |    |
|----------------------|----|
| 6.1 Conclusion ----- | 56 |
|----------------------|----|

References

Appendix A – Program Code

Appendix B – Interoperability

Appendix C – Possibilities of the cause of transmission for the ASDUs

Appendix D – General structure of the ASDU message